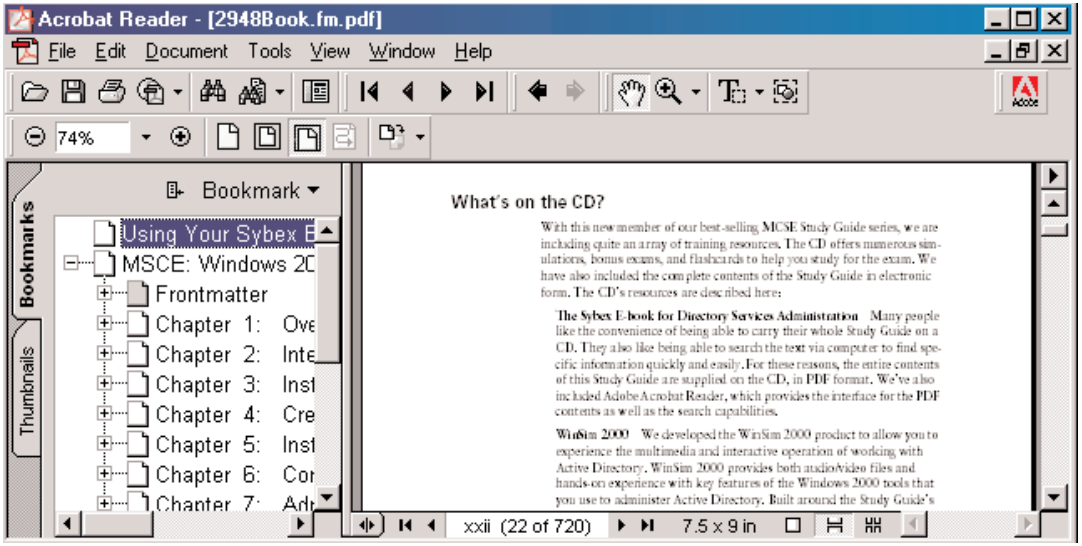
Using Your Sybex Electronic Book

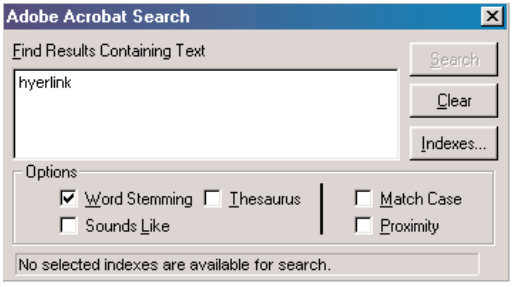
To realize the full potential of this Sybex electronic book, you must have Adobe Acrobat Reader with Search installed on your computer. To find out if you have the correct version of Acrobat Reader, click on the Edit menu—Search should be an option within this menu file. If Search is not an option in the Edit menu, please exit this application and install Adobe Acrobat Reader with Search from this CD (double-click rp500enu.exe in the Adobe folder).

Navigation

Navigate through the book by clicking on the headings that appear in the left panel; the corresponding page from the book displays in the right panel.



Search



To search, click the Search Query button on the toolbar or choose Edit >Search > Query to open the Search window. In the Adobe Acrobat Search dialog's text field, type the text you want to find and click Search.

Use the Search Next button (Control+U) and Search Previous button (Control+Y) to go to other matches in the book. The Search command also has powerful tools for limiting and expanding the definition of the term you are searching for. Refer to Acrobat's online Help (Help > Plug-In Help > Using Acrobat Search) for more information.

Click here to begin using your Sybex Electronic Book!

CCNP™:
Switching
Study Guide

Todd Lammle
Eric Quinn

San Francisco • London

SYBEX

 www.sybex.com

Associate Publisher: Neil Edde
Acquisitions and Developmental Editor: Maureen Adams
Editor: Sharon Wilkey
Production Editor: Kelly Winquist
Technical Editors: Patrick Bass, Arthur Pfund
Book Designer: Bill Gibson
Graphic Illustrators: Jeff Wilson, Happenstance Type-O-Rama; Tony Jonick
Electronic Publishing Specialists: Stacey Loomis and Rozi Harris, Interactive Composition Corporation
Proofreaders: Laurie O'Connell, Nancy Riddiough, Dave Nash, Sarah Tannehill
Indexer: Ted Laux
CD Coordinator: Dan Mummert
CD Technician: Kevin Ly
Cover Designer: Archer Design
Cover Photographer: Natural Selection

Library of Congress Card Number: 2002108075

ISBN: 0-7821-4153-6

Manufactured in the United States of America

10 9 8 7 6 5 4 3 2 1

To Our Valued Readers:

The Cisco Certified Network Professional program well deserves its position as the leading high-level certification in the internetworking arena. Sybex is proud to have helped hundreds of thousands of CCNP candidates prepare for their exams over the years, and we are excited about the opportunity to continue to provide individuals with the knowledge and skills they'll need to succeed in the highly competitive IT industry.

With the recent revision of the four exams required for the CCNP—Routing, Switching, Remote Access, and Support—Cisco raised the bar considerably, adding simulation questions to two of the and refreshing the question pools of all exams to better reflect current technologies. Sybex welcomes these changes as we strongly advocate a comprehensive and practical instructional approach to certification exam preparation. It has always been Sybex's mission to teach exam candidates how new technologies work in the real world, not to simply feed them answers to test questions. Sybex was founded on the premise of providing technical skills to IT professionals, and we have continued to build on that foundation. Over the years, we have made significant improvements to our study guides based on feedback from readers, suggestions from instructors, and comments from industry leaders.

Cisco's new CCNP exams are indeed challenging. The authors have worked hard to ensure that this Study Guide is comprehensive, in-depth, and pedagogically sound. We're confident that this book, along with the collection of cutting-edge software study tools included on the CD, will meet and exceed the demanding standards of the certification marketplace and help you, the CCNP exam candidate, succeed in your endeavors.

Good luck in pursuit of your CCNP certification!

Neil Edde
Associate Publisher—Certification
Sybex, Inc.

Software License Agreement: Terms and Conditions

The media and/or any online materials accompanying this book that are available now or in the future contain programs and/or text files (the "Software") to be used in connection with the book. SYBEX hereby grants to you a license to use the Software, subject to the terms that follow. Your purchase, acceptance, or use of the Software will constitute your acceptance of such terms.

The Software compilation is the property of SYBEX unless otherwise indicated and is protected by copyright to SYBEX or other copyright owner(s) as indicated in the media files (the "Owner(s)"). You are hereby granted a single-user license to use the Software for your personal, noncommercial use only. You may not reproduce, sell, distribute, publish, circulate, or commercially exploit the Software, or any portion thereof, without the written consent of SYBEX and the specific copyright owner(s) of any component software included on this media.

In the event that the Software or components include specific license requirements or end-user agreements, statements of condition, disclaimers, limitations or warranties ("End-User License"), those End-User Licenses supersede the terms and conditions herein as to that particular Software component. Your purchase, acceptance, or use of the Software will constitute your acceptance of such End-User Licenses.

By purchase, use or acceptance of the Software you further agree to comply with all export laws and regulations of the United States as such laws and regulations may exist from time to time.

Reusable Code in This Book

The author(s) created reusable code in this publication expressly for reuse by readers. Sybex grants readers limited permission to reuse the code found in this publication or its accompanying CD-ROM so long as the author(s) are attributed in any application containing the reusable code and the code itself is never distributed, posted online by electronic transmission, sold, or commercially exploited as a stand-alone product.

Software Support

Components of the supplemental Software and any offers associated with them may be supported by the specific Owner(s) of that material, but they are not supported by SYBEX. Information regarding any available support may be obtained from the Owner(s) using the information provided in the appropriate read.me files or listed elsewhere on the media.

Should the manufacturer(s) or other Owner(s) cease to offer support or decline to honor any offer, SYBEX bears no responsibility. This notice concerning support for the Software is provided for your information only. SYBEX is not the agent or principal of the Owner(s), and SYBEX is in no way responsible for providing any support for the Software, nor is it liable or responsible for any support provided, or not provided, by the Owner(s).

Warranty

SYBEX warrants the enclosed media to be free of physical defects for a period of ninety (90) days after purchase. The Software is not available from SYBEX in any other form or media than that enclosed herein or posted to www.sybex.com. If you discover a defect in the media during this warranty period, you may obtain a replacement of identical format at no charge by sending the defective media, postage prepaid, with proof of purchase to:

SYBEX Inc.
Product Support Department
1151 Marina Village Parkway
Alameda, CA 94501
Web: http://www.sybex.com

After the 90-day period, you can obtain replacement media of identical format by sending us the defective disk, proof of purchase, and a check or money order for $10, payable to SYBEX.

Disclaimer

SYBEX makes no warranty or representation, either expressed or implied, with respect to the Software or its contents, quality, performance, merchantability, or fitness for a particular purpose. In no event will SYBEX, its distributors, or dealers be liable to you or any other party for direct, indirect, special, incidental, consequential, or other damages arising out of the use of or inability to use the Software or its contents even if advised of the possibility of such damage. In the event that the Software includes an online update feature, SYBEX further disclaims any obligation to provide this feature for any specific duration other than the initial posting.

The exclusion of implied warranties is not permitted by some states. Therefore, the above exclusion may not apply to you. This warranty provides you with specific legal rights; there may be other rights that you may have that vary from state to state. The pricing of the book with the Software by SYBEX reflects the allocation of risk and limitations on liability contained in this agreement of Terms and Conditions.

Shareware Distribution

This Software may contain various programs that are distributed as shareware. Copyright laws apply to both shareware and ordinary commercial software, and the copyright Owner(s) retains all rights. If you try a shareware program and continue using it, you are expected to register it. Individual programs differ on details of trial periods, registration, and payment. Please observe the requirements stated in appropriate files.

Copy Protection

The Software in whole or in part may or may not be copy-protected or encrypted. However, in all cases, reselling or redistributing these files without authorization is expressly forbidden except as specifically provided for by the Owner(s) therein.

To Carolann and Lee, for putting up with the long overseas trips followed by a return to writing.

—Eric Quinn

Acknowledgments

Thanks go out to Maureen and Kelly for keeping the book organized, Patrick for double checking my work, and Sharon for making the words flow. Without them, this new version wouldn't be here.

—Eric Quinn

The authors would like to thank all the folks associated with Sybex who helped get this book on the shelves. Sharon Wilkey was a superb editor. This book would be a stack of typewritten pages without the layout finesse of Rozi Harris, Stacey Loomis, and the compositors at Interactive Composition Corporation. Tony Jonick and Jeff Wilson magically transformed sketches into works of art. Thanks to technical editors Patrick Bass and Arthur Pfund for being our watchdogs. Finally, our other watchdogs are the proof-readers: thanks to Laurie O'Connell, Nancy Riddiough, Dave Nash, and Sarah Tannehill.

Introduction

Welcome to the exciting world of Cisco certification! You have picked up this book because you want something better; namely, a better job with more satisfaction. Rest assured that you have made a good decision. Cisco certification can help you get your first networking job, or more money and a promotion if you are already in the field.

Cisco certification can also improve your understanding of the internetworking of more than just Cisco products: You will develop a complete understanding of networking and how different network topologies work together to form a network. This is beneficial to every networking job and is the reason Cisco certification is in such high demand, even at companies with few Cisco devices.

Cisco is the king of routing and switching, the Microsoft of the internetworking world. The Cisco certifications reach beyond the popular certifications, such as the MCSE and CNE, to provide you with an indispensable factor in understanding today's network—insight into the Cisco world of internetworking. By deciding that you want to become Cisco certified, you are saying that you want to be the best—the best at routing and the best at switching. This book will lead you in that direction.

How to Use This Book

If you want a solid foundation for the serious effort of preparing for the Cisco Certified Network Professional (CCNP) Switching exam, then look no further. We have spent hundreds of hours putting together this book with the sole intention of helping you to pass the CCNP Switching exam.

This book is loaded with lots of valuable information, and you will get the most out of your studying time if you understand how we put this book together.

To best benefit from this book, we recommend the following study method:

1. Take the assessment test immediately following this introduction. (The answers are at the end of the test.) It's OK if you don't know any of the answers; that is why you bought this book! Carefully read over the explanations for any question you get wrong and note which chapters the material comes from. This information should help you plan your study strategy.

2. Study each chapter thoroughly, making sure that you fully understand the information and the test objectives listed at the beginning of each chapter. Pay extra-close attention to any chapter where you missed questions in the assessment test.
3. If you do not have Cisco equipment available, be sure to study the examples carefully. Also, check `www.routersim.com` for router simulator software that provides drag-and-drop networking configurations.
4. Answer all of the review questions related to each chapter. (The answers appear at the end of the chapter.) Note the questions that confuse you and study those sections of the book again. Do not just skim these questions! Make sure you understand completely the reason for each answer.
5. Try your hand at the practice exams that are included on the companion CD. The questions in these exams appear only on the CD. This will give you a complete overview of what you can expect to see on the real CCNP Switching exam.
6. Test yourself using all the flashcards on the CD. There are brand new and updated flashcard programs on the CD to help you prepare completely for the CCNP Switching exam. These are a great study tool!

The electronic flashcards can be used on your Windows computer, Pocket PC, or Palm device.

7. Make sure you read the "Key Terms" and "Exam Essentials" lists at the end of the chapters. These study aids will help you finish each chapter with the main points fresh in the your mind; they're also helpful as a quick refresher before heading into the testing center.

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. If you work hard, you will be surprised at how quickly you learn this material.

If you follow the steps listed above, and really study and practice the review questions, CD exams, and electronic flashcards, it would be hard to fail the CCNP Switching exam.

What Does This Book Cover?

This book covers everything you need to pass the CCNP Switching exam. The following list describes what you will learn in each chapter:

- Chapter 1 describes the traditional campus network model and moves into the new emerging campus model. Layer 2, 3, and 4 switching is also discussed. In addition, this chapter discusses the Cisco three-layer model, the Cisco switching product line, and how to build switch and core blocks.
- Chapter 2 describes the various Ethernet media types and how to log in and configure both a set-based and IOS-based Cisco Catalyst switch.
- Chapter 3 covers VLANs—how they work and how to configure them in a Cisco internetwork. Trunking and VLAN Trunk Protocol (VTP) are described and implemented.
- Chapter 4 gives you an in-depth look at the Spanning Tree Protocol (STP), its timers, and how to configure STP in a switch.
- Chapter 5 shows you how to configure STP timers and includes a discussion of root bridge selection. Redundant links with STP are also covered.
- Chapter 6 covers Inter-Switch Link (ISL) routing. Both internal route processors and external route processors are covered, as well as how to configure both internal and external route processors to connect multiple VLANs.
- Chapter 7 provides the fundamentals of Multi-Layer Switching on both internal and external route processors. In addition to covering IP routing with MLS, we show you how to configure the MLS engine.
- Chapter 8 covers the background of multicast addresses and how to translate from a layer 3 address to a layer 2 multicast address. This chapter also covers IGMP and CGMP.
- Chapter 9 is about configuring multicast in a Cisco internetwork. Enabling multicast, joining a multicast group, and enabling CGMP are also covered.

- Appendix A includes all the commands used in this book along with explanations of each command and how they are used with both access layer and distribution layer switches.
- Appendix B is a list of all multicast addresses as listed in RFC 1112. It also includes a list of all the assigned multicast addresses.

Each chapter begins with a list of the topics covered related to the CCNP Switching test, so make sure to read them over before working through the chapter. In addition, each chapter ends with review questions specifically designed to help you retain the knowledge presented. To really nail down your skills, read each question carefully, and if possible, work through the chapters' hands-on labs.

What's on the CD?

We worked hard to provide some really great tools to help you with your certification process. All of the following tools should be loaded on your workstation when studying for the test.

The EdgeTest Test Preparation Software

The test preparation software, provided by EdgeTek Learning Systems, prepares you to pass the CCNP Switching exam. In this test engine, you will find all the review and assessment questions from the book, plus two additional bonus exams that appear exclusively on the CD. You can take the assessment test, test yourself by chapter or by topic, take the practice exams, or take a randomly generated exam comprising all the questions.

To find more test-simulation software for all Cisco and Microsoft exams, look for the exam link on `www.lammleprep.com`.

Electronic Flashcards for PC, Pocket PC, and Palm Devices

To prepare for the exam, you can read this book, study the review questions at the end of each chapter, and work through the practice exams included in the book and on the companion CD. But wait, there's more! You can also test yourself with the flashcards included on the CD. If you can get through these difficult questions and understand the answers, you'll know you're ready for the CCNP Switching exam.

The flashcards include 190 questions specifically written to hit you hard and make sure you are ready for the exam. Between the review questions, practice exams, and flashcards, you'll be more than prepared for the exam.

CCNP Switching Study Guide in PDF

Sybex offers the *CCNP Switching Study Guide* in PDF format on the CD so you can read the book on your PC or laptop. This will be helpful to readers who travel and don't want to carry a book, as well as to readers who prefer to read from their computer. (Acrobat Reader 5 is also included on the CD.)

Commands Used in this Study Guide

We've compiled a list of all the Cisco commands used in each chapter. This list is in PDF format on the companion CD-ROM so you can easily search the list for the commands you need.

Simulation Questions

In addition to multiple-choice and drag-and-drop questions, Cisco has included some questions on their exams that simulate working on routers and switches in a network environment. In response, we have included a simulation question program on our test engine. We designed our program to help further your hands-on networking skills and to fully prepare you for taking the Switching (640-604) exam. At the time of this printing, Cisco is only including simulation questions on the Routing (640-603) and Remote Access (640-605) exams. Please visit the Cisco training and certification website (`http://www.cisco.com/public/training_cert.shtml`) for the latest exam information.

Cisco—A Brief History

Many readers may already be familiar with Cisco and what they do. However, those of you who are new to the field, just coming in fresh from your MCSE, and those of you who maybe have 10 or more years in the field but wish to brush up on the new technology may appreciate a little background on Cisco.

In the early 1980s, Len and Sandy Bosack, a married couple who worked in different computer departments at Stanford University, were having trouble getting their individual systems to communicate (like many married people). So in their living room they created a gateway server that made it easier for their disparate computers in two different departments to communicate

using the IP protocol. In 1984, they founded cisco Systems (notice the small *c*) with a small commercial gateway server product that changed networking forever. Some people think the name was intended to be San Francisco Systems but the paper got ripped on the way to the incorporation lawyers—who knows? In 1992, the company name was changed to Cisco Systems, Inc.

The first product the company marketed was called the Advanced Gateway Server (AGS). Then came the Mid-Range Gateway Server (MGS), the Compact Gateway Server (CGS), the Integrated Gateway Server (IGS), and the AGS+. Cisco calls these "the old alphabet soup products."

In 1993, Cisco came out with the amazing 4000 router and then created the even more amazing 7000, 2000, and 3000 series routers. These are still around and evolving (almost daily, it seems).

Cisco has since become an unrivaled worldwide leader in networking for the Internet. Its networking solutions can easily connect users who work from diverse devices on disparate networks. Cisco products make it simple for people to access and transfer information without regard to differences in time, place, or platform.

In the big picture, Cisco provides end-to-end networking solutions that customers can use to build an efficient, unified information infrastructure of their own or to connect to someone else's. This is an important piece in the Internet/networking–industry puzzle because a common architecture that delivers consistent network services to all users is now a functional imperative. Because Cisco Systems offers such a broad range of networking and Internet services and capabilities, users who need to regularly access their local network or the Internet can do so unhindered, making Cisco's wares indispensable.

Cisco answers this need with a wide range of hardware products that form information networks using the Cisco Internetwork Operating System (IOS) software. This software provides network services, paving the way for networked technical support and professional services to maintain and optimize all network operations.

Along with the Cisco IOS, one of the services Cisco created to help support the vast amount of hardware it has engineered is the Cisco Certified Internetwork Expert (CCIE) program, which was designed specifically to equip people to effectively manage the vast quantity of installed Cisco networks. The business plan is simple: If you want to sell more Cisco equipment and have more Cisco networks installed, ensure that the networks you install run properly.

Clearly, having a fabulous product line isn't all it takes to guarantee the huge success that Cisco enjoys—lots of companies with great products are

now defunct. If you have complicated products designed to solve complicated problems, you need knowledgeable people who are fully capable of installing, managing, and troubleshooting them. That part isn't easy, so Cisco began the CCIE program to equip people to support these complicated networks. This program, known colloquially as the Doctorate of Networking, has also been very successful, primarily due to its extreme difficulty. Cisco continuously monitors the program, changing it as it sees fit, to make sure that it remains pertinent and accurately reflects the demands of today's internetworking business environments.

Building upon the highly successful CCIE program, Cisco Career Certifications permit you to become certified at various levels of technical proficiency, spanning the disciplines of network design and support. So, whether you're beginning a career, changing careers, securing your present position, or seeking to refine and promote your position, this is the book for you!

Cisco's Network Support Certifications

Initially, to secure the coveted CCIE, you took only one test and then you were faced with the (extremely difficult) lab, an all-or-nothing approach that made it tough to succeed. In response, Cisco created a series of new certifications to help you get the coveted CCIE, as well as aid prospective employers in measuring skill levels. With these new certifications, which added a better approach to preparing for that almighty lab, Cisco opened doors that few were allowed through before. So, what are these certifications and how do they help you get your CCIE?

Cisco Certified Network Associate (CCNA)

The CCNA certification was the first in the new line of Cisco certifications, and was the precursor to all current Cisco certifications. With the new certification programs, Cisco has created a type of stepping-stone approach to CCIE certification. Now, you can become a Cisco Certified Network Associate with the help of the *CCNA: Cisco Certified Network Associate Study Guide* (Sybex), and $125 for the test. And you don't have to stop there—you can choose to continue with your studies and achieve a higher certification, called the Cisco Certified Network Professional (CCNP). Someone with a CCNP has all the skills and knowledge he or she needs to attempt the CCIE lab. However, because no textbook can take the place of practical experience, we'll discuss what else you need to be ready for the CCIE lab shortly.

Cisco Certified Network Professional (CCNP)

So you're thinking, "Great, what do I do after passing the CCNA exam?" Well, if you want to become a CCIE in Routing and Switching (the most popular certification), understand that there's more than one path to that much-coveted CCIE certification. The first way is to continue studying and become a Cisco Certified Network Professional (CCNP), which means four more tests, in addition to the CCNA certification.

The CCNP program will prepare you to understand and comprehensively tackle the internetworking issues of today and beyond—and it is not limited to the Cisco world. You will undergo a metamorphosis, vastly increasing your knowledge and skills through the process of obtaining these certifications.

While you don't need to be a CCNP or even a CCNA to take the CCIE lab, it's extremely helpful if you already have these certifications.

What Skills Do You Need to Become a CCNP?

Cisco demands a certain level of proficiency for its CCNP certification. In addition to mastering the skills required for the CCNA, you should be able to do the following:

- Install, configure, operate, and troubleshoot complex routed LAN, routed WAN, and switched LAN networks, along with dial-access services.
- Understand complex networks, such as IP, IGRP, IPX, async routing, extended access lists, IP RIP, route redistribution, IPX RIP, route summarization, OSPF, VLSM, BGP, serial interfaces, EIGRP, Frame Relay, ISDN, ISL, X.25, DDR, PSTN, PPP, VLANs, Ethernet, access lists, 802.10, and transparent and translational bridging.
- Install and/or configure a network to increase bandwidth, quicker network response times, and improve reliability and quality of service.
- Maximize performance through campus LANs, routed WANs, and remote access.
- Improve network security.
- Create a global intranet.
- Provide access security to campus switches and routers.

- Provide increased switching and routing bandwidth—end-to-end resiliency services.
- Provide custom queuing and routed priority services.

How Do You Become a CCNP?

After becoming a CCNA, the four exams you must take to get your CCNP are as follows:

Exam 640-603: Routing This exam continues to build on the fundamentals learned in the CCNA course. It focuses on large multiprotocol internetworks and how to manage them with access lists, queuing, tunneling, route distribution, route maps, BGP, EIGRP, OSPF, and route summarization. The *CCNP: Routing Study Guide* (Sybex) covers all the objectives you need to understand to pass the Routing exam.

Exam 640-604: Switching This exam tests your knowledge of the 1900, 2900, 3500, and 5000 series of Catalyst switches. This book covers all the objectives you need to understand to pass the Switching exam.

Exam 640-605: Remote Access This exam tests your knowledge of installing, configuring, monitoring, and troubleshooting Cisco ISDN and dial-up access products. You must understand PPP, ISDN, Frame Relay, and authentication. The *CCNP: Remote Access Study Guide* (Sybex) covers all the exam objectives.

Exam 640-606: Support This tests you on the Cisco troubleshooting skills needed for Ethernet and Token Ring LANs, IP, IPX, and AppleTalk networks, as well as ISDN, PPP, and Frame Relay networks. The *CCNP: Support Study Guide* (Sybex) covers all the objectives you need to understand to pass the Support exam.

`www.routersim.com` has a complete Cisco router simulator for all CCNP exams.

If you hate tests, you can take fewer of them by signing up for the Support exam and then taking just one more long exam called the Foundation R/S exam (640-509). Doing this also gives you your CCNP—but beware; it's a really long test that fuses all the material from the Routing, Switching, and Remote Access exams into one exam. Good luck! However, by taking this exam, you get three tests for the price of two, which saves you $125 (if you pass). Some people think it's easier to take the Foundation R/S exam because

you can leverage the areas that you would score higher in against the areas in which you wouldn't.

Remember that test objectives and tests can change at any time without notice. Always check the Cisco website for the most up-to-date information (www.cisco.com).

Cisco Certified Internetwork Expert (CCIE)

You've become a CCNP, and now you fix your sights on getting your Cisco Certified Internetwork Expert (CCIE) in Routing and Switching—what do you do next? Cisco recommends that before you take the lab, you take the Cisco Internetwork Design (CID) exam (640-025) and the Cisco-authorized course called Installing and Maintaining Cisco Routers (IMCR). By the way, no Sylvan Prometric test for IMCR exists at the time of this writing, and Cisco recommends a *minimum* of two years of on-the-job experience before taking the CCIE lab. After jumping those hurdles, you then have to pass the CCIE-R/S Exam Qualification (350-001) before taking the actual lab.

How Do You Become a CCIE?

To become a CCIE, Cisco recommends you do the following:

1. Attend all the recommended courses at an authorized Cisco training center and pony up around $15,000–$20,000, depending on your corporate discount.
2. Pass the written qualification exam ($300 per exam—so hopefully, you'll pass it the first time).
3. Pass the one-day, hands-on lab at Cisco. This costs $1,250 per lab, and many people fail two or more times. (Some never make it through!) Also, there are a limited number of places to take the lab: San Jose, California; Research Triangle Park, North Carolina; Sydney, Australia; Tokyo, Japan; Sao Paulo, Brazil; Bangalore, India; Johannesburg, South Africa; Beijing, China; Singapore; and Brussels, Belgium. This means that you might just need to add travel costs to that $1,250. Cisco has added new sites lately for the CCIE lab; it is best to check the Cisco website for the most current information.

Cisco has changed the CCIE lab from a two-day to a one-day lab. Please see www.cisco.com for the latest information.

What Skills Do You Need to Become a CCIE?

The CCIE Routing and Switching exam includes the advanced technical skills that are required to maintain optimum network performance and reliability, as well as advanced skills in supporting diverse networks that use disparate technologies. CCIEs just don't have problems getting jobs; these experts are inundated with offers to work for six-figure salaries. But that's because it isn't easy to attain the level of capability that is mandatory for Cisco's CCIE. For example, a CCIE can easily do the following:

- Install, configure, operate, and troubleshoot complex routed LAN, routed WAN, switched LAN, and ATM networks, and dial-access services.
- Diagnose and resolve network faults.
- Use packet/frame analysis and Cisco debugging tools.
- Document and report the problem-solving processes used.
- Understand general LAN/WAN characteristics, including data encapsulation and layering; windowing and flow control, and their relation to delay; error detection and recovery; link-state, distance vector, and switching algorithms; management, monitoring, and fault isolation.
- Understand a variety of corporate technologies—including major services provided by Desktop, WAN, and Internet groups—as well as the functions; addressing structures; and routing, switching, and bridging implications of each of their protocols.
- Understand Cisco-specific technologies, including router/switch platforms, architectures, and applications; communication servers; protocol translation and applications; configuration commands and system/network impact; and LAN/WAN interfaces, capabilities, and applications.
- Design, configure, install, and verify voice-over-IP and voice-over-ATM networks.

Cisco's Network Design Certifications

In addition to the network support certifications, Cisco has created another certification track for network designers. The two certifications within this track are the Cisco Certified Design Associate and Cisco Certified Design Professional certifications. If you're reaching for the CCIE stars, we highly recommend the CCNP and CCDP certifications before attempting the lab (or attempting to advance your career).

This certification will give you the knowledge you need to design routed LAN, routed WAN, and switched LAN and ATM LANE networks.

Cisco Certified Design Associate (CCDA)

To become a CCDA, you must pass the Designing Cisco Networks (DCN) exam (640-441). To pass this test, you must understand how to do the following:

- Design simple routed LAN, routed WAN, and switched LAN and ATM LANE networks.
- Use Network-layer addressing.
- Filter with access lists.
- Use and propagate VLAN.
- Size networks.

The Sybex *CCDA: Cisco Certified Design Associate Study Guide* (1999) is the most cost-effective way to study for and pass your CCDA exam.

Cisco Certified Design Professional (CCDP)

If you're already a CCNP and CCDA and want to get your CCDP, you can simply take the CID 640-025 test. If you're not yet a CCNP, however, you must take the CCDA, CCNA, Routing, Switching, Remote Access, and CID exams.

CCDP certification skills include the following:

- Designing complex routed LAN, routed WAN, and switched LAN and ATM LANE networks
- Building upon the base level of the CCDA technical knowledge

CCDPs must also demonstrate proficiency in the following:

- Network-layer addressing in a hierarchical environment
- Traffic management with access lists
- Hierarchical network design
- VLAN use and propagation
- Performance considerations: required hardware and software; switching engines; memory, cost, and minimization

Where Do You Take the Exams?

You may take the exams at any of the more than 800 Sylvan Prometric Authorized Testing Centers around the world (`www.2test.com`), or call 800-204-EXAM (3926). You can also register and take the exams at a VUE authorized center (`www.vue.com`) or call (877) 404-EXAM (3926).

To register for a Cisco Certified Network Professional exam:

1. Determine the number of the exam you want to take. (The CCNP Switching exam number is 640-604.)
2. Register with the nearest Sylvan Prometric Registration Center or VUE testing center. At this point, you will be asked to pay in advance for the exam. At the time of this writing, the exams are $125 each and must be taken within one year of payment. You can schedule exams up to six weeks in advance or as late as the same day you want to take it—but if you fail a Cisco exam, you must wait 72 hours before you will be allowed to retake the exam. If something comes up and you need to cancel or reschedule your exam appointment, contact Sylvan Prometric or 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 CCNP Switching Exam

The CCNP Switching test contains 55–60 questions to be completed in 75 minutes. Cisco does not publish specific exam passing scores; however, in general you must get a score of about 75% to pass this exam. As was

stated before, check the Cisco website for more information on the specifics before you take your exam.

Many questions on the exam have answer choices that at first glance look identical—especially the syntax questions! Remember to read through the choices carefully, because close 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 the 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.

The CCNP Switching 640-604 exam can include the following test formats:

- Multiple-choice single answer
- Multiple-choice multiple answer
- Drag-and-drop
- Fill-in-the-blank
- Router simulations

In addition to multiple choice and fill-in response questions, Cisco Career Certifications exams may include performance simulation exam items.

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.
- 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 double-check 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.

How to Contact the Author

You can reach Todd Lammle through GlobalNet Training Solutions, Inc. (`www.globalnettraining.com`), his training and systems integration company in Dallas, Texas—or through his software company (`www.routersim.com`) in Denver, Colorado, which creates both Cisco and Microsoft software simulation programs.

You can e-mail Eric Quinn at `halthron@yahoo.com`.

Assessment Test

1. Transparent bridging uses which protocol to stop network loops on layer 2 switched networks?

   A. IP routing

   B. STP

   C. VSTP

   D. UplinkFast Bridging

2. Choose the three components that make MLS implementation possible. (Choose all that apply.)

   A. MLS-CP

   B. MLSP

   C. MLS-SE

   D. MLS-RP

3. Why would you configure VTP version 2 on your network? (Choose all that apply.)

   A. You need to support Token Ring VLANs.

   B. You want to correct TLV errors.

   C. You want to forward VTP domain messages without the switches checking the version.

   D. You have all Cisco switches.

4. An interface has been configured to use PIM sparse-dense mode. Which of the following criteria force the interface to operate in dense mode? (Choose all that apply.)

   A. DVMRP neighbors that are directly connected.

   B. Non-pruned PIM neighbors.

   C. Join request received by a host.

   D. The interface is connected to a Catalyst 5000 series switch.

5. Which of the following is the proper syntax for enabling IP multicast on a router?

   A. `multicast ip routing`

   B. `ip-multicast routing`

   C. `ip multicast-routing`

   D. `ip mroute cache`

6. Which of the following are true regarding the blocking state of an STP switch port? (Choose all that apply.)

   A. Blocking ports do not forward any frames.

   B. Blocking ports listen for BPDUs.

   C. Blocking ports forward all frames.

   D. Blocking ports do not listen for BPDUs.

7. Choose the correct definition of an XTAG.

   A. A value assigned to each packet to assign it to an MLS flow

   B. A value assigned by the router to each MLS-SE in the layer 2 network

   C. A value assigned by each MLS-SE for each MLS-RP in the layer 2 network

   D. A value assigned by the NFFC or PFC to identify each flow

8. What Cisco Catalyst switches provide distribution layer functions? (Choose all that apply.)

   A. 1900

   B. 2926G

   C. 5000

   D. 6000

   E. 8500

9. What is the difference between a bridge and a layer 2 switch? (Choose all that apply.)

   A. Switches are software based.

   B. Bridges are hardware based.

   C. Switches are hardware based.

   D. Bridges are software based.

10. What would you type at a 1900 console prompt to see the transmit and receive statistics of VTP?

    A. `show vtp stat`

    B. `show stat`

    C. `show vtp domain`

    D. `show interface e0/9`

11. If you wanted to configure VLAN 6 on an internal route processor with an IP address of 10.1.1.1/24, which of the following commands would you use?

    A. `set vlan6 ip address 10.1.1.1 255.255.255.0`

    B. `configure terminal, vlan6 ip address 10.1.1.1 255.255.255.0`

    C. `configure terminal, interface vlan 6, ip address 10.1.1.1 255.255.255.0`

    D. `set interface vlan6, ip address 10.1.1.1 255.255.255.0`

12. Which of the following is the correct multicast MAC address if it is mapped from the multicast IP address 224.127.45.254?

    A. 01-00-5e-7f-2d-fe

    B. 01-00-5e-7e-2d-fe

    C. 00-00-e0-7f-2d-fe

    D. 01-00-e0-7f-2d-fe

13. Which of the following describes local VLAN services?

A. Users do not cross layer 3 devices, and the network services are in the same broadcast domain as the users. This type of traffic never crosses the backbone.

B. Users cross the backbone to log in to servers for file and print services.

C. Users would have to cross a layer 3 device to communicate with the network services, but they might not have to cross the backbone.

D. Layer 3 switches or routers are required in this scenario because the services must be close to the core and would probably be based in their own subnet.

14. What type of router uses session 15?

A. An external router using SNMP

B. An external router using SMTP

C. A daughter card on a supervisor module

D. A PFC on a 6500

15. Which of the following protocols is used to determine the locations of data loops and the election of a root bridge?

A. STP

B. VSTP

C. BPDU

D. BackboneFast

16. What is the syntax for configuring a router to be an RP Mapping Agent?

A. `ip multicast mapping-agent` *`scope`*

B. `ip pim send-rp-discovery` *`scope`*

C. `ip rp-mapping-agent` *`scope`*

D. `ip auto-rp mapping-agent` *`scope`*

17. Which of the following is an IEEE standard for frame tagging?

A. ISL

B. 802.3z

C. 802.1q

D. 802.3u

18. How do you set the enable mode password on a 5000 series switch?

A. `set sco password todd`

B. `set user password todd`

C. `set password todd`

D. `set enablepass`

E. `set enable password todd`

19. Which of the following is true?

A. You are required to assign a password to an RSM interface CLI.

B. You must perform a `no shutdown` command for every subinterface on an external route processor.

C. You must perform a `no shutdown` command for every VLAN on an internal route processor.

D. You can use a 2500 series router for ISL routing.

20. Which version of IGMP is the Cisco proprietary version?

A. IGMPv1

B. IGMPv2

C. CGMP

D. None

21. If you wanted to set a default route on a 5000 series switch, which of the following commands would you use?

A. `route add 0.0.0.0 0.0.0.0 172.16.1.1`

B. `set route default 0.0.0.0 172.16.1.1`

C. `set route default 172.16.1.1`

D. `set route 0.0.0.0 0.0.0.0 172.16.1.1`

22. Which of the following is a type of access policy that you can apply at the core layer?

A. Port security

B. Access lists

C. High reliability

D. Physical security

23. Which of the following defines remote VLAN services?

A. Users do not cross layer 3 devices, and the network services are in the same broadcast domain as the users. This type of traffic never crosses the backbone.

B. Users cross layer 2 devices only to find the network file and print services needed to perform their job function.

C. Users would have to cross a layer 3 device to communicate with the network services, but they might not have to cross the backbone.

D. Layer 3 switches or routers are required in this scenario because the services must be close to the core and would probably be based in their own subnet.

24. If you want to clear the VTP prune eligibility from all VLANs except VLAN 2, what command would you type in on a set-based switch?

A. `delete pruneeligible 3, 4, 5, etc`

B. `delete vtp pruneeligible 1, 3-1005`

C. `clear vtp pruneeligible 3-1005`

D. `clear vtp pruneeligible 1, 3-1005`

25. Which of the following devices is responsible for rewriting a layer 3 switched packet? (Choose all that apply.)

A. Multi-layer Switch Feature Card (MSFC)

B. Route Switch Module (RSM)

C. NetFlow Feature Card (NFFC)

D. Policy Feature Card (PFC)

26. When must you run IGMPv1?

A. When using Auto-RP.

B. When running DVMRP tunnels.

C. When hosts use IGMPv1.

D. You never have to use IGMPv1.

27. If you wanted to have a 5000 switch supervisor module in a VLAN other than the default of VLAN 1, what should you type?

A. `set interface slo 3`

B. `set interface sc0 2`

C. `set sco2 3`

D. `set vlan management 2`

28. What does a switch do with a multicast frame received on an interface?

A. Forwards the switch to the first available link

B. Drops the frame

C. Floods the network with the frame looking for the device

D. Sends back a message to the originating station asking for a name resolution

29. Choose the effects of configuring PIM SM on an interface.

A. Enabling IGMP

B. Enabling CGMP

C. Enabling IGMP and CGMP

D. Enabling Auto-RP

30. Choose the three basic steps in establishing a shortcut cache (MLS cache) entry. (Choose all that apply.)

A. Identification of the MLS-RP

B. Identification of the MLS-SE

C. Identification of a candidate packet

D. Identification of an enable packet

E. Identification of ISL trunking

31. What is the default VLAN on all switches?

A. VLAN 64

B. VLAN 1005

C. VLAN 1

D. VLAN 10

32. Which of the following is a type of policy that you can apply at the distribution layer? (Choose all that apply.)

A. Port security

B. Access lists

C. Distribute lists

D. Physical security

33. Which of the following is true regarding the Cisco 2926G switch?

A. Provides an enterprise solution for up to 96 users and up to 36 Gigabit Ethernet ports for servers

B. Supports a large number of connections and also supports an internal route processor module

C. Only uses an external router processor such as a 3600 or 7200 series router

D. Also recommended for use at the core layer

34. How many bits are available for mapping a layer 3 IP address to a multicast MAC address?

A. 16

B. 32

C. 23

D. 24

35. What command will set the enable mode password on a 1900 switch?

A. `1900EN(config)#enable password level 1 todd`

B. `1900EN(config)#enable password level 15 todd`

C. `1900EN#set enable password todd`

D. `1900EN(Config)#enable password todd`

36. What does the PVST protocol provide?

A. One instance of spanning tree per network

B. One instance of STP per VLAN

C. Port Aggregation Protocol support

D. Routing between VLANs

37. On which of the following cards is the MLS cache stored? (Choose all that apply.)

A. MSFC

B. PFC

C. RSM

D. NFFC

38. Which of the following are examples of ways to directly connect to a switch? (Choose all that apply.)

A. Console port

B. VTY line

C. Auxiliary port

D. Telnet

39. Which of the following IP address ranges is the valid multicast address range?

A. 127.0.0.0–127.255.255.255

B. 223.0.0.1–237.255.255.255

C. 224.0.0.1–239.0.0.0

D. 224.0.0.0–239.255.255.255

40. Which of the following defines enterprise services?

A. Users do not cross layer 3 devices, and the network services are in the same broadcast domain as the users. This type of traffic never crosses the backbone.

B. No layer 3 switches or devices are used in this network.

C. The users would have to cross a layer 3 device to communicate with the network services, but they might not have to cross the backbone.

D. Layer 3 switches or routers are required in this scenario because the services must be close to the core and would probably be based in their own subnet.

41. What is the default LAN switch type for the 1900 switch?

A. FastForward

B. Cut-through

C. LANSwitch type 1

D. FragmentFree

E. Store-and-forward

42. Which of the following is true regarding ICMPv2?

A. It can be used only on Ethernet LANs.

B. It is used to update multicast caches on workstations.

C. ICMP works only with Unix devices.

D. It enables clients to inform routers of their intent to leave.

43. What type of cable must you use to connect between two switch uplink ports?

    A. Straight

    B. Rolled

    C. Crossover

    D. Fiber

44. Which LAN switch methods have a fixed latency time? (Choose all that apply.)

    A. Cut-through

    B. Store-and-forward

    C. FragmentCheck

    D. FragmentFree

45. Which of the following is true regarding an RSFC card? (Choose all that apply.)

    A. Passwords are required to be set on the RSFC card.

    B. The RSFC takes one slot in a 5000 series chassis.

    C. The RSFC is a daughter card for the Supervisor Engine II G and Supervisor III G cards.

    D. The RSFC is a fully functioning router running the Cisco IOS.

46. If you have an RSM as module 3, how would you connect from the Catalyst 5000 prompt?

    A. `connect 3`

    B. `telnet 3`

    C. `session 3`

    D. `module 3`

47. How do you set the usermode password on a 5000 switch?

A. `set sco password todd`

B. `set user password todd`

C. `set password`

D. `set enable password todd`

48. What are the three problems that are associated with layer 2 switching and are solved by STP?

A. Address learning

B. Routing

C. Forwarding and filtering frames

D. Forwarding and filtering packets

E. Loop avoidance

F. IP addressing

49. When will a switch update its VTP database?

A. Every 60 seconds.

B. When a switch receives an advertisement that has a higher revision number, the switch will overwrite the database in NVRAM with the new database being advertised.

C. When a switch broadcasts an advertisement that has a lower revision number, the switch will overwrite the database in NVRAM with the new database being advertised.

D. When a switch receives an advertisement that has the same revision number, the switch will overwrite the database in NVRAM with the new database being advertised.

50. What is the typical time that it takes a switch port to go from blocking to forwarding state?

A. 5 seconds

B. 50 seconds

C. 10 seconds

D. 100 seconds

51. Which topology scenario(s) support Multi-Layer Switching (MLS)? (Choose all that apply.)

A. Router on a stick

B. Multiple switches connected via ISL trunks with only one switch connected to a router

C. Multiple switches connected to a router

D. Multiple routers connected to one switch

52. Which of the following commands is used to view the configuration of an RSM?

A. `show vlan`

B. `show config`

C. `show run`

D. `show port` *`slot/type`*

53. To configure a root bridge on a set-based switch, what command would be used?

A. `set spanning tree backup`

B. `set spantree secondary`

C. `set spantree root`

D. `spanning tree 2`

54. What are the two types of distribution trees?

A. RP trees

B. Multicast trees

C. Shared root trees

D. Source root trees

55. When setting the VLAN port priority, what are the available values you can use?

A. 0–63

B. 1–64

C. 0–255

D. 1–1005

56. What are valid ways that an administrator can configure VLAN memberships? (Choose all that apply.)

A. DHCP server

B. Static

C. Dynamic

D. VTP database

57. What is the distance you can run an MMF, 62.5-micron Gigabit Ethernet cable?

A. 400 meters

B. 25 meters

C. 260 meters

D. 3 kilometers

E. 10 kilometers

58. You have just been hired as a consultant for a small company that has users distributed across many floors in the same building. Servers for the company are all located on the first floor, and 30 users access them from various parts of the building. What switch would you install for the access layer connection?

A. 1900 series

B. 5000 series

C. 6000 series

D. 8000 series

59. Which of the following commands will display XTAG information on a switch?

A. `show mls entry`

B. `show mls statistics`

C. `show mls`

D. `show mls rp ip`

60. Which component or device performs the MLS frame rewrite? (Choose all that apply.)

A. PFC

B. MSFC

C. RSM

D. NFFC

Answers to Assessment Test

1. B. The Spanning Tree Protocol was designed to help stop network loops that can happen with transparent bridge networks running redundant links. See Chapter 5 for more information.
2. B, C, D. MLSP is the routing protocol for MLS, MLS-SE is the switching engine, and MLS-RP is the route processor. MLS-CP is an invalid answer. See Chapter 7 for more information.
3. A, B, C. If you have Token Ring, you would want to run VTP version 2. For more information, see Chapter 3.
4. A, B. Join requests cause the interface to operate in PIM sparse mode. If a Catalyst is connected, the interface must be configured to use CGMP. See Chapter 8 for more information.
5. C. The first two are not valid commands. `ip mroute cache` allows the interface to use fast switching or other types of interface switching for multicast traffic. See Chapter 9 for more information.
6. A, B. When a port is in blocking state, no frames are forwarded. This is used to stop network loops. However, the blocked port will listen for BPDUs received on the port. For more information on STP, see Chapter 4.
7. C. XTAG values are locally significant values that are assigned by the Multi-layer Switching Switch Engine (MLS-SE) to keep track of the Multi-layer Switching Route Processors (MLS-RPs) in the network. See Chapter 7 for more information.
8. B, C, D. The 2926G, 5000 series, and 6000 series were specifically designed to provide distribution layer functions. See Chapter 1 for more information on the distribution layer and the Cisco switches designed to run at the distribution layer.
9. C, D. Bridges are considered software based and switches are considered hardware based. See Chapter 4 for more information.
10. A. The command `show vtp stat` is used to see VTP updates being sent and received on your switch. For more information, see Chapter 3.

11. C. The command `interface vlan #` is used to create a VLAN interface. The IP address of the interface is then configured with the `ip address` command. See Chapter 6 for more information on internal and external route processors.

12. A. 23 bits allows us to use the 127 value in the second octet. The MAC prefix is always 01-00-5e. See Chapter 8 for more information.

13. A. Local VLAN services are network services that are located in the same VLAN as the user trying to access them. Packets will not pass through a layer 3 device. See Chapter 1 for more information.

14. C. The session command is used on a modular switch to access an internal router. The session number will be greater than the available slot numbers if the card is mounted on the Supervisor card.

15. C. Bridge Protocol Data Units are sent out every two seconds by default and provide information to switches throughout the internetwork. This includes finding redundant links, electing the root bridge, monitoring the links in the spanning tree, and notifying other switches in the network about link failures. See Chapter 5 for more information.

16. B. The router uses PIM to distribute RP information to multicast routers. The other syntax options are not valid. See Chapter 9 for more information.

17. C. Cisco's propriety version of frame tagging is ISL. However, if you do not have all Cisco switches, the IEEE 802.1q version would be used. For more information, see Chapter 3.

18. D. The command `set enablepass` will set the password on a 5000 series switch. See Chapter 2 for more information on configuring the 5000 series of switches.

19. C. An external route processor configured with subinterfaces does not need a `shutdown` performed on each subinterface, only the main interface. However, an internal route processor must have a `no shutdown` command performed under every VLAN interface. See Chapter 6 for more information on internal and external route processors.

20. D. CGMP is not a version of IGMP but was developed by Cisco Systems. See Chapter 8 for more information.

21. C. The command `set route default` and the command `set route 0.0.0.0` are the same command and can be used to set a default gateway on a 5000 series switch. See Chapter 6 for more information on configuring a 5000 series switch.

22. C. A high level of reliability, including redundancy, is encouraged at the core layer. See Chapter 1 for more information on policies.

23. C. To communicate to another VLAN, packets must cross a layer 3 device. See Chapter 1 for more information on local and remote VLAN services.

24. C. You cannot turn off `pruneeligible` for VLAN 1, which makes the third answer the only correct one. For more information, see Chapter 3.

25. C, D. The Multi-layer Switch Feature Card (MSFC) is a Route Processor (RP) and does not perform the rewrites for MLS packets. The same goes for the Route Switch Module (RSM). The NetFlow Feature Card (NFFC) and the Policy Feature Card (PFC) are responsible for the MLS packet rewrite. See Chapter 7 for more information.

26. C. Use IGMPv1 when the clients subscribing are using IGMPv1.

27. B. The set command `set interface sc0` *`vlan#`* changes the default VLAN for the supervisor module to the specified VLAN. See Chapter 2 for more information.

28. C. The switch will flood the network with the frame looking for the device. For more information on LAN switching, see Chapter 4.

29. A. Adding the PIM configuration to the interface enables only Internet Group Management Protocol (IGMP) in addition to PIM. Auto-RP and Cisco Group Management Protocol (CGMP) must be configured separately. See Chapter 9 for more information.

30. A, C, D. The Multi-layer Switching Switch Engine (MLS-SE) needs to know three things to create an entry: the Multi-layer Switching Route Processor (MLS-RP), a candidate packet, and an enable packet. See Chapter 7 for more information.

31. C. VLAN 1 is a default VLAN and used for management by default. See Chapter 5 for more information.

32. B, C. Access lists can be configured at the distribution layer for packet filtering purposes, and a distribute list controls how routing traffic is forwarded. See Chapter 1 for more information on policies at each layer.

33. C. The 2926G is not capable of handling an internal route processor. See Chapter 1 for more information regarding the 2926G switch.

34. C. Due to the prefix length and the high order bit already in use in the multicast MAC address, only 23 bits are left for mapping. See Chapter 8 for more information.

35. B. The command to set the enable password on a 1900 switch is `enable password level 15 password`. See Chapter 2 for more information.

36. B. The Cisco proprietary protocol Per-VLAN Spanning Tree (PVST) uses a separate instance of spanning tree for each and every VLAN. See Chapter 5 for more information.

37. B, D. The RSM and MSFC are route processors that do not store MLS caches. See Chapter 7 for more information.

38. A, C. Connecting to the console port or auxiliary port is out-of-band management because you are not accessing the equipment from within the network. Instead, you are connecting directly to the switch. See Chapter 2 for more information on basic switch setup.

39. D. The first answer is a Class B range of addresses. 223.0.0.1 does not have the proper mask. The third answer is within the valid range, but it is not all-inclusive. See Chapter 8 for more information.

40. D. Enterprise services are defined as services that are provided to all users on the internetwork. See Chapter 1 for more information.

41. D. The 1900 defaults to FragmentFree, but it can be changed to store-and-forward. For more information on LAN switch types, see Chapter 4.

42. D. Internet Control Message Protocol (ICMP) version 2 is used by ICMP routers to enable clients to send messages, telling the router that they no longer want to subscribe to the multicast stream. See Chapter 8 for more information regarding ICMP.

43. C. A crossover cable is used to connect switches to switches and hubs to hubs. See Chapter 2 for more information on the Catalyst 5000 configuration.

44. A, D. Cut-through and FragmentFree always read only a fixed amount of a frame. For more information on LAN switch types, see Chapter 4.

45. C, D. The Route Switch Feature Card (RSFC) is a daughter card used on a Supervisor II and III card to provide a fully functioning router IOS. See Chapter 6 for more information on internal and external route processors.

46. C. The session command is used to create a session from the switch CLI to the RSM CLI. See Chapter 6 for more information.

47. C. The set command `set password` sets the usermode password on a 5000 series switch. See Chapter 2 for more information on configuring the 5000 series of switches.

48. A, C, E. Layer 2 features include address learning, forwarding and filtering of the network, and loop avoidance. See Chapter 4 for more information.

49. B. Only when a VTP update is received with a higher data VTP revision number will a switch update its VTP database. For more information, see Chapter 3.

50. B. Fifty seconds is the default time for changing from blocking to forwarding state. This is to allow enough time for all switches to update their STP database. For more information on STP, see Chapter 4.

51. A, B, D. The router on a stick is the typical and simplest topology for Multi-Layer Switching (MLS). Multiple switches connected to each other can use MLS if only one switch is connected to the router. Multiple routers can be connected to one switch as long as each router has only one link to the switch. See Chapter 7 for more information.

52. C. The RSM commands are the same for any Cisco IOS router, and the `show running-config` is used to view the current configuration. See Chapter 6 for more information on internal and external route processors.

53. C. The `set spantree root` command enables you to configure a root bridge. See Chapter 5 for more information.

54. C, D. Multicast trees don't exist. Some protocols that are based in shared root trees can create RPTs (or RP trees) that are parallel to the shortest path tree, but this is a flavor of shared root tree distribution.

55. A. A priority from 0 to 63 can be set for each VLAN.

56. B, C. Static VLANs are set port by port on each interface or port. Dynamic VLANs can be assigned to devices via a server.

57. C. The maximum distance a Multi-Mode Fiber, 62.5-micron Gigabit Ethernet link can run is 260 meters.

58. A. Because the question involves a small company and no growth was specified, a couple of 1900s would be the most cost-effective solution.

59. C. The `show mls rp ip` command is used on routers and doesn't provide XTAG information. Neither do any of the other switch commands.

60. A, D. MSFC and RSMs are layer 3 devices that are used in Catalyst switches. Pattern matching and frame rewrites are done by the NFFC and PFC.

Chapter

1

The Campus Network

THE CCNP EXAM TOPICS COVERED IN THIS CHAPTER INCLUDE THE FOLLOWING:

- ✓ **Identify the correct Cisco Systems product solution given a set of network switching requirements**
- ✓ **Provide physical connectivity between two devices within a switch block**
- ✓ **Provide connectivity from an end user station to an access layer device**
- ✓ **Provide connectivity between two network devices**

A campus network is a building or group of buildings that connects to one network, called an enterprise network. Typically, one company owns the entire network, including the wiring between buildings. This local area network (LAN) typically uses Ethernet, Token Ring, Fiber Distributed Data Interface (FDDI), or Asynchronous Transfer Mode (ATM) technologies.

The main challenge for network administrators is to make the campus network run efficiently and effectively. To do this, they must understand current campus networks as well as the new emerging campus networks. Therefore, in this chapter, you will learn about current and future requirements of campus internetworks (the connecting of several campuses). We'll explain the limitations of traditional campus networks as well as the benefits of the emerging campus designs. You will learn how to choose from among the new generation of Cisco switches to maximize the performance of your networks. Understanding how to design for the emerging campus networks is not only critical to your success on the Switching exam, it's also critical for implementing production networks.

As part of the instruction in network design, we'll discuss the specifics of technologies, including how to implement Ethernet and the differences between layer 2, layer 3, and layer 4 switching technologies. In particular, you will learn how to implement FastEthernet, Gigabit Ethernet, Fast EtherChannel, and Multi-Layer Switching (MLS) in the emerging campus designs. This will help you learn how to design, implement, and maintain an efficient and effective internetwork.

Finally, you will learn about the Cisco hierarchical model, which is covered in all the Cisco courses. In particular, you will learn which Catalyst switches can—and should—be implemented at each layer of the Cisco model. And you will learn how to design networks based on switch and core blocks.

This chapter, then, will provide you with a thorough overview of campus network design (past, present, and future) and teach you how, as a network administrator, to choose the most appropriate technology for a particular network's needs. This will enable you to configure and design your network now, with the future in mind.

Understanding Campus Internetworks

It doesn't seem that terribly long ago that the mainframe ruled the world and the PC was used simply to placate some users. However, in their arrogance, mainframe administrators never really took the PC seriously, and like rock 'n' roll naysayers, they said it would never last. Maybe they were right after all—at least in a way. In many cases, server farms have replaced distributed servers in the field.

In the last 15 years, we have seen operators and managers of the mainframe either looking for other work or taking huge pay cuts. Their elitism exacerbated the slap in the face when people with no previous computer experience were suddenly making twice their salary after passing a few key certification exams.

Mainframes were not necessarily discarded; they just became huge storage areas for data and databases. The NetWare or NT server took over as a file/print server and soon started running most other programs and applications as well.

The last 20 years have witnessed the birth of the LAN and the growth of WANs (wide area networks) and the Internet. So where are networks headed in the twenty-first century? Are we still going to see file and print servers at all branch locations? Are all workstations just going to connect to the Internet with ISPs to separate the data, voice, and other multimedia applications?

Looking Back at Traditional Campus Networks

In the 1990s, the traditional campus network started as one LAN and grew and grew until segmentation needed to take place just to keep the network up and running. In this era of rapid expansion, response time was secondary to just making sure the network was functioning.

And by looking at the technology, you can see why keeping the network running was such a challenge. Typical campus networks ran on 10BaseT or 10Base2 (thinnet). As a result, the network was one large collision domain—not to mention even one large broadcast domain. Despite these limitations, Ethernet was used because it was scalable, effective, and somewhat inexpensive compared to other options. ARCnet was used in some networks, but Ethernet and ARCnet are not compatible, and the networks became two separate entities. ARCnet soon became history.

Because a campus network can easily span many buildings, bridges were used to connect the buildings; this broke up the collision domains, but the network was still one large broadcast domain. More and more users were attached to the hubs used in the network, and soon the performance of the network was considered extremely slow.

Performance Problems and Solutions

Availability and performance are the major problems with traditional campus networks. Bandwidth helps compound these problems. The three performance problems in traditional campus networks included collisions, bandwidth, and broadcasts and multicasts.

Collisions

A campus network typically started as one large collision domain, so all devices could see and also collide with each other. If a host had to broadcast, then all other devices had to listen, even though they themselves were trying to transmit. And if a device were to jabber (malfunction), it could bring the entire network down.

Because routers didn't really become cost-effective until the late 1980s, bridges were used to break up collision domains. That was an improvement, but the network was still one large broadcast domain and the broadcast problems still existed. Bridges also solved distance-limitation problems because they usually had repeater functions built into the electronics and/or they could break up the physical segment.

Bandwidth

The *bandwidth* of a segment is measured by the amount of data that can be transmitted at any given time. Think of bandwidth as a water hose; the

amount of water that can go through the hose depends on two elements:

- Pressure
- Distance

The pressure is the current, and the bandwidth is the size of the hose. If you have a hose that is only 1/4 inch in diameter, you won't get much water through it regardless of the current or the size of the pump on the transmitting end.

Another issue is distance. The longer the hose, the more the water pressure drops. You can put a repeater in the middle of the hose and re-amplify the pressure of the line, which would help, but you need to understand that all lines (and hoses) have degradation of the signal, which means that the pressure drops off the farther the signal goes down the line. For the remote end to understand digital signaling, the pressure must stay at a minimum value. If it drops below this minimum value, the remote end will not be able to receive the data. In other words, the far end of the hose would just drip water instead of flow. You can't water your crops with drips of water; you need a constant water flow.

The solution to bandwidth issues is maintaining your distance limitations and designing your network with proper segmentation of switches and routers. Congestion on a segment happens when too many devices are trying to use the same bandwidth. By properly segmenting the network, you can eliminate some of the bandwidth issues. You never will have enough bandwidth for your users; you'll just have to accept that fact. However, you can always make it better.

Broadcasts and Multicasts

Remember that all protocols have broadcasts built in as a feature, but some protocols can really cause problems if not configured correctly. Some protocols that, by default, can cause problems if not correctly implemented are Internet Protocol (IP), Address Resolution Protocol (ARP), Network Basic Input Output System (NetBIOS), Internetwork Packet Exchange (IPX), Service Advertising Protocol (SAP), and Routing Information Protocol (RIP). However, remember that there are features built into the Cisco router Internetworking Operating System (IOS) that, if correctly designed and implemented, can alleviate these problems. Packet filtering, queuing, and

choosing the correct routing protocols are some examples of how Cisco routers can eliminate some broadcast problems.

Multicast traffic can also cause problems if not configured correctly. Multicasts are broadcasts that are destined for a specific or defined group of users. If you have large multicast groups or a bandwidth-intensive application such as Cisco's IPTV application, multicast traffic can consume most of the network bandwidth and resources.

To solve broadcast issues, create network segmentation with bridges, routers, and switches. However, understand that you'll move the bottleneck to the routers, which break up the broadcast domains. Routers process each packet that is transmitted on the network, which can cause the bottleneck if an enormous amount of traffic is generated.

Virtual LANs (VLANs) are a solution as well, but VLANs are just broadcast domains with boundaries created by routers. A VLAN is a group of devices on different network segments defined as a broadcast domain by the network administrator. The benefit of VLANs is that physical location is no longer a factor for determining the port into which you would plug a device into the network. You can plug a device into any switch port, and the network administrator gives that port a VLAN assignment. Remember that routers or layer 3 switches must be used for different VLANs to communicate.

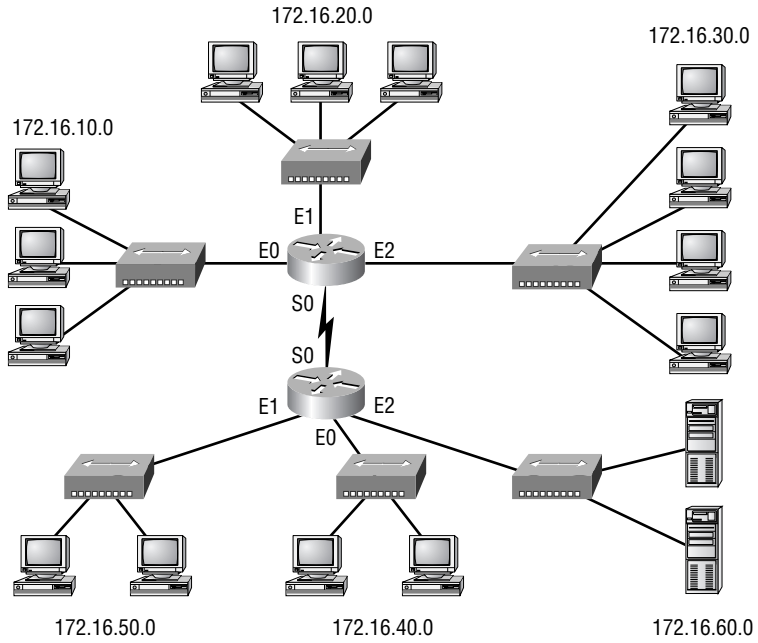
The 80/20 Rule

The traditional campus network placed users and groups in the same physical location. If a new salesperson was hired, they had to sit in the same physical location as the other sales personnel and be connected to the same physical network segment in order to share network resources. Any deviation from this caused major headaches for the network administrators.

The rule that needed to be followed in this type of network was called the *80/20 rule* because 80 percent of the users' traffic was supposed to remain on the local network segment and only 20 percent or less was supposed to cross the routers or bridges to the other network segments. If more than 20 percent of the traffic crossed the network segmentation devices, performance issues arose. Figure 1.1 shows a traditional 80/20 network.

Because network administrators are responsible for network design and implementation, they improved network performance in the 80/20 network by making sure all the network resources for the users were contained within their own network segment. The resources included network servers, printers, shared directories, software programs, and applications.

FIGURE 1.1 A traditional 80/20 network



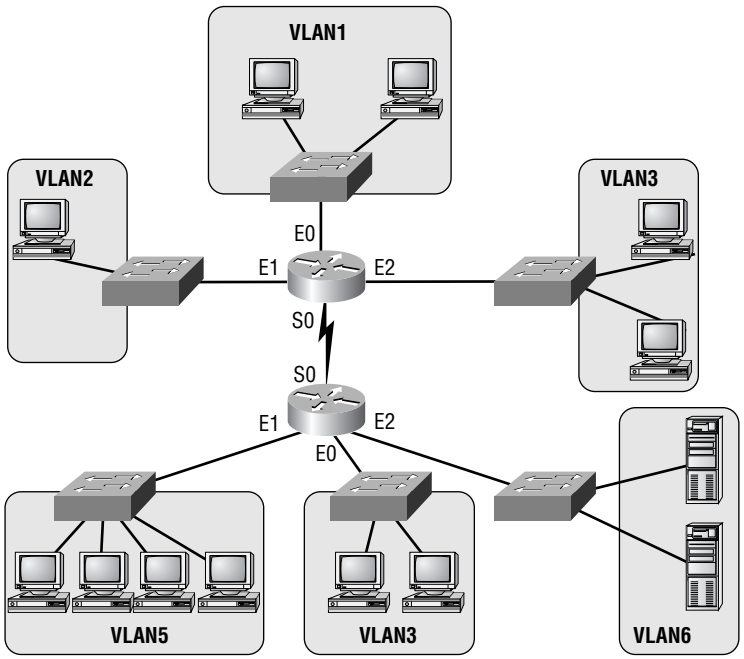
The New 20/80 Rule

With new Web-based applications and computing, any PC can be a subscriber or publisher at any time. Also, because businesses are pulling servers from remote locations and creating server farms (sounds like a mainframe, doesn't it?) to centralize network services for security, reduced cost, and administration, the old 80/20 rule is obsolete and could not possibly work in this environment. All traffic must now traverse the campus backbone, which means we now have a *20/80 rule* in effect. Twenty percent of what the user performs on the network is local, whereas up to 80 percent crosses the network segmentation points to get to network services. Figure 1.2 shows the new 20/80 network.

The problem with the 20/80 rule is not the network wiring and topology as much as it is the routers themselves. They must be able to handle an enormous number of packets quickly and efficiently at wire speed. This is probably where we should be talking about how great Cisco routers are and how our

networks would be nothing without them. We'll get to that later in this chapter—trust us.

FIGURE 1.2 A 20/80 network

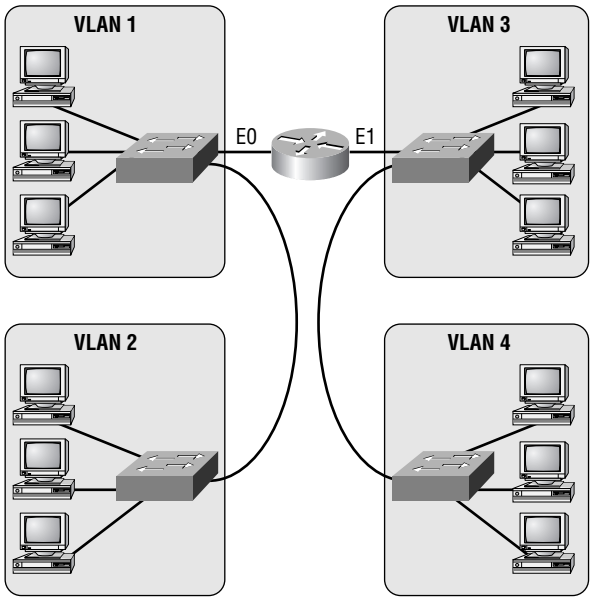


Virtual LANs

With this new 20/80 rule, more and more users need to cross broadcast domains (VLANs), and this puts the burden on routing, or layer 3 switching. By using VLANs within the new campus model, you can control traffic patterns and control user access easier than in the traditional campus network. Virtual LANs break up broadcast domains by using either a router or a switch that can perform layer 3 functions. Figure 1.3 shows how VLANs are created and might look in an internetwork.

Chapter 3, "VLANs," includes detailed information about VLANs and how to configure them in an internetwork. It is imperative that you understand VLANs because the traditional way of building the campus network is being redesigned and VLANs are a large factor in building the new campus model.

FIGURE 1.3 VLANs break up broadcast domains in a switched internetwork.



Introducing the New Campus Model

The changes in customer network requirements—in combination with the problems with collision, bandwidth, and broadcasts—have necessitated a new network campus design. Higher user demands and complex applications force the network designers to think more about traffic patterns instead of solving a typical isolated department issue. We can no longer just think about creating subnets and putting different departments into each subnet. We need to create a network that makes everyone capable of reaching all network services easily. Server farms, where all enterprise servers are located in one physical location, really take a toll on the existing network infrastructure and make the way we used to design networks obsolete. We must pay attention to traffic patterns and how to solve bandwidth issues. This can be accomplished with higher-end routing and switching techniques.

Because of the new bandwidth-intensive applications, video and audio, to the desktop, as well as more and more work being performed on the Internet, the new campus model must be able to provide the following:

Fast convergence When a network change takes place, the network must be able to adapt very quickly to new changes and keep data moving quickly.

Deterministic paths Users must be able to gain access to a certain area of the network without fail.

Deterministic failover The network design must have provisions that make sure the network stays up and running even if a link fails.

Scalable size and throughput As users and new devices are added to the network, the network infrastructure must be able to handle the new increase in traffic.

Centralized applications Enterprise applications accessed by all users must be available to support all users on the internetwork.

The new 20/80 rule Instead of 80 percent of the users' traffic staying on the local network, 80 percent of the traffic will now cross the backbone and only 20 percent will stay on the local network.

Multiprotocol support Campus networks must support multiple protocols, both routed and routing protocols. Routed protocols are used to send user data through the internetwork (for example, IP or IPX). Routing protocols are used to send network updates between routers, which will in turn update their routing tables. Examples of routing protocols include RIP, Enhanced Interior Gateway Routing Protocol (EIGRP), and Open Shortest Path First (OSPF).

Multicasting Multicasting is sending a broadcast to a defined subnet or group of users. Users can be placed in multicast groups, for example, for videoconferencing.

Network Services

The new campus model provides remote services quickly and easily to all users. The users have no idea where the resources are located in the internetwork, nor should they care. There are three types of network services, which are created and defined by the administrator and should appear to the users as local services:

- Local services

- Remote services
- Enterprise services

Local Services

Local services are network services that are located on the same subnet or network as the users accessing them. Users do not cross layer 3 devices, and the network services are in the same broadcast domain as the users. This type of traffic never crosses the backbone.

Remote Services

Remote services are close to users but not on the same network or subnet as the users. The users would have to cross a layer 3 device to communicate with the network services. However, they might not have to cross the backbone.

Enterprise Services

Enterprise services are defined as services that are provided to all users on the internetwork. Layer 3 switches or routers are required in this scenario because an enterprise service must be close to the core and would probably be based in its own subnet. Examples of these services include Internet access, e-mail, and possibly videoconferencing. When servers that host enterprise services are placed close to the backbone, all users would be the same distance from the servers, but all user data would have to cross the backbone to get to the services.

Using Switching Technologies

Switching technologies are crucial to the new network design. Because the prices on layer 2 switching have been dropping dramatically, it is easier to justify the cost of buying switches for your entire network. This doesn't mean that every business can afford switch ports for all users, but it does allow for a cost-effective upgrade solution when the time comes.

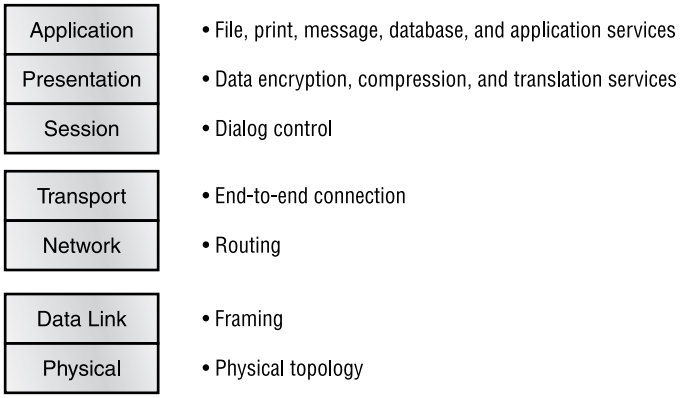
To understand switching technologies and how routers and switches work together, you must understand the Open Systems Interconnection (OSI) model. This section will give you a general overview of the OSI model and the devices that are specified at each layer.

You'll need a basic understanding of the OSI model to fully understand discussions in which it is included throughout the rest of the book. For more detailed information about the OSI model, please see *CCNA: Cisco Certified Network Associate Study Guide,* 3rd Edition by Todd Lammle (Sybex, 2002).

Open Systems Interconnection (OSI) Model

As you probably already know, the *Open Systems Interconnection (OSI) model* has seven layers, each of which specifies functions that enable data to be transmitted from host to host on an internetwork. Figure 1.4 shows the OSI model and the functions of each layer.

FIGURE 1.4 The OSI model and the layer functions



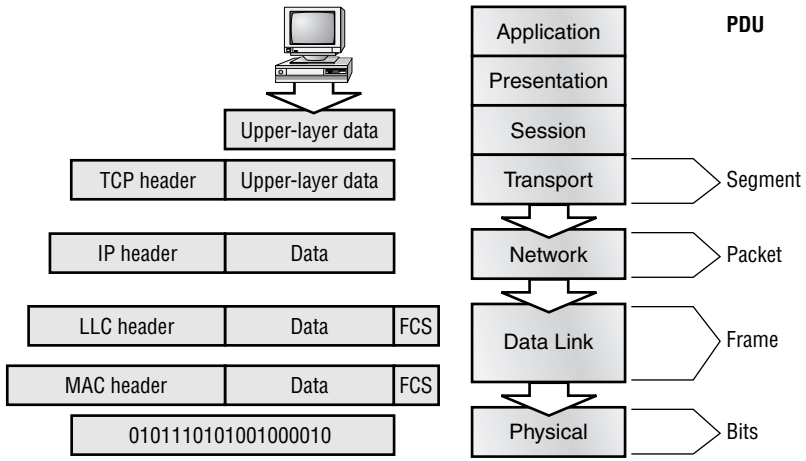
The OSI model is the cornerstone for application developers to write and create networked applications that run on an internetwork. What is important to network engineers and technicians is the encapsulation of data as it is transmitted on a network.

Data Encapsulation

Data encapsulation is the process by which the information in a protocol is wrapped, or contained, in the data section of another protocol. In the OSI reference model, each layer encapsulates the layer immediately above it as the data flows down the protocol stack.

The logical communication that happens at each layer of the OSI reference model doesn't involve many physical connections because the information each protocol needs to send is encapsulated in the layer of protocol information beneath it. This encapsulation produces a set of data called a packet (see Figure 1.5).

FIGURE 1.5 Data encapsulation at each layer of the OSI reference model



Looking at Figure 1.5, you can follow the data down through the OSI reference model as it's encapsulated at each layer. Cisco courses typically focus only on layers 2–4.

Each layer communicates only with its peer layer on the receiving host, and they exchange Protocol Data Units (PDUs). The PDUs are attached to the data at each layer as it traverses down the model and is read only by its peer on the receiving side. Each layer has a specific name for the PDU, as shown in Table 1.1.

TABLE 1.1 OSI Encapsulation

OSI Layer	Name of Protocol Data Units (PDUs)
Transport	Segments
Network	Packets
Data Link	Frames
Physical	Bits

Starting at the Application layer, data is converted for transmission on the network, then encapsulated in Presentation layer information. When the Presentation layer receives this information, it looks like generic data. The Presentation layer hands the data to the Session layer, which is responsible for synchronizing the session with the destination host.

The Session layer then passes this data to the Transport layer, which transports the data from the source host to the destination host in a reliable fashion. But before this happens, the Network layer adds routing information to the packet. It then passes the packet on to the Data Link layer for framing and for connection to the Physical layer. The Physical layer sends the data as 1s and 0s to the destination host. Finally, when the destination host receives the 1s and 0s, the data passes back up through the model, one layer at a time. The data is de-encapsulated at each of the OSI model's peer layers.

At a transmitting device, the data encapsulation method is as follows:

1. User information is converted to data for transmission on the network.
2. Data is converted to segments at the Transport layer, and a reliable session is possibly set up.
3. Segments are converted to packets or datagrams at the Network layer, and routing information is added to the PDU.
4. Packets or datagrams are converted to frames at the Data Link layer, and hardware addresses are used to communicate with local hosts on the network medium.
5. Frames are converted to bits, and 1s and 0s are encoded within the digital signal.

Now that you have a sense of the OSI model and how routers and switches work together, it is time to turn our attention to the specifics of each layer of switching technology.

Layer 2 Switching

Layer 2 switching is hardware based, which means it uses the *Media Access Control (MAC)* address from the host's network interface cards (NICs) to filter the network. Switches use *application-specific integrated circuits (ASICs)* to build and maintain filter tables. It is OK to think of a layer 2 switch as a multiport bridge.

Layer 2 switching provides the following:

- Hardware-based bridging (MAC)
- Wire speed
- High speed
- Low latency
- Low cost

Layer 2 switching is so efficient because there is no modification to the data packet, only to the frame encapsulation of the packet, and only when the data packet is passing through dissimilar media (such as from Ethernet to FDDI).

Use layer 2 switching for workgroup connectivity and network segmentation (breaking up collision domains). This enables you to create a flatter network design and one with more network segments than traditional 10BaseT shared networks.

Layer 2 switching has helped develop new components in the network infrastructure:

Server farms Servers are no longer distributed to physical locations because virtual LANs can be used to create broadcast domains in a switched internetwork. This means that all servers can be placed in a central location, yet a certain server can still be part of a workgroup in a remote branch, for example.

Intranets These enable organization-wide client/server communications based on a Web technology.

These new technologies are enabling more data to flow off local subnets and onto a routed network, where a router's performance can become the bottleneck.

Limitations of Layer 2 Switching

Layer 2 switches have the same limitations as bridge networks. Remember that bridges are good if you design the network by the 80/20 rule: users spend 80 percent of their time on their local segment.

Bridged networks break up collision domains, but the network is still one large broadcast domain. Similarly, layer 2 switches (bridges) cannot break up broadcast domains, which can cause performance issues and limits the size of your network. Broadcast and multicasts, along with the slow convergence of spanning tree, can cause major problems as the network grows.

Because of these problems, layer 2 switches cannot completely replace routers in the internetwork.

Routing

We want to explain how routing works and how routers work in an internetwork before discussing layer 3 switching next. Routers and layer 3 switches are similar in concept but not design. In this section, we'll discuss routers and what they provide in an internetwork today.

Routers break up collision domains like bridges do. In addition, routers also break up broadcast/multicast domains.

The benefits of routing include:

- Breakup of broadcast domains
- Multicast control
- Optimal path determination
- Traffic management
- Logical (layer 3) addressing
- Security

Routers provide optimal path determination because the router examines each and every packet that enters an interface and improves network segmentation by forwarding data packets to only a known destination network. Routers are not interested in hosts, only networks. If a router does not know about a remote network to which a packet is destined, it will just drop the packet and not forward it. Because of this packet examination, traffic management is obtained.

The Network layer of the OSI model defines a virtual—or logical—network address. Hosts and routers use these addresses to send information from host to host within an internetwork. Every network interface must have a logical address, typically an IP address.

Security can be obtained by a router reading the packet header information and reading filters defined by the network administrator (access lists).

Layer 3 Switching

The only difference between a layer 3 switch and a router is the way the administrator creates the physical implementation. Also, traditional routers

use microprocessors to make forwarding decisions, and the switch performs only hardware-based packet switching. However, some traditional routers can have other hardware functions as well in some of the higher-end models. Layer 3 switches can be placed anywhere in the network because they handle high-performance LAN traffic and can cost-effectively replace routers.

Layer 3 switching is all hardware-based packet forwarding, and all packet forwarding is handled by hardware ASICs. Layer 3 switches really are no different functionally from a traditional router and perform the same functions, which are listed here:

- Determine paths based on logical addressing
- Run layer 3 checksums (on header only)
- Use Time to Live (TTL)
- Process and respond to any option information
- Can update Simple Network Management Protocol (SNMP) managers with Management Information Base (MIB) information
- Provide security

The benefits of layer 3 switching include the following:

- Hardware-based packet forwarding
- High-performance packet switching
- High-speed scalability
- Low latency
- Lower per-port cost
- Flow accounting
- Security
- Quality of service (QoS)

Layer 4 Switching

Layer 4 switching is considered a hardware-based layer 3 switching technology that can also consider the application used (for example, Telnet or FTP). Layer 4 switching provides additional routing above layer 3 by using the port numbers found in the Transport layer header to make routing decisions.

These port numbers are found in Request for Comments (RFC) 1700 and reference the upper-layer protocol, program, or application.

Layer 4 information has been used to help make routing decisions for quite a while. For example, extended access lists can filter packets based on layer 4 port numbers. Another example is accounting information gathered by NetFlow switching in Cisco's higher-end routers.

The largest benefit of layer 4 switching is that the network administrator can configure a layer 4 switch to prioritize data traffic by application, which means a QoS can be defined for each user. For example, a number of users can be defined as a Video group and be assigned more priority, or bandwidth, based on the need for videoconferencing.

However, because users can be part of many groups and run many applications, the layer 4 switches must be able to provide a huge filter table or response time would suffer. This filter table must be much larger than any layer 2 or 3 switch. A layer 2 switch might have a filter table only as large as the number of users connected to the network, maybe even smaller if some hubs are used within the switched fabric. However, a layer 4 switch might have five or six entries for each and every device connected to the network! If the layer 4 switch does not have a filter table that includes all the information, the switch will not be able to produce wire-speed results.

Multi-Layer Switching (MLS)

Multi-layer switching combines layer 2, 3, and 4 switching technologies and provides high-speed scalability with low latency. It accomplishes this combination of high-speed scalability with low latency by using huge filter tables based on the criteria designed by the network administrator.

Multi-layer switching can move traffic at wire speed and also provide layer 3 routing, which can remove the bottleneck from the network routers. This technology is based on the concept of route once, switch many.

Multi-layer switching can make routing/switching decisions based on the following:

- MAC source/destination address in a Data Link frame
- IP source/destination address in the Network layer header
- Protocol field in the Network layer header
- Port source/destination numbers in the Transport layer header

There is no performance difference between a layer 3 and a layer 4 switch because the routing/switching is all hardware based.

MLS will be discussed in more detail in Chapter 7, "Multi-Layer Switching"

It is important that you have an understanding of the different OSI layers and what they provide before continuing on to the Cisco three-layer hierarchical model.

Understanding the Cisco Hierarchical Model

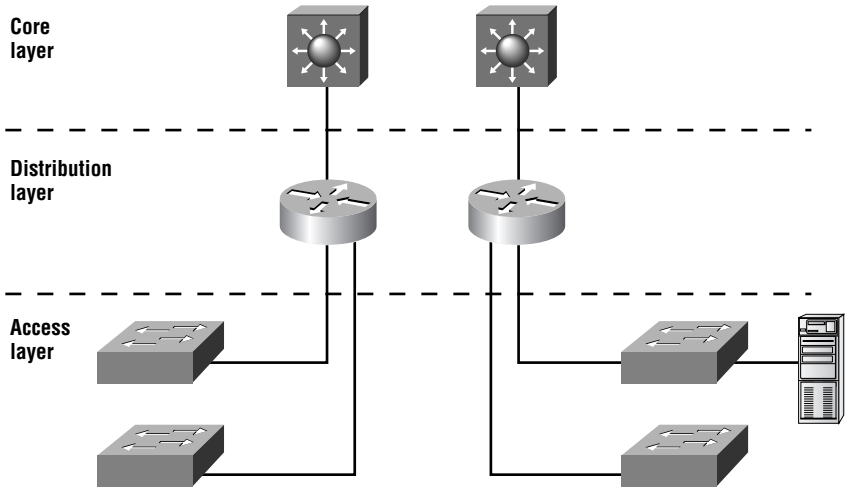
Most of us learned about hierarchy early in life. Anyone with older siblings learned what it was like to be at the bottom of the hierarchy! Regardless of where you were first exposed to hierarchy, most of us experience it in many aspects of our lives. *Hierarchy* helps us to understand where things belong, how things fit together, and what functions go where. It brings order and understandability to otherwise complex models. If you want a pay raise, hierarchy dictates that you ask your boss, not your subordinate. That is the person whose role it is to grant (or deny) your request.

Hierarchy has many of the same benefits in network design that it has in other areas. When used properly in network design, it makes networks more predictable. It helps us to define and expect at which levels of the hierarchy we should perform certain functions. You would ask your boss, not your subordinate, for a raise because of their positions in the business hierarchy. The hierarchy requires that you ask someone at a higher level than yours. Likewise, you can use tools such as access lists at certain levels in hierarchical networks and you must 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 to summarize a complex collection of details into an understandable model. Then, as specific configurations are needed, the model dictates the appropriate manner for them to be applied.

The *Cisco hierarchical model* is used to help you design a scalable, reliable, cost-effective hierarchical internetwork. Cisco defines three layers of hierarchy, as shown in Figure 1.6, each with specific functionality.

FIGURE 1.6 The Cisco hierarchical model



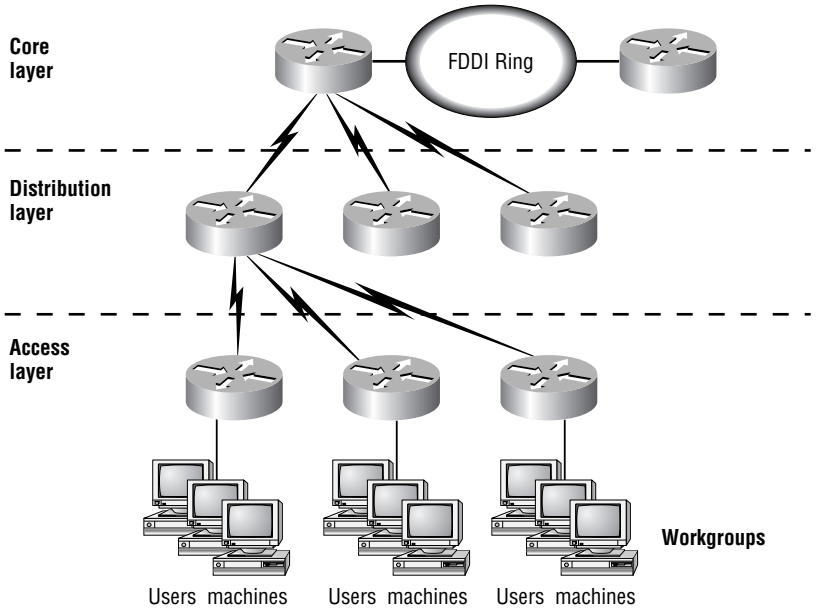
The three layers are as follows:

- Core
- Distribution
- Access

Each layer has specific responsibilities. Remember, however, that the three layers are logical and not necessarily physical. "Three layers" does not necessarily mean "three separate devices." Consider the OSI model, another logical hierarchy. The 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 you build physical implementations of hierarchical networks, you might have many devices in a single layer, or you might have a single device performing functions at two layers. The definition of the layers is logical, not physical.

Before we examine these layers and their functions, consider a common hierarchical design, as shown in Figure 1.7. The phrase "keep local traffic local" has almost become a cliché in the networking world. However, the underlying concept has merit. Hierarchical design lends itself perfectly to fulfilling this concept. Now, let's take a closer look at each of the layers.

FIGURE 1.7 A hierarchical network design



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 core layer of the network is to switch traffic as quickly as possible. The traffic transported across the core is common to a majority of users. However, remember that user data is processed at the distribution layer, and the distribution layer forwards the requests to the core, if needed.

If there is a failure in the core, *every single* user can be affected. Therefore, fault tolerance at this layer is an issue. 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 look at some design specifics to consider. Let's start with some things you know you don't want to do:

- Don't do anything to slow down traffic. This includes using access lists, routing between VLANs, and packet filtering.
- Don't support workgroup access here.

- Avoid expanding the core when the internetwork grows (that is, adding routers). If performance becomes an issue in the core, give preference to upgrades over expansion.

Now, there are a few things that you want to make sure to get done as you design the core:

- Design the core for high reliability. Consider Data Link technologies that facilitate both speed and redundancy, such as FDDI, FastEthernet (with redundant links), or even ATM.
- Design with speed in mind. The core should have very little latency.
- Select routing protocols with lower convergence times. Fast and redundant Data Link connectivity is no help if your routing tables are shot!

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 function of the distribution layer is 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 user requests are serviced (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. The core layer is then responsible for quickly transporting the request to the correct service.

The distribution layer is the place to implement policies for the network. Here, you can exercise considerable flexibility in defining network operation. Generally, the following should be done at the distribution layer:

- Implement tools such as access lists, packet filtering, and queuing.
- Implement security and network policies, including address translation and firewalls.
- Redistribute between routing protocols, including static routing.
- Route between VLANs and other workgroup support functions.
- Define broadcast and multicast domains.

Things to avoid at the distribution layer are limited to those functions that exclusively belong to one of the other layers.

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 that most users need will be available locally. Any traffic for remote services is handled by the distribution layer. The following functions should be included at this layer:

- Continued (from distribution layer) access control and policies.
- Creation of separate collision domains (segmentation).
- Workgroup connectivity to the distribution layer.
- Technologies such as dial-on-demand routing (DDR) and Ethernet switching are frequently seen in the access layer. Static routing (instead of dynamic routing protocols) is seen here as well.

As already noted, having three separate levels does not have to imply having three separate routers. It could be fewer, or it could be more. Remember that this is a *layered* approach.

Using Cisco Catalyst Products

Understanding the campus size and traffic is an important factor in network design. A large campus is defined as several or many colocated buildings, and a medium campus is one or more colocated buildings. Small campus networks have only one building.

By understanding your campus size, you can choose Cisco products that will fit your business needs and grow with your company. Cisco switches are produced to fit neatly within its three-layer model. This helps you decide which equipment to use for your network efficiently and quickly.

It should be noted that switches have two broad operating systems in use. The Catalyst Operating System (CatOS) is the traditional method and is often referred to as using set commands because when configuring, the command often begins with the word "set." Switches in this line include the 4000, 2900G, 5000/5500, and the 6000/6500.

The switches based on the IOS are called Catalyst IOS (CatIOS) switches. The interface to configure these switches resembles that of the IOS router but isn't entirely the same. Anyone familiar with configuring a router, though,

will be comfortable configuring one of these switches. The switches that use this include the 1900EN, the 2900XL, the 3500XL, and the 8500 series.

For some switches, you have a choice between the two types of operating systems. When this occurs, the CatOS is the default OS. An example of this is the 6000/6500 series.

Cisco Express Forwarding (CEF) allows for real layer 3 switches to forward traffic based on a complete layer 3 topology map. This map is shared with the ASICs at each port, enabling each port to know which port a packet should be forwarded to. Rather than forwarding based on MAC address, forwarding is done by layer 3 address. Only switches that have true layer 3 capabilities can do this type of switching. These devices include the 8500, 4006, 2948G, and 6000/6500 with PFC2.

There are two general rules when it comes to Cisco switches:

- The model number can typically be split into two sections: a base model—for example, the 2900XL, and then the number of ports it has—48. This equals the 2948XL. For slot-based switches, the second number usually refers to the number of physical slots it has. The 6509 is a nine-slot device in the 6500 family of switches.
- The lower model numbers usually cost less, and purchasing a device with more ports drives down the per-port cost.

Access Layer Switches

The access layer, as you already know, is where users gain access to the internetwork. The switches deployed at this layer must be able to handle connecting individual desktop devices to the internetwork. The switches here are usually characterized as having a large number of ports and being low cost. Most access switches don't have a lot of frills.

The Cisco solutions at the access layer include the following:

1900/2800 Provide switched 10Mbps to the desktop or to 10BaseT hubs in small to medium campus networks. They also allow for higher-speed 100Mbps connections to upstream switches and routers. They are generally recommended for under 50 users in a location.

2900XL/3500XL Provides 10/100/1000Mbps switched access for up to 50 users and gigabit speeds for servers and uplinks. Some models of the 2900XLs allow for Gigabit Ethernet, and all models of the 3500XLs support Gigabit Ethernet. There is a version of the 3500XL that provides inline power for IP telephones. The 2900XL and 3500XL are the only low-cost switches to support both ISL and 802.1q trunking. Trunking is covered in detail in Chapter 3. The later model 2950XL and 3550XL support only 802.1q.

If power for IP phones is required but a switch with inline power is not available, Cisco also has a product called the "Inline Power Patch Panel" that adds inline power to an existing Catalyst switch.

4000 Provides a 10/100/1000Mbps advanced high-performance enterprise solution for up to 96 users and up to 36 Gigabit Ethernet ports for servers. Some models also support the delivery of inline power for IP telephones.

5000/5500 Used in large campuses to provide access for more than 250 users. The Catalyst 5000 series supports 10/100/1000Mbps Ethernet switching.

Distribution Layer Switches

As discussed earlier, the primary function of the distribution layer is to provide routing, filtering, and WAN access and to determine how packets can access the core, if needed.

Distribution layer switches are the aggregation point for multiple access switches and must be capable of handling large amounts of traffic from these access layer devices. The distribution layer switches must also be able to participate in multi-layer switching (MLS) and be able to handle a route processor.

The Cisco switches that provide these functions are as follows:

2926G/2948G The 2926G is a robust switch that uses an external router processor, such as a 3600 or 7200 series router. The 2948G is a true layer 3 device, able to do layer 3 switching.

5000/5500 The most effective distribution layer switch, it can support a large number of connections and also an internal route processor module called a Route Switch Module (RSM). It can process switch up to 176KBps.

6000 The Catalyst 6000 can provide up to 384 10/100Mbps Ethernet connections, 192 100FX FastEthernet connections, or 130 Gigabit Ethernet ports. In addition to regular connections, IP telephone connections with inline power are also supported. The 6000 can be outfitted with a Multi-layer Switch Feature Card (MSFC) to provide router functionality as well as a Policy Feature Card (PFC) for layer 3 switching functionality.

Core Layer Switches

The core layer must be efficient and do nothing to slow down packets as they traverse the backbone. The following switches are recommended for use in the core:

5000/5500 The 5000 is a great distribution layer switch, and the 5500 is a great core layer switch. The Catalyst 5000 series of switches includes the 5000, 5002, 5500, 5505, and 5509. All the 5000 series switches use the same cards and modules, which makes them cost-effective and provides protection for your investment.

6500 The Catalyst 6500 series switches are designed to address the need for gigabit port density, high availability, and multi-layer switching for the core layer backbone and server-aggregation environments. These switches use the Cisco IOS to utilize the high speeds of the ASICs, which allows the delivery of wire-speed traffic management services end to end.

8500 The Cisco Catalyst 8500 is a core layer switch that provides high-performance switching. The Catalyst 8500 uses ASICs to provide multiple-layer protocol support including IP, IP multicast, bridging, ATM switching, and policy-enabled QoS.

All these switches provide wire-speed multicast forwarding, routing, and Protocol Independent Multicast (PIM) for scalable multicast routing. These switches are perfect for providing the high bandwidth and performance needed for a core router. The 6500 and 8500 switches can aggregate multiprotocol traffic from multiple remote wiring closets and workgroup switches.

Applying the Building Blocks

Remember the saying, "Everything I need to know I learned in kindergarten"? Well, it appears to be true. Cisco has determined that following the hierarchical model they have created promotes a building block approach to network design. If you did well with building blocks in your younger years, you can just apply that same technique to building large, multimillion-dollar networks. Kind of makes you glad it's someone else's money you're playing with, doesn't it?

In all seriousness, Cisco has determined some fundamental campus elements that help you build network building blocks:

Switch blocks Access layer switches connected to the distribution layer devices.

Core blocks Support of multiple switch blocks connected together with possibly 5500, 6500, or 8500 switches.

Within these fundamental elements, there are three contributing variables:

Server blocks Groups of network servers on a single subnet

WAN blocks Multiple connections to an ISP or multiple ISPs

Mainframe blocks Centralized services to which the enterprise network is responsible for providing complete access

By understanding how these work, you can build large, expensive networks with confidence (using someone else's money). After the network has been built, you will need to allow the switches to talk to each other to allow for redundancy and to route around outages. We will cover these topics later in this section after the blocks are discussed.

Switch Block

The *switch block* is a combination of layer 2 switches and layer 3 routers. The layer 2 switches connect users in the wiring closet into the access layer and provide 10Mbps or 100Mbps dedicated connections; 1900/2820 and 2900 Catalyst switches can be used in the switch block.

From here, the access layer switches will connect into one or more distribution layer switches, which will be the central connection point for all switches coming from the wiring closets. The distribution layer device is either a switch with an external router or a multi-layer switch. The distribution layer switch will then provide layer 3 routing functions, if needed.

The distribution layer router will prevent broadcast storms that could happen on an access layer switch from propagating throughout the entire internetwork. The broadcast storm would be isolated to only the access layer switch in which the problem exists.

Switch Block Size

To understand how large a switch block can be, you must understand the traffic types and the size and number of workgroups that will be using them. The number of switches that can collapse from the access layer to the distribution layer depend on the following:

- Traffic patterns
- Routers at the distribution layer
- Number of users connected to the access layer switches
- Distance VLANs must traverse the network
- Spanning tree domain size

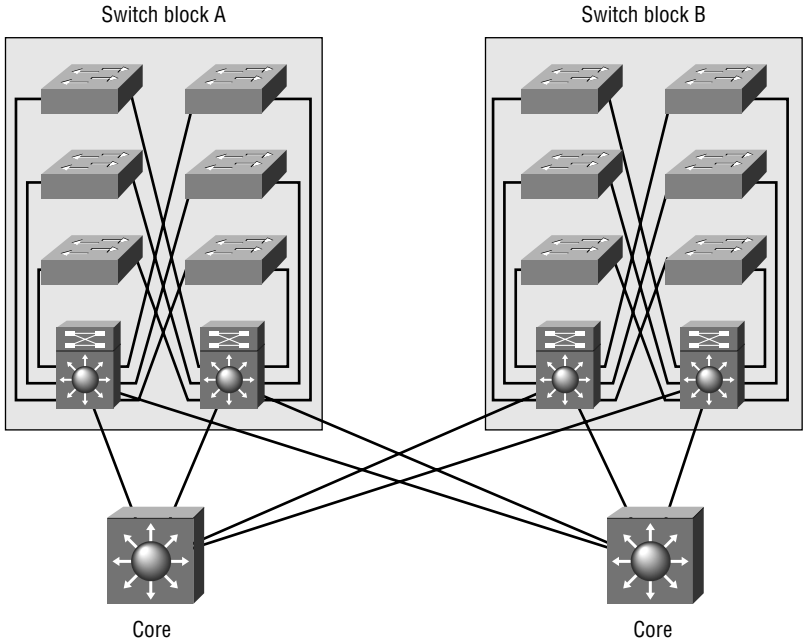
If routers at the distribution layer become the bottleneck in the network (which means the CPU processing is too intensive), the switch block has grown too large. Also, if too many broadcasts or multicast traffic slow down the switches and routers, your switch blocks have grown too large.

Having a large number of users does not necessarily indicate that the switch block is too large; too much traffic going across the network does.

Core Block

If you have two or more switch blocks, the Cisco rule of thumb states that you need a *core block*. No routing is performed at the core, only transferring of data. It is a pass-through for the switch block, the server block, and the Internet. Figure 1.8 shows a possible core block.

FIGURE 1.8 The core block



The core is responsible for transferring data to and from the switch blocks as quickly as possible. You can build a fast core with a frame, packet, or cell (ATM) network technology. The Switching exam is based on an Ethernet core network.

Typically, you would have only one subnet configured on the core network. However, for redundancy and load balancing, you could have two or more subnets configured.

Switches can trunk on a certain port or ports. This means that a port on a switch can be a member of more than one VLAN at the same time. However, the distribution layer will handle the routing and trunking for VLANs, and the core is only a pass-through after the routing has been performed. Because of this, core links will not carry multiple subnets per link; the distribution layer will.

A Cisco 6500 or 8500 switch is recommended at the core, and even though only one of those switches might be sufficient to handle the traffic, Cisco recommends two switches for redundancy and load balancing. You could consider a 5500 Catalyst switch if you don't need the power of the 6500 or the 8500.

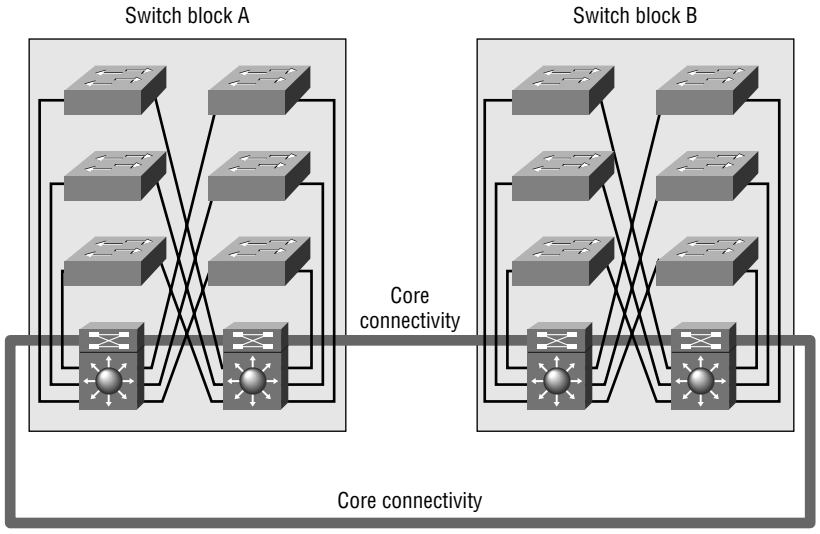
Collapsed Core

A *collapsed core* is defined as one switch performing both core and distribution layer functions. The collapsed core is typically found in a small network; however, the functions of the core and distribution layer are still distinct.

Redundant links between the distribution layer and the access layer switches, and between each access layer switch, can support more than one VLAN. The distribution layer routing is the termination for all ports.

Figure 1.9 shows a collapsed core network design.

FIGURE 1.9 Collapsed core

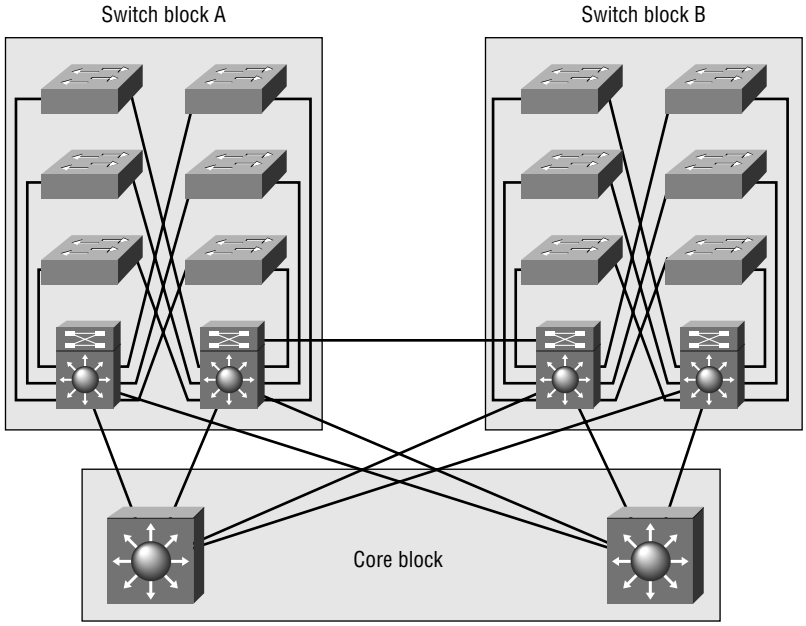


In a collapsed core network, Spanning Tree Protocol (STP) blocks the redundant links to prevent loops. Hot Standby Routing Protocol (HSRP) can provide redundancy in the distribution layer routing. It can keep core connectivity if the primary routing process fails.

Dual Core

If you have more than two switch blocks and need redundant connections between the core and distribution layer, you need to create a dual core. Figure 1.10 shows a possible dual core configuration. Each connection would be a separate subnet.

FIGURE 1.10 Dual core configuration



In Figure 1.10, you can see that each switch block is redundantly connected to each of the two core blocks. The distribution layer routers already have links to each subnet in the routing tables, provided by the layer 3 routing protocols. If a failure on a core switch takes place, convergence time will not be an issue. HSRP can be used to provide quick cutover between the cores.

Core Size

Routing protocols are the main factor in determining the size of your core. This is because routers, or any layer 3 device, isolate the core. Routers send updates to other routers, and as the network grows, so do these updates, so it takes longer to converge or to have all the routers update. Because at least one of the routers will connect to the Internet, it's possible that there will be more updates throughout the internetwork.

The routing protocol dictates the size of the distribution layer devices that can communicate with the core. Table 1.2 shows a few of the more popular routing protocols and the number of blocks each routing protocol supports.

Remember that this includes all blocks, including server, mainframe, and WAN.

TABLE 1.2 Blocks Supported by Routing Protocol

Routing Protocol	Max Number of Peers	Number of Subnet Links to the Core	Max Number of Supported Blocks
OSPF	50	2	25
EIGRP	50	2	25
RIP	30	2	15

Scaling Layer 2 Backbones

Typically, layer 2 switches are in the remote closets and represent the access layer, the layer where users gain access to the internetwork. Ethernet switched networks scale well in this environment, where the layer 2 switches then connect into a larger, more robust layer 3 switch representing the distribution layer. The layer 3 device is then connected into a layer 2 device representing the core. Because routing is not necessarily recommended in a classic design model at the core, the model then looks like Table 1.3.

TABLE 1.3 Classic Design Model

Access	Distribution	Core
Layer 2 switch	Layer 3 switch	Layer 2 switch

Spanning Tree Protocol (STP)

Chapter 4, "Layer 2 Switching and the Spanning Tree Protocol (STP)," and Chapter 5, "Using Spanning Tree with VLANs," detail the STP, but some discussion is necessary here. STP is used by layer 2 bridges to stop network loops in networks that have more than one physical link to the same network. There is a limit to the number of links in a layer 2 switched backbone that needs to be taken into account. As you increase the number of core

switches, the problem becomes that the number of links to distribution links must increase also, for redundancy reasons. If the core is running the Spanning Tree Protocol, then it can compromise the high-performance connectivity between switch blocks. The best design on the core is to have two switches without STP running. You can do this only by having a core without links between the core switches. This is demonstrated in Figure 1.11.

FIGURE 1.11 Layer 2 backbone scaling without STP

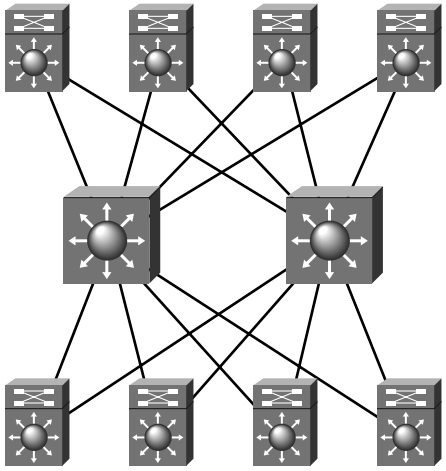


Figure 1.11 shows redundancy between the core and distribution layer without spanning tree loops. This is accomplished by not having the two core switches linked together. However, each distribution layer 3 switch has a connection to each core switch. This means that each layer 3 switch has two equal-cost paths to every other router in the campus network.

Scaling Layer 3 Backbones

As discussed in "Scaling Layer 2 Backbones," you'll typically find layer 2 switches connecting to layer 3 switches, which connect to the core with the layer 2 switches. However, it is possible that some networks might have layer 2/layer 3/layer 3 designs (layer 2 connecting to layer 3 connecting to layer 3). But this is not cheap, even if you're using someone else's money. There is always some type of network budget, and you need to have good reason to spend the type of money needed to build layer 3 switches into the core.

There are three reasons you would implement layer 3 switches into the core:

- Fast convergence
- Automatic load balancing
- Elimination of peering problems

Fast Convergence

If you have only layer 2 devices at the core layer, the STP will be used to stop network loops if there is more than one connection between core devices. The STP has a convergence time of more than 50 seconds, and if the network is large, this can cause an enormous number of problems if it has just one link failure.

STP is not implemented in the core if you have layer 3 devices. Routing protocols, which can have a much faster convergence time than STP, are used to maintain the network.

Automatic Load-Balancing

If you provide layer 3 devices in the core, the routing protocols can load-balance with multiple equal-cost links. This is not possible with layer 3 devices only at the distribution layer because you would have to selectively choose the root for utilizing more than one path.

Elimination of Peering Problems

Because routing is typically performed in the distribution layer devices, each distribution layer device must have "reachability" information about each of the other distribution layer devices. These layer 3 devices use routing protocols to maintain the state and reachability information about neighbor routers. This means that each distribution device becomes a peer with every other distribution layer device, and scalability becomes an issue because every device has to keep information for every other device.

If your layer 3 devices are located in the core, you can create a hierarchy, and the distribution layer devices will no longer be peers to each other's distribution device. This is typical in an environment in which there are more than 100 switch blocks.

Summary

In this chapter, you learned about switches and the different models available from Cisco. It is imperative that you understand the different models and what they are used for in the Cisco hierarchical design.

The past and future requirements of campus internetworks are an important part of your studies for your Cisco Switching exam. We discussed the current campus designs as well as how to implement FastEthernet, Gigabit Ethernet, Fast EtherChannel, and Multi-Layer Switching (MLS) in the emerging campus designs.

We also discussed the differences between layer 2, layer 3, and layer 4 switching technologies. You learned about the Cisco three-layer model and the different Catalyst switches that can be implemented at each layer of the Cisco model.

The chapter ended with a discussion of the switch and core blocks, which are based on the Cisco three-layer model, and how to design networks based on this model.

Exam Essentials

Understand the concept behind the three-layer model. Know that the access layer is used to provide access for most users into the rest of the network. Know that the distribution layer is used for routing, filtering, and for some access tasks. Know that the core layer is used to link switch blocks, and nothing that slows traffic down should be run here.

Understand the reasoning behind each of the switch block types. Know that a switch block is a collection of switching devices that provide access and distribution layer functions. Know what each of the block models is designed to do with the equipment available and know the terms behind the building of these blocks, terms such as *collapsed core*.

Understand the different product lines and the individual products that Cisco has available for switching tasks. Know which devices provide real layer 3 services, which ones are used in what spot in the switch block, and which ones can provide services not related to switching.

Key Terms

Before you take the exam, be sure you're familiar with the following terms:

20/80 rule	enterprise services
80/20 rule	hierarchy
access layer	layer 2 switching
application-specific integrated circuits (ASICs)	layer 3 switching
bandwidth	layer 4 switching
Cisco hierarchical model	local services
collapsed core	Media Access Control (MAC)
core block	multi-layer switching
core layer	Open Systems Interconnection (OSI) model
data encapsulation	remote services
distribution layer	switch block

Written Labs

In this section, you will complete the following written labs:

- Switching Definitions
- Cisco's Three-Layer Model
- Switching Theory

Lab 1.1: Switching Definitions

In the following table, the first column contains definitions of different types of switching. Fill in the second column with the number or numbers of the correct switching technology.

1. Layer 2 switching
2. Layer 3 switching
3. Layer 4 switching
4. Multi-layer switching

Definition	Switching type
Based on "route once, switch many"	
Enables prioritization based on specific applications	
Creates security by using source or destination addresses and port numbers	
Can use NetFlow switching	
Enables you to create flatter networks	
Builds a filtering table based on application port numbers	
Communicates with peer layers in a different system with packets	
Reads the TCP and UDP port fields for filtering and forwarding information	
Uses access lists to control traffic	
Uses hardware-based routing	
Uses hardware-based bridging	
Uses an ASIC to handle frame forwarding	
Provides both layer 2 and layer 3 functions	

Lab 1.2: Cisco's Three-Layer Model

Options 1, 2, and 3 are the layers in the Cisco three-layer model. Match the functions to the correct layer.

1. Access layer
2. Distribution layer
3. Core layer

Function	Layer
Routes traffic between VLANs	
Uses collision domains	
Uses broadcast domains	
Uses access lists	
Provides end users with access to the network	
Communicates between the switch blocks and to the enterprise servers	
Switches traffic as quickly as possible	

Lab 1.3: Switching Theory

Write the answers to the following questions:

1. Which device is used to break up broadcast domains?
2. Which device is used to break up collision domains?
3. What are the four methods of encapsulating user data through the OSI model?
4. Which Cisco layer is used to pass traffic as quickly as possible?
5. What is the Protocol Data Unit (PDU) used at the Transport layer?
6. What is the PDU used at the Network layer?
7. Which Cisco layer is used to break up collision domains?
8. Which OSI layer creates frames by encapsulating packets with a header and trailer?
9. What devices can provide multicast control and security?
10. What breaks up broadcast domains in a layer 2 switched network?

Review Questions

1. You work for a large company that needs to connect four buildings with a high-speed, high-bandwidth backbone. They are all on the same city block, and fiber already connects the buildings. There are multiple departments in each building and all run multiple protocols. The company already owns Cisco Catalyst 6000 series switches, which you can use for the distribution layer. What switch should you use for the core layer?

   A. 2900

   B. 4000

   C. 6500

   D. 8500

2. You need to install a large switched network for a company that has already defined its business requirements to be gigabit speed data transfer, high availability, and ISL routing to the server farms for all 300 users. What switch would you install for the distribution layer?

   A. 2900 with gigabit uplinks

   B. 4000 series

   C. 6000 series with a 16-port gigabit module

   D. 8500 series with gigabit uplinks

3. You just have been hired as a consultant for a small company that has users distributed across many floors in the same building. Servers for the company are all located on the first floor, and 30 users access them from various parts of the building. What switch would you install for the access layer connection?

   A. 1900 series

   B. 5000 series

   C. 6000 series

   D. 8000 series

4. You have just been promoted to network manager (congratulations!) for a large company. You need to connect four switch blocks; each contains 1500 users. You want to control broadcast domains at the switch blocks and use ISL to trunk between them. What switch would you purchase for the distribution layer?

   A. 1900 with gigabit links

   B. 4000 with gigabit VLAN

   C. 5500 with RSM module

   D. Catalyst 6000 with 16-port gigabit module

5. Which layer must be efficient and do nothing to slow down packets as they traverse the backbone?

   A. Access

   B. Distribute

   C. Distribution

   D. Backbone

   E. Core

6. Which of the following switches are recommended for use in the core? (Choose all that apply.)

   A. 4000

   B. 5000

   C. 6500

   D. 8500

7. Which of the following is the main factor in determining the size of your core?

   A. Routing protocols

   B. Routed protocols

   C. IP broadcasts

   D. ARPs

   E. ICMP redirects

   F. Number of distribution layer switches

8. The number of switches that can collapse from the access layer to the distribution layer depends on _____ . (Choose all that apply.)

   A. Traffic patterns

   B. Routers at the distribution layer

   C. Number of users connecting to the core layer

   D. Number of users connected to the access layer switches

   E. Number of distribution layer switches

   F. Distance VLANs must traverse the network

   G. Spanning tree domain size

9. Which of the following is generally performed at the distribution layer? (Choose all that apply.)

   A. Breaking up of collision domains

   B. No packet filtering

   C. Access lists, packet filtering, and queueing

   D. Routing between VLANs

10. Which of the following is also generally performed at the distribution layer? (Choose all that apply.)

    A. Broadcast and multicast domain definition

    B. Security and network policies

    C. Redistribution between routing protocols

    D. User access to the network

11. Which of the following is true regarding the access layer? (Choose all that apply.)

    A. This is where users gain access to the internetwork.

    B. The switches deployed at this layer must be able to handle connecting individual desktop devices to the internetwork.

    C. It is the aggregation point for multiple access switches.

    D. It can participate in MLS and handle a router processor.

12. Which of the following series of switches are suggested for use at the access layer? (Choose all that apply.)

    A. 1900/2800

    B. 2900

    C. 4000

    D. 5000

    E. 6000

    F. 8000

13. Which of the following Cisco switches provides a 10/100/1000Mbps advanced high-performance enterprise solution for up to 96 users and up to 36 Gigabit Ethernet ports for servers?

    A. 2926G

    B. 4000 series

    C. 6000 series

    D. 8000 series

14. Which of the following switches provides 10/100Mbps switched access for up to 50 users and gigabit speeds for servers and uplinks?

    A. 1900

    B. 2900

    C. 4000

    D. 6000

    E. 8000

15. Which of the following switches provides switched 10Mbps to the desktop or to 10BaseT hubs in small to medium campus networks?

    A. 1900/2800

    B. 2926G

    C. 4000 series

    D. 6000 series

16. Which layer of switching makes no modification of the data packet?

    A. Layer 2

    B. Layer 3

    C. Layer 4

    D. MLS

17. Layer 2 switching is _____ . (Choose all that apply.)

    A. Software based

    B. Hardware based

    C. Wire speed

    D. Asymmetrical

    E. Filtered using ASICs

18. Which Cisco switch can provide up to 384 10/100Mbps Ethernet connections, 192 100FX FastEthernet connections, or 130 Gigabit Ethernet ports?

    A. 1900EN XL

    B. 2926G

    C. 4000

    D. 6000

19. Which of the following describes Cisco Catalyst 5000 series switches?

    A. Provide an enterprise solution for up to 96 users and up to 36 Gigabit Ethernet ports for servers.

    B. Support a large number of connections and also support an internal route processor module.

    C. Only use an external router processor such as a 4000 or 7000 series router.

    D. The 5000 series is the Catalyst low-end model.

20. Which of the following is true regarding the distribution layer switches? (Choose all that apply.)

A. The distribution layer is the aggregation point for multiple access switches.

B. This is where users gain access to the internetwork.

C. The switches deployed at this layer must be able to handle connecting individual desktop devices to the internetwork.

D. The distribution layer can participate in MLS and handle a router processor.

Answers to Written Labs

Answers to Lab 1.1

Definition	Numbered Answer
Based on "route once, switch many"	4
Enables prioritization based on specific applications	3
Creates security by using source or destination addresses and port numbers	3
Can use NetFlow switching	2, 3
Enables you to create flatter networks	1
Builds a filtering table based on application port numbers	3
Communicates with peer layers in a different system with packets	2
Reads the TCP and UDP port fields for filtering and forwarding information	3
Uses access lists to control traffic	2, 3
Uses hardware-based routing	2
Uses hardware-based bridging	1
Uses an ASIC to handle frame forwarding	1, 2
Provides both layer 2 and layer 3 functions	4

Answers to Lab 1.2

Function	Layer
Routes traffic between VLANs	2
Uses collision domains	1
Uses broadcast domains	2
Uses access lists	2

Function	Layer
Provides end users with access to the network	1
Communicates between the switch blocks and to the enterprise servers	3
Switches traffic as quickly as possible	3

Answers to Lab 1.3

1. A layer 3 device, usually a router. Layer 2 devices do not break up broadcast domains.
2. A layer 2 device, typically a switch. Although routers break up both collision domains and broadcast domains, layer 2 switches are primarily used to break up collision domains.
3. Segment, packet, frame, bits. It is important to understand the question. This question asked for the encapsulation methods, which means how data is encapsulated as user data goes from the Application layer down to the Physical layer.
4. The core layer should have no packet manipulation, if possible.
5. Segments are the name for the PDU used at the Transport layer.
6. A packet or datagram is the PDU used at the Network layer.
7. Access layer. Remember, the distribution layer is used to break up broadcast domains, and the access layer is used to break up collision domains.
8. Data Link. Data is encapsulated with header and trailer information at the Data Link layer.
9. Routers or layer 3 devices are the only devices that control broadcasts and multicasts, as well as providing packet filtering.
10. Virtual LANs. These are configured on the layer 2 switches, and layer 3 devices provide a means for moving traffic between the VLANs.

Answers to Review Questions

1. D. A Cisco 6500 or 8500 switch is recommended at the core, and even though only one of those switches might be sufficient to handle the traffic, Cisco recommends two switches for redundancy and load balancing. You could consider a 5500 Catalyst switch if you don't need the power of the 6500 or the 8500. Because the customer is using 6500 at the distribution layer, you should use 8500s as the core switches. D is the best answer.
2. C. The Catalyst 6000 can provide up to 384 10/100Mbps Ethernet connections, 192 100FX FastEthernet connections, or 130 Gigabit Ethernet ports. Because there are 300 users, the 6000 series would be a good fit. The 8500 is a recommended core switch, and the question asks for an access layer/distribution layer solution.
3. A. A 5000 series switch might be overkill for the needs of the company. Because the question involves a small company and no growth was specified, a couple of 1900s would be the most cost-effective solution.
4. C. The 5500 can use a Route Switch Module (RSM) to provide layer 3 services to the internetwork. It also can provide a large number of ports per switch.
5. E. The core layer should be designed to connect distribution layer devices. No packet manipulation should occur at this layer.
6. C, D. The core layer needs very fast switches to move data as quickly as possible between distribution layer devices.
7. A. Routing protocols are protocols that are used to update routers with network information. Routed protocols are used to send user data through an internetwork.
8. A, B, D, F, G. Traffic patterns, the number of routers, the number of users connected into access layer switches, distance, and spanning tree size are all factors that contribute to the number of switches that can collapse from the access layer to the distribution layer.
9. C, D. The distribution layer performs routing, which breaks up broadcast domains. Routers can be configured with access lists, packet filters, and queueing.

10. A, B, C. The distribution layer performs routing, which breaks up broadcast domains by default. Security can be performed as well as network policies implemented. Routing protocols can be redistributed with most Cisco routers.

11. A, B. The access layer breaks up collision domains and connects the access layer to the internetwork by connecting to the distribution layer.

12. A, B, C, D. Any switches from the 1900 series to the 5000 series can work at the access layer. The 5000 and above are used at the distribution layer and the core layer.

13. B. The Cisco 4000 series was created for high performance, up to 36 gigabit ports, and 96-user connectivity.

14. B. The 1900 is fixed 10Mbps or 100Mbps ports and cannot handle gigabit speeds. The 2900 is the lowest model to handle gigabit speeds for up to 50 users maximum.

15. A. The 1900 is a low-end model that provides 10Mbps switched networking with up to 24 ports.

16. A. The Data Link layer (layer 2) encapsulates the packet but does not make any changes to it.

17. B, C, E. Layer 2 switching is considered hardware based because it uses an ASIC chip to make filtering decisions. It is also considered wire speed because no modification to the data packet takes place.

18. D. The Cisco Catalyst 6000 series provides up to 384 10/100Mbps Ethernet ports for user connectivity. It can also provide 192 100Mbps FastEthernet fiber uplinks or 130 Gigabit Ethernet ports.

19. B. The 5000 series Catalyst switches are the mainstay of the Cisco workforce. They can provide a very large number of connections and use an internal Route Switch Module (RSM) to run a fast router on the back plane of the switch.

20. A, D. The distribution layer connects the access layer devices, performs routing, and can provide multi-layer switching.

Chapter 2

Connecting the Switch Block

THE CCNP EXAM TOPICS COVERED IN THIS CHAPTER INCLUDE THE FOLLOWING:

- ✓ **Provide physical connectivity between two devices within a switch block**
- ✓ **Provide connectivity from an end user station to an access layer device**
- ✓ **Provide connectivity between two network devices**
- ✓ **Configure a switch for initial operation**
- ✓ **Apply IOS command set to diagnose and troubleshoot a switched network problems**

Bandwidth is now as important as crude oil. Without oil, we have no cars or factories, and basically, the economy stops. Oil is the fuel of the industrial world's economies. And network bandwidth is the oil of the twenty-first century. Without it—or when it's in short supply—our networks come to a grinding halt. If you think we're exaggerating, or you don't agree at all, just try shutting down a part of your network at work and watch the wars begin. Department will turn against department, friend will turn against friend—people will stop at nothing to get their computers up and running on the network, much like the chaos that would result if a Middle Eastern country were to refuse us our oil. Sure, if we have oil but no bandwidth, we can drive our cars and heat our homes, but we wouldn't be able to use the Internet. And without the Internet, we'd have to get into our cars and drive everywhere, among other inconveniences. Not a nice thought.

So, can we have bandwidth and world peace all at the same time? Yes. By creating a sound, hierarchical network that follows the Cisco three-layer model, you too can be a Nobel laureate at home and on the job.

This chapter will help you understand the different *contention media* available. Contention networks are first come, first served, or what we call Ethernet. This book covers only contention media because it runs at least 50 percent of the networks in the world, if not much more.

We'll teach you the basics of Ethernet networking and how to use the various flavors of Ethernet networking in your access, distribution, and core networks. After you have learned about the different Ethernet cable media types, you'll learn how to log in and configure both a set-based switch and an IOS-based switch. The chapter will end with a hands-on lab in which you'll connect the switches together and configure them.

Understanding Cable Media

To know when and how to use the different kinds of cable media, you need to understand what users *do* on the corporate network. The way to find this information is to ask questions. After that, you can use monitoring equipment to really see what is going on inside the network cabling. Before you deploy an application on a corporate network, carefully consider bandwidth requirements as well as latency issues. More and more users need to compete for bandwidth on the network because of bandwidth-consuming applications. Although layer 2 switches break up collision domains and certainly help a congested network if correctly designed and installed, you must also understand the different cable media types available and where to use each type for maximum efficiency. That's where this chapter comes in.

The Background of IEEE Ethernet

In 1980, the Digital Equipment Corporation, Intel, and Xerox (DIX) consortium created the original Ethernet. Predictably, Ethernet_II followed and was released in 1984. The standards-setting organization, the Institute of Electrical and Electronics Engineers (IEEE), termed this the 802 project. The 802 project was initially divided into three groups:

- The High Level Interface (HILI) became the 802.1 committee and was responsible for high-level internetworking protocols and management.
- The Logical Link Control (LLC) group became the 802.2 committee and focused on end-to-end link connectivity and the interface between the higher layers and the medium-access-dependent layers.
- The Data Link and Medium Access Control (DLMAC) group became responsible for the medium-access protocols. The DLMAC ended up splitting into three committees:
  - 802.3 for Ethernet
  - 802.4 for Token Bus
  - 802.5 for Token Ring

DEC, Intel, and Xerox pushed Ethernet, while Burroughs, Concord Data Systems, Honeywell, Western Digital, and later, General Motors and Boeing, pushed 802.4. IBM took on 802.5.

The IEEE then created the 802.3 subcommittee to come up with an Ethernet standard that happens to be almost identical to the Ethernet_II version of Ethernet. The two differ only in their descriptions of the Data Link layer. Ethernet_II has a Type field, whereas 802.3 has a Length field. Even so, they're both common in their Physical layer specifications, MAC addressing, and understanding of the LLC layer's responsibilities.

See *CCNA: Cisco Certified Network Associate Study Guide, 3rd Edition* by Todd Lammle (Sybex, 2002) for a detailed explanation of Ethernet frame types.

Ethernet_II and 802.3 both define a bus-topology LAN at 10Mbps, and the cabling defined in these standards is identical:

10Base2/Thinnet Segments up to 185 meters using RG58 coax at 50 ohms.

10Base5/Thicknet Segments up to 500 meters using RG8 or RG11 at 50 ohms.

10BaseT/UTP All hosts connect by using unshielded twisted-pair (UTP) cable to a central device (a hub or switch). Category 3 UTP is specified to support up to 10Mbps, category 5 to 100Mbps, category 6 to 155Mbps, and category 7 to 1Gbps.

Switched Ethernet

Ethernet is the most popular type of network in the world and will continue to be so. It is important to understand how hubs and switches work within an Ethernet internetwork.

By using *switched Ethernet* in layer 2 of your network, you no longer have to share bandwidth with the different departments in the corporation. With hubs, all devices have to share the same bandwidth, which can cause havoc in today's networks. This makes a switched Ethernet LAN much more scalable than one based on shared Ethernet.

Remember that layer 2 switches break up collision domains, but the network is still one large broadcast domain. Switched Ethernet has replaced shared hubs in the networking world because each connection from a host to the switch is its own collision domain. Remember that, with shared hubs, the network was one large collision domain and one large broadcast domain, whereas layer 2 switches break up collision domains on each port, but all ports are still considered, by default, to be in one large broadcast domain. Only virtual LANs, covered in Chapter 3, "VLANs," break up broadcast domains in a layer 2 switched network.

Switched Ethernet is a good way to dynamically allocate dedicated 10Mbps, 100Mbps, and 1000Mbps connections to each user. By also running full-duplex Ethernet, you can theoretically double the throughput on each link. In the next sections, we'll discuss how Ethernet is used in your internetwork, the differences between the Ethernet types, and half- and full-duplex.

Using Ethernet Media in Your Internetwork

In this section, you'll learn the difference between the Ethernet media types and how to use them in your internetworks. We'll cover the following Ethernet types:

- 10BaseT
- FastEthernet
- Gigabit Ethernet

10BaseT

10BaseT stands for 10 million bits per second (Mbps), baseband technology, twisted-pair. This Ethernet technology has the highest install base of any network in the world. It runs the Carrier Sense Multiple Access/Collision Detection (CSMA/CD) protocol and, if correctly installed, is an efficient network. However, if it gets too large and the network is not segmented correctly, problems occur. It is important to understand collision and broadcast domains and how to correctly design the network with switches and routers.

Use 10BaseT at the Access Layer

10BaseT Ethernet is typically used only at the access layer, and even then, FastEthernet (100BaseT) is quickly replacing it as the prices for 100BaseT continue to drop. It would be poor design to place 10BaseT at the distribution or core layers. You need transits that are much faster than 10BaseT at these layers.

Distance

The distance that 10BaseT can run and be within specification is 100 meters (330 feet). The 100 meters includes the following:

- Five meters from the switch to the patch panel
- Ninety meters from the patch panel to the office punch-down block
- Five meters from the punch-down block to the desktop connection

This doesn't mean that you can't run more than 100 meters on a cable run; it just is not guaranteed to work.

FastEthernet

FastEthernet is 10 times faster than 10Mbps Ethernet. The great thing about FastEthernet is that, like 10BaseT, it is still based on the CSMA/CD signaling. This means that you can run 10BaseT and 100BaseT on the same network without any problems. What a nice upgrade path this type of network can give you. You can put all your clients on 10BaseT and upgrade only the servers to 100BaseT if you need to. However, you can't even buy a PC that doesn't have a 10/100 Ethernet card in it anymore, so you really don't need to worry about compatibility and speed issues from the user's perspective.

Use FastEthernet at All Three Layers

FastEthernet works great at all layers of the hierarchical model. It can be used to give high performance to PCs and other hosts at the access layer, provide connectivity from the access layer to the distribution layer switches, and connect the distribution layer switches to the core network. Connecting a server block to the core layer would need, at a minimum, FastEthernet or maybe even Gigabit Ethernet.

IEEE Specifications for FastEthernet

There are two different specifications for FastEthernet, but the IEEE 802.3u is the most popular. The 802.3u specification is 100Mbps over category 3 or 5, twisted-pair (typically just category 5 or 5-plus is used for FastEthernet). The second Ethernet specification, called 802.12, used a different signaling technique, which was more efficient than the CSMA/CD access method. The IEEE passed both methods in June 1995, but because 802.3 Ethernet had such a strong name in the industry, 802.12, also called Demand Priority Access Method (DPAM), has virtually disappeared from the market. As with the Macintosh and NetWare operating systems, it doesn't mean anything if you have a better product; it matters only how you market it.

The IEEE 802.3u committee's goals can be summarized as follows:

- Provide seamless integration with the installed base
- Provide 100BaseT at only two times the cost (or less) of 10BaseT
- Increase aggregate bandwidth
- Provide multiple-vendor standardization and operability
- Provide time-bounded delivery

Media Independent Interface (MII)

FastEthernet requires a different interface than 10BaseT Ethernet. 10Mbps Ethernet used the Attachment Unit Interface (AUI) to connect Ethernet segments together. This provided a decoupling of the MAC layer from the different requirements of the various Physical layer topologies, which allowed the MAC to remain constant but meant the Physical layer could support any existing and new technologies. However, the AUI interface could not support 100Mbps Ethernet because of the high frequencies involved. 100BaseT needed a new interface, and the Media Independent Interface (MII) provides it.

100BaseT actually created a new subinterface between the Physical layer and the Data Link layer, called the Reconciliation Sublayer (RS). The RS maps the 1s and 0s to the MII interface. The MII uses a nibble, which is defined as 4 bits. AUI used only 1 bit at a time. Data transfers across the MII at one nibble per clock cycle, which is 25MHz. 10Mbps uses a 2.5MHz clock.

Full-Duplex Ethernet and FastEthernet

Full-duplex Ethernet can both transmit and receive simultaneously and uses point-to-point connections. It is typically referred to as collision free because it doesn't share bandwidth with any other devices. Frames sent by two nodes cannot collide because there are physically separate transmit and receive circuits between the nodes.

Both 10Mbps and 100Mbps Ethernet use four of the eight pins available in standard category 5 UTP cable. Pin 1 on one side and pin 3 on the other are linked, as are pins 2 and 6. When the connection is configured for half- duplex, the data can flow in only one direction at a time, while with full-duplex, data can come and go without collisions because the receive and send channels are separate.

Full-duplex is available when connected to a switch but not to a hub. Full-duplex is also available on 10Mbps, 100Mbps, and Gigabit Ethernet. Because it eliminates collisions, a full-duplex connection will disable the collision detection function on the port.

Use Full-Duplex Ethernet in the Distribution Layer

Because users typically work with client/server applications using read/write asymmetrical traffic, the best performance for full-duplex would be in the distribution layer, not necessarily in the access layer.

Full-Duplex with Flow Control was created to avoid packets being dropped if the buffers on an interface fill up before all packets can be processed. However, some vendors might not interoperate, and the buffering might have to be handled by upper-layer protocols instead.

Auto-Negotiation

Auto-negotiation is a process that enables clients and switches to agree on a link capability. This is used to determine the link speed as well as the duplex being used. The auto-negotiation process uses priorities to set the link configuration. Obviously, if both a client and switch port can use 100Mbps, full-duplex connectivity, that would be the highest-priority ranking, whereas half-duplex, 10Mbps Ethernet would be the lowest ranking.

You need to understand that the auto-negotiation protocols do not work that well and you would be better off to configure the switch and NICs to run in a dedicated mode instead of letting the clients and switches auto-negotiate. Later in this chapter, we'll show you how to configure your switches with both the speed and duplex options.

Auto-negotiation is one of the most common causes of frame check sequence (FCS) and alignment errors. If two devices are connected, and one is set to full-duplex and the other is set to half-duplex, one is sending and receiving on the same two wires while the other is using two wires to send and two to receive. Statically configuring the duplex on the ports eliminates this problem.

Intermittent connectivity issues can often be traced to auto-negotiation problems. If a single user occasionally has long connectivity outages, statically setting speed and duplex on both ends often helps.

Distance

FastEthernet does have some drawbacks. It uses the same signaling techniques as 10Mbps Ethernet, so it has the same distance constraints. In addition, 10Mbps Ethernet can use up to four repeaters, whereas FastEthernet can use only one or two, depending on the type of repeater. Table 2.1 shows a comparison of FastEthernet technologies.

TABLE 2.1 Comparison of FastEthernet Technologies

Technology	Wiring Category	Distance
100BaseTX	Category 5 UTP wiring; categories 6 and 7 are now available. Category 6 is sometimes referred to as cat 5 plus. Two-pair wiring.	100 meters
100BaseT4	Four-pair wiring, using UTP category 3, 4, or 5.	100 meters
100BaseFX	Multi-Mode Fiber (MMF) with 62.5-micron fiber-optic core with a 125-micron outer cladding (62.5/125).	400 meters

Gigabit Ethernet

In the corporate market, *Gigabit Ethernet* is the new hot thing. What is so great about Gigabit is that it can use the same network that your 10Mbps and 100Mbps Ethernet now use. You certainly do have to worry about distance constraints, but what a difference it can make in just a server farm alone!

Just think how nice it would be to have all your servers connected to Ethernet switches with Gigabit Ethernet and all your users using 100BaseT switched connections. Of course, all your switches would connect with Gigabit links as well. Add xDSL and cable to connect to the Internet and you have more bandwidth than you ever could have imagined just a few years ago. Will it be enough bandwidth a few years from now? Probably not. If you have the bandwidth, users will find a way to use it.

Use Gigabit Ethernet in the Switch, Core, and Server Blocks

Gigabit Ethernet can work in the switch block, the core block, and your server blocks:

Switch block You can use Gigabit Ethernet between the access layer switches and the distribution layer switches. Gigabit is not typically connected to end users, but that can change quickly.

Core block You can use Gigabit Ethernet to connect distribution layer switches in each building to the core switches.

Server block By placing a Gigabit switch in the server block, you can effectively connect your high-performance servers to the network with gigabit speeds. However, remember that, unless the server is tremendously fast, you might not notice a difference in speeds as compared to FastEthernet because the server processing can become the bottleneck. Time to throw out your Pentium 90 servers.

Protocol Architecture

Gigabit Ethernet became an IEEE 802.3 standard in the summer of 1998. The standard was called 802.3z. Gigabit is a combination of Ethernet 802.3 and FiberChannel and uses Ethernet framing the same way 10BaseT and FastEthernet do. This means that not only is it fast, but it can run on the same network as older Ethernet technology, which provides a nice migration plan. The goal of the IEEE 802.3z was to maintain compatibility to the 10Mbps

and 100Mbps existing Ethernet network. They needed to provide a seamless operation to forward frames between segments running at different speeds. The committee kept the minimum and maximum frame lengths the same. However, they needed to change the CSMA/CD for half-duplex operation from its 512-bit times to help the distance that Gigabit Ethernet could run.

Will Gigabit ever run to the desktop? Maybe. People said that FastEthernet would never run to the desktop when it came out, but it's now common. If Gigabit is run to the desktop, however, it's hard to imagine what we'll need to run the backbone with. 10000BaseT to the rescue! Yes, 10 Gigabit Ethernet is out!

Comparing 10BaseT, FastEthernet, and Gigabit Ethernet

There are some major differences between FastEthernet and Gigabit Ethernet. FastEthernet uses the Media Independent Interface (MII), and Gigabit uses the Gigabit Media Independent Interface (GMII). 10BaseT used the Attachment Unit Interface, or AUI. A new interface was designed to help FastEthernet scale to 100Mbps, and this interface was redesigned for Gigabit Ethernet. The GMII uses an 8-bit data path instead of the 4-bit path that FastEthernet MII uses. The clocking must operate at 125MHz to achieve the 1Gbps data rate.

Cisco offers a gigabit aggregation product in the 3500 series, the 3508, that has eight gigabit ports. Some private corporate tests have shown earlier versions of the 3508 to have throughput of 1 gigabit in each direction on the first two ports but only 650Mb in each direction on the other six. The 3550 series hasn't shown this problem.

Time Slots

Because Ethernet networks are sensitive to the round-trip-delay constraint of CSMA/CD, time slots are extremely important. Remember that in 10BaseT and 100BaseT, the time slots were 512-bit times. However, this is not feasible for Gigabit because the time slot would be only 20 meters in length. To make Gigabit useable on a network, the time slots were extended to 512 bytes (4096-bit times!). However, the operation of full-duplex Ethernet was not changed at all. Table 2.2 compares the new Gigabit Ethernet technologies.

Real World Scenario

Jumbo Frames

If Gigabit Ethernet is used from source to destination, you might consider using Jumbo frames. These are Ethernet frames that are 9000 bytes long. Jumbo frames don't work well if Gigabit is not used from end to end because fragmentation will take place, causing a small amount of latency.

Although Jumbo frames aren't likely to be used to the desktop, they can speed up the process of data transfer between servers. An e-commerce web server that makes a lot of calls to a database and gets large amounts of data at once would be a good candidate.

TABLE 2.2 Comparison of Gigabit Ethernet Technologies

Technology	Wiring Category	Cable Distance
1000BaseCX	Copper-shielded twisted-pair	25 meters
1000BaseT	Copper category 5, four-pair wiring, UTP	100 meters
1000BaseSX	MMF using 62.5 and 50-micron core, uses a 780-nanometer laser	260 meters
1000BaseLX	Single-mode fiber that uses a 9-micron core, 1300-nanometer laser	from 3 kilometers up to 10 kilometers
1000BaseZX	9-micron single-mode fiber or disposition shifted fiber	Up to 100 kilometers

Connecting and Logging In to a Switch

In this section, you will learn about two types of switches Cisco sells: the Catalyst 1900, 2900XL, and 3500XL, which are IOS based, and the

Catalyst 5000, which is set based. The Catalyst 1900 switch can now use a command-line interface (CLI), and the Cisco Internetworking Operating System (IOS) runs on the switch. This makes configuring the switch very similar to how you would configure a router. The 5000 series is still set based, which means you use the command `set` to configure the router. Throughout the rest of this book, we'll show you commands for these switches.

There are two types of operating systems that run on Cisco switches:

IOS based You can configure the switch from a command-line interface (CLI) that is very similar to the one used on Cisco routers. Catalyst 1900, 2820, 2900XL and 3500XL switches can be used with an IOS-based CLI, although some can be set with a menu system as well.

Set based Uses older, set-based CLI configuration commands. The Cisco switches that use the set-based CLI are the 2926 series, the 1948G, the 4000, the 5000, and the 6000 series.

It's time to be introduced to the Catalyst switches. Why the 1900? Cisco uses it on the exams, of course, and it enables you to run a CLI with IOS-based commands on a less-expensive switch than you would need to use with the 5000 series. The 1900 switches are great for home offices or other small offices where you can get 10Mbps switched ports with 100Mbps uplinks at a decent price. It sure beats shared hubs!

Cabling the Switch Block Devices

You can physically connect to a Cisco Catalyst switch by connecting either to the console port or an Ethernet port, just as you would with a router.

Connecting to the Console Port

The 1900, 2900, 3500, and 5000 series switches all have a console connector. However, the older 5000 series switches have a console connector that uses only an RS-232-type connector, which comes with the switch when purchased. The 1900, 2900, and 3500 switches, on the other hand, have a console port on the back, which is an RJ-45 port. The console cables for these switches are rolled cables.

1924 switches use a null-modem cable for the console port.

After you connect to the console port, you need to start a terminal emulation program, such as HyperTerminal in Windows. The settings are as follows:

- 9600bps
- 8 data bits
- No parity
- 1 stop bit
- No flow control

Do not connect an Ethernet cable, ISDN, or live telephone line into the console port. These things can damage the electronics of the switch.

Connecting to an Ethernet Port

The Catalyst 1900/2800 series switches have fixed port types. They are not modular like the 5000 series switches. The 1900/2800 switches use only 10BaseT ports for workstations and 100BaseT or FX for uplinks. Each switch has either 12 (model 1912) or 24 (model 1924) 10BaseT switch ports with 2 FastEthernet uplinks. The 100BaseTX ports are referred to as ports A and B. We have connected servers into these ports and are able to run 100Mbps—works great for a small network. To connect the ports to another switch as an uplink, you must use a crossover cable. It would be nice if there were a button for this function, but there isn't.

The 2900 and 3500 are largely Ethernet devices. The modular switches can use ATM, Token Ring, and FDDI, but most of the ports aren't fixed at a single speed. Each of the "regular" Ethernet ports are capable of running at either 10Mbps or 100Mbps, and Gigabit ports are fixed at 1000Mbps.

The Catalyst 5000 switches can run either 10Mbps or 100Mbps on any port, depending on the type of cards you buy. The supervisor cards always take the first slot and have two FastEthernet or Gigabit Ethernet ports for uplinks using either copper or fiber. All devices connected into either the 1900/2800 or 5000 series switches must be within 100 meters (330 feet) of the switch port.

When connecting devices such as workstations, servers, printers, and routers to the switch, you must use a straight-through cable. Use a crossover cable to connect between switches.

When a device is connected to a port, the port status LED light (also called the port link LED or link state LED) on the switching module panel comes on and stays on. If the light does not come on, the other end might be off or there might be a cable problem. Also, if a light comes on and off, an auto-speed and duplex problem is possible. We'll show you how to check that in the next section.

5000 Switch Startup

The 5000 series switch loads the software image from flash, and then asks you to enter a password, even if there isn't one set. Press Enter and you will see a `Console>` prompt. At this point, you can enter enable mode and configure the switch by using `set` commands:

```
BOOTROM Version 5.1(2), Dated Apr 26 1999 10:41:04
BOOT date: 08/02/02 BOOT time: 08:49:03
Uncompressing NMP image.  This will take a minute...
Downloading epld sram device please wait ...
Programming successful for Altera 10K10 SRAM EPLD
Updating epld flash version from 0000 to 0600

Cisco Systems Console

Enter password: [press return here]
2001 Mar 22 22:22:56 %SYS-5-MOD_OK:Module 1 is online
2001 Mar 22 22:23:06 %SYS-5-MOD_OK:Module 2 is online

Console>
```

1900 Switch Startup

When you connect to the 1900 console, the following menu appears. By pressing K, you can use the command-line interface, and M will enable you to configure the switch through a menu system. The I option enables you to configure the IP configuration of the switch (this can also be accomplished through the menu or CLI at any time). After the IP configuration is set, the I selection no longer appears:

```
1 user(s) now active on Management Console.

         User Interface Menu
```

```
        [M] Menus
        [K] Command Line
        [I] IP Configuration

Enter Selection:  K

        CLI session with the switch is open.
        To end the CLI session, enter [Exit].

>
```

2900XL/3500XL Switch Startup

Like everything else about them, the 2900 and 3500 boot up in a fashion similar to a router. As the switch boots, it will show diagnostics on the screen. It will display the version of code, information about the flash storage, various part and serial numbers, and so on. After everything is done, it has a setup mode, if there isn't a configuration already present:

```
          -- System Configuration Dialog --

At any point you may enter a question mark '?' for help.
Use ctrl-c to abort configuration dialog at any prompt.
Default settings are in square brackets '[]'.

Continue with configuration dialog? [yes/no]:
```

Cisco IOS- and Set-Based Commands

In this section, you'll learn how to configure the basics on both types of switches. Specifically, you'll learn how to do the following:

- Set the passwords
- Set the hostname
- Configure the IP address and subnet mask
- Identify the interfaces
- Set a description on the interfaces
- Configure the port speed and duplex

- Verify the configuration
- Erase the switch configuration

Setting the Passwords

The first thing you should do is configure the passwords. You don't want unauthorized users connecting to the switch. You can set both the user mode and privileged mode passwords, just as you can with a router. However, you use different commands.

As with any Cisco router, the login (user mode) password can be used to verify authorization of the switch, including Telnet and the console port. The enable password is used to allow access to the switch so the configuration can be viewed or changed.

The enable secret on a 5000 series switch may be from 0 through 30 characters and is case sensitive. On the 1900, 2900, and 3500, the password must be from 4 to 8 characters and they are not case sensitive.

5000 Series Set-Based Switch

To configure the two passwords on a 5000 series switch, use the command `set password` for the user mode password and the command `set enablepass` for the enable password:

```
2001 Mar 21 06:31:54 %SYS-5-MOD_OK:Module 1 is online
2001 Mar 21 06:31:54 %SYS-5-MOD_OK:Module 2 is online

Console> en

Enter password:
Console> (enable) set password ?
Usage: set password
Console> (enable) set password  [press enter]
Enter old password:
Enter new password:
Retype new password:
Password changed.
```

When you see the `Enter old password` prompt, you can leave it blank and press Enter if you don't have a password set. The output for the `Enter`

new password prompt doesn't show on the console screen. If you want to clear the user mode (login) password, type in the old password and then just press Enter when you're asked for a new password.

To set the enable password, use the command set enablepass and then press Enter:

```
Console> (enable) set enablepass
Enter old password:
Enter new password:
Retype new password:
Password changed.
Console> (enable)
```

You can type **exit** at this point to log out of the switch completely, which will enable you to test your new passwords.

1900 IOS-Based Switch

Even though the 1900 switch is a CLI running an IOS, the commands for the user mode and enable mode passwords are different than they are for a router. You use the command enable password, which is the same, but you choose different access levels, which is optional on a Cisco router but not on the 1900 switch. The enable secret password can be set as well, and it supercedes the enable password level 15. The Telnet password is set by setting either the enable password level 15 or the enable secret password.

Press K to enter CLI mode, and then enter enable mode and global configuration mode by using the configure terminal command:

```
1 user(s) now active on Management Console.

         User Interface Menu

      [M] Menus
      [K] Command Line
      [I] IP Configuration

Enter Selection:  K

       CLI session with the switch is open.
       To end the CLI session, enter [Exit].
```

```
#configure terminal
Enter configuration commands, one per line. End with CNTL/Z
(config)#enable password ?
   level  Set exec level password
(config)#enable password level ?
   <1-15>  Level number
```

To enter the user mode password, use level number 1. To enter the enable mode password, use level mode 15:

```
(config)#enable password level 1 todd
(config)#enable password level 15 sanfran
(config)#enable secret cisco
(config)#exit
#exit
CLI session with the switch is now closed.
Press any key to continue.
Catalyst 1900 Management Console
Copyright (c) Cisco Systems, Inc.  1993-1998
All rights reserved.
Enterprise Edition Software
Ethernet Address:      00-30-80-CC-7D-00
PCA Number:            73-3122-04
PCA Serial Number:     FAB033725XG
Model Number:          WS-C1912-A
System Serial Number:  FAB0339T01M
Power Supply S/N:      PHI031801CF
PCB Serial Number:     FAB033725XG,73-3122-04
-------------------------------------------------
1 user(s) now active on Management Console.
        User Interface Menu
     [M] Menus
     [K] Command Line
Enter Selection:  K
Enter password:  ****
       CLI session with the switch is open.
      To end the CLI session, enter [Exit].
```

```
>en
 Enter password:  ****
 #
```

Notice that the program prompted for a user mode password, which was the level 1 password entered. The enable password was the enable secret password set, which superceded the enable password level 15.

2900XL/3500XL IOS-Based Switch

The 2900 and 3500 are more like routers when it comes to configuring passwords than the 1900 is. You have the option of configuring encrypted or unencrypted passwords for both user mode access and privileged mode access as well as setting privilege levels:

```
2900XL(config)#enable password ?
  0      Specifies an UNENCRYPTED password will follow
  7      Specifies a HIDDEN password will follow
  LINE   The UNENCRYPTED (cleartext) 'enable' password
  level  Set exec level password
2900XL(config)#enable secret ?
  0      Specifies an UNENCRYPTED password will follow
  5      Specifies an ENCRYPTED secret will follow
  LINE   The UNENCRYPTED (cleartext) 'enable' secret
  level  Set exec level password
```

Setting the Hostname

The hostname on a switch, as well as on a router, is only locally significant. This means that it doesn't have any function on the network or for name resolution whatsoever. However, it is helpful to set a hostname on a switch so you can identify the switch when connecting to it. A good rule of thumb is to name the switch after the location it is serving.

Management applications, such as CiscoWorks, and processes, such as the Cisco Discovery Protocol (CDP), will use the hostname of a device to differentiate it from other devices. Not changing the hostname can lead to some confusion and cause more work to find out just which "Switch" is having problems.

5000 Series Set-Based Switch

To set the hostname on a 5000 series switch, use the `set system name` command:

```
Cisco Systems Console           Thu Mar 21 2001, 06:31:54

Enter password:
Console> en
Enter password:
Console> (enable) set system name Todd5000
Todd5000 (enable) set system name Todd5000>
Todd5000> (enable)
```

Because the location is his office, Todd5000 works for Todd. Notice that the first command used did not include a > prompt. We like to see that prompt, but you have to choose it. On a router, you can change the prompt, but the default is always a > prompt.

1900/2900XL/3500XL IOS-Based Switch

The switch command to set the hostname is exactly as it is with any router. The 2900 and 3500 will begin life with a device name of "Switch," just like the 5000. The 1900 doesn't have a name, as you can see below. You use the `hostname` command to make the change (remember, it is one word):

```
1 user(s) now active on Management Console.

        User Interface Menu

     [M] Menus
     [K] Command Line
     [I] IP Configuration
Enter Selection:  K
Enter password:  ****
      CLI session with the switch is open.
      To end the CLI session, enter [Exit].
>enable
Enter password:  ****
#configure terminal
```

```
Enter configuration commands, one per line. End with CNTL/Z
(config)#hostname Todd1900EN
Todd1900EN(config)#
```

Setting the IP Information

You do not have to set any IP configuration on the switch to make it work. You can just plug in devices and they should start working, as they do on a hub. IP address information is set so that you can either manage the switch via Telnet or other management software or configure the switch with different VLANs and other network functions.

5000 Series Set-Based Switch

To set the IP address information on a 5000 series switch, configure the supervisor engine that is plugged into slot 1 of every switch. This is called the *in-band* logical interface. Use the command `set interface sc0`:

```
Todd5000> (enable) set interface sc0 172.16.10.17
   255.255.255.0
Interface sc0 IP address and netmask set.
```

By default, the switch is configured for VLAN 1, which can be seen by using the `show interface` command. Notice also that the broadcast address for the subnet shows up and that you can change that by entering it with the `set interface sc0` command (but we can think of only one reason you would want to change that—to mess with the people in your MIS department):

```
Todd5000> (enable) show interface
sl0: flags=51<UP,POINTOPOINT,RUNNING>
  slip 0.0.0.0 dest 0.0.0.0
sc0: flags=63<UP,BROADCAST,RUNNING>
vlan 1 inet 172.16.10.17 netmask 255.255.255.0 broadcast
  172.16.10.255
Todd5000> (enable)
```

The command `set interface sl0` *`ip_address mask`* would be used for modem access to the switch. This enables addressing on the Serial Line Internet Protocol (SLIP) process. Before accessing the switch via a modem, the modem process must be enabled on the switch by using the `set system modem enable` command. The modem operates at a speed of 9600bps by default.

Real World Scenario

Remote Management

Many organizations have a large number of switches that need to be managed and often they need access directly to the console port for remote administration. A setup that allows remote access direct to the console port is desirable because some problems will prevent telnet or management access, which means you have to physically be there. Not something desirable at 3 A.M.!

Rather than installing several modems and telephone lines, consider an access server. Access servers such as the 2509-2512 allow for reverse telnet for up to 16 devices at a time and also allow for security features such as a RADIUS or TACACS+ authentication server or an IOS firewall configuration.

If you wanted to have the switch in a different VLAN, instead of the default VLAN 1, you could use the `set interface sc0` command:

```
Todd5000> (enable) set interface sc0 2
Interface sc0 vlan set.
Todd5000> (enable) show interface
sl0: flags=51<UP,POINTOPOINT,RUNNING>
  slip 0.0.0.0 dest 0.0.0.0
sc0: flags=63<UP,BROADCAST,RUNNING>
 vlan 2 inet 172.16.10.11 netmask 255.255.255.0 broadcast
   172.16.10.255
Todd5000> (enable)
```

Cisco recommends that you use VLAN 1 for management of the switch device and then create other VLANs for users. In other words, they don't recommend what we just showed you.

1900 IOS-Based Switch

To set the IP configuration on a 1900 switch, use the command `ip address`. By typing the command `show ip`, you can see the configuration (by default, nothing is set):

```
Todd1900EN#show ip
IP Address: 0.0.0.0
Subnet Mask: 0.0.0.0
```

```
Default Gateway: 0.0.0.0
Management VLAN:  1
Domain name:
Name server 1: 0.0.0.0
Name server 2: 0.0.0.0
HTTP server : Enabled
HTTP port :  80
RIP : Enabled
```

The default gateway should also be set, and the command is `ip default-gateway`:

```
Todd1900EN#configure terminal
Enter configuration commands, one per line.  End with
   CNTL/Z
Todd1900EN(config)#ip address  172.16.10.16 255.255.255.0
Todd1900EN(config)#ip default-gateway  172.16.10.1
Todd1900EN(config)#

Todd1900EN#show ip
IP Address: 172.16.10.16
Subnet Mask: 255.255.255.0
Default Gateway: 172.16.10.1
Management VLAN:  1
Domain name:
Name server 1: 0.0.0.0
Name server 2: 0.0.0.0
HTTP server : Enabled
HTTP port :  80
RIP : Enabled
Todd1900EN#
```

2900XL/3500XL IOS-Based Switch

The 2900s and 3500s operate in a similar manner to the 1900. An IP address will be configured for a particular VLAN, and then the management interface must be placed into that VLAN. Don't worry about what a VLAN is or how it works just yet; that will be covered in Chapter 3. The default VLAN for the switch is VLAN 1.

```
2924XL(config)#interface vlan 1
2924XL(config-if)#ip address 10.1.1.20 255.255.255.0
```

```
2924XL(config-if)#exit
2924XL(config)#ip default-gateway 10.1.1.1
```

To change what VLAN the management interface of a switch belongs to, you must first configure the appropriate VLAN and then move the management interface into the new VLAN by using the command `management`. Be sure to change the default gateway when you do this!

```
2924XL(config)#interface vlan 2
2924XL(config-if)#ip address 20.2.2.22 255.255.255.0
2924XL(config-if)#management
2924XL(config-if)#exit
2924XL(config)#ip default-gateway 20.2.2.1
```

Identifying Switch Interfaces

It is important to understand how to access switch ports. The 5000 series uses the *`slot/port`* command. The 1900 series uses the `type` *`slot/port`* command.

5000 Series Set-Based Switch

You can use the `show` command to view port statistics on a 5000 switch. Notice that, by default, the duplex and speed of the port are both set to `auto`. Also, typically the ports on a 2900, 4000, 5000, and 6000 series switch can be enabled, but it might be necessary to configure the ports so that they can be enabled with the `set port enable` command. You can turn off any port with the `set port disable` command:

```
Todd5000> (enable) show port ?
Usage: show port
       show port <mod_num>
       show port <mod_num/port_num>
Todd5000> (enable) show port 2/1
Port  Name   Status  Vlan  Level    Duplex Speed Type
----- ------------------ ---------- ---------- ------------
 2/1        connect   2     normal   auto  auto 10/100BaseTX

Todd5000> (enable) set port disable 2/1
Port 2/1 disabled.
Todd5000> (enable) show port 2/1
```

```
Port  Name     Status     Vlan     Level  Duplex Speed  Type
----- -------------------- ---------- ------ ------ -----
 2/1           disabled   1       normal   auto  auto 10/100BaseTX

Todd5000> (enable) set port enable 2/1
Port 2/1 enabled.
Todd5000> (enable) show port 2/1
Port  Name      Status      Vlan        Level  Duplex  Speed Type
----- ------  --------- ---------- ---------- ------ --- ------
2/1           connect    1       normal   auto  auto 10/100BaseTX
```

The command `show config` displays the complete current configuration of the set-based switch.

1900/2900XL/3500XL IOS-Based Switch

These switches take the *`type slot/port`* command with either the `interface` command or the `show` command. The `interface` command enables you to set interface-specific configurations. The 1900 and 3500 switches have only one slot, slot 0, whereas the 2900 can have up to three slots if it is modular:

```
2900XL#config t
2900XL(config)#interface FastEthernet ?
  <0-2>  FastEthernet interface number

2900XL(config)#interface FastEthernet 2/?
  <1-24>  FastEthernet interface number
```

Here, a 1900 is being demonstrated:

```
Todd1900EN#config t
Enter configuration commands, one per line.  End with CNTL/Z
Todd1900EN(config)#interface ethernet ?
   <0-0>  IEEE 802.3
Todd1900EN(config)#interface ethernet 0?
   /
Todd1900EN(config)#interface ethernet 0/?
   <1-25>  IEEE 802.3
```

```
Todd1900EN(config)#interface ethernet 0/1
Todd1900EN(config-if)#?
Interface configuration commands:
  cdp             Cdp interface subcommands
  description     Interface specific description
  duplex          Configure duplex operation
  exit            Exit from interface configuration mode
  help            Description of the interactive help system
  no              Negate a command or set its defaults
  port            Perform switch port configuration
  shutdown        Shutdown the selected interface
  spantree        Spanning tree subsystem
  vlan-membership VLAN membership configuration
```

You can switch between interfaces by using the `interface e 0/#` command. Notice that we demonstrate the following commands with spaces or without—it makes no difference.

To configure the two FastEthernet ports, the command is `interface fastethernet 0/#`. When going from a 10BaseT port to a FastEthernet port, you may type exit to go back one level before typing the new port name:

```
Todd1900EN(config-if)#interface e 0/2
Todd1900EN(config-if)#interface e0/3
Todd1900EN(config-if)#exit

Todd1900EN(config)#interface fastEthernet ?
   <0-0>  FastEthernet IEEE 802.3
Todd1900EN(config)#interface fastEthernet 0/?
   <26-27>  FastEthernet IEEE 802.3
Todd1900EN(config)#interface fastEthernet 0/26
Todd1900EN(config-if)#interface fastEthernet 0/27
Todd1900EN(config-if)# [control+Z]
```

You can view the ports with the `show interface` command:

```
Todd1900EN#show interface e0/1
Ethernet 0/1 is Suspended-no-linkbeat
Hardware is Built-in 10Base-T
Address is 0030.80CC.7D01
MTU 1500 bytes, BW 10000 Kbits
```

```
802.1d STP State:  Forwarding     Forward Transitions:  1
[output cut]
 Todd1900EN#show interface f0/26
FastEthernet 0/26 is Suspended-no-linkbeat
Hardware is Built-in 100Base-TX
Address is 0030.80CC.7D1A
MTU 1500 bytes, BW 100000 Kbits
802.1d STP State:  Blocking     Forward Transitions:  0
[output cut]
```

Configuring Interface Descriptions

You can set a description on an interface, which will enable you to administratively set a name for each interface. As with the hostname, the descriptions are only locally significant.

5000 Series Set-Based Switch

To set a description for the 5000 switch, use the `set port name` *`slot/port`* command. Spaces are allowed. You can set a name up to 21 characters long:

```
Todd5000> (enable) set port name 2/1 Sales Printer
Port 2/1 name set.
Todd5000> (enable) show port 2/1
Port  Name Status   Vlan Level  Duplex Speed  Type
----- -------------- ---------- ---- ----- ------ -------
2/1  Sales Printer  notconnect 2  normal  auto  auto 10/100BaseTX
```

1900/2900XL/3500XL IOS-Based Switch

For the 1900 series switch, use the `description` command. You cannot use spaces with the `description` command, but you can use underlining if you need to:

```
Todd1900EN#config t
Enter configuration commands, one per line.  End with CNTL/Z
Todd1900EN(config)#interface e0/1
Todd1900EN(config-if)#description Finance_VLAN
Todd1900EN(config-if)#interface f0/26
Todd1900EN(config-if)#description trunk_to_Building_4
Todd1900EN(config-if)#
```

You can view the descriptions with either the `show interface` command or the `show running-config` command:

```
Todd1900EN#show interface e0/1
Ethernet 0/1 is Suspended-no-linkbeat
Hardware is Built-in 10Base-T
Address is 0030.80CC.7D01
MTU 1500 bytes, BW 10000 Kbits
802.1d STP State:  Forwarding     Forward Transitions:  1
Port monitoring: Disabled
Unknown unicast flooding: Enabled
Unregistered multicast flooding: Enabled
Description: Finance_VLAN
Duplex setting: Half duplex
Back pressure: Disabled

Todd1900EN#show running-config
Building configuration...

Current configuration:
hostname "Todd1900EN"
!
ip address 172.16.10.16 255.255.255.0
ip default-gateway 172.16.10.1
!
interface Ethernet 0/1

  description "Finance_VLAN"
!
 [output cut]
```

Configuring the Port Speed and Duplex

By default, all 10/100 ports on the 5000 series switch are set to auto-detect the speed and duplex of the port. However, the 1900 switch has only 12 or 24 10BaseT ports, which cannot be changed, along with one AUI on the back, also fixed at 10Mb. It comes with one or two FastEthernet ports, which enable you to change the duplex only. The 2820 series has 24 10BaseT ports and two modular slots for FastEthernet. The 2900XL supports up to

48 10/100 ports with up to two slots for modular expansion. Typically, Gigabit Ethernet is used here. The 3500XL has up to 48 10/100 ports with a variable number of gigabit ports built in.

5000 Series Set-Based Switch

Because the ports on a 10/100 card are auto-detect, you don't have to necessarily set the speed and duplex. However, there are situations when the auto-detect does not work correctly, and by setting the speed and duplex, you can stabilize the link:

```
Todd5000> (enable) set port speed 2/1 ?
Usage: set port speed <mod_num/port_num>
   <4|10|16|100|auto>
Todd5000> (enable) set port speed 2/1 100
Port(s) 2/1 speed set to 100Mbps.
```

If you set the port speed to `auto`, both the speed and duplex are set to auto-negotiate the link. You can't set the duplex without first setting the speed:

```
Todd5000> (enable) set port duplex 2/1 ?
Usage: set port duplex <mod_num/port_num> <full|half>
Todd5000> (enable) set port duplex 2/1 full
Port(s) 2/1 set to full-duplex.
Todd5000> (enable) ^C
```

Notice that the command Ctrl+C was used in the preceding code. This is a break sequence used on both types of switches.

You can view the duplex and speed with the `show port` command:

```
Todd5000> (enable) show port 2/1
Port  Name          Status     Vlan   Level  Duplex Speed Type
----- ------------- ---------- ------- ------ ------ ----- ----
 2/1  Sales Printer notconnect  2    normal full  100 10/100BaseTX
```

1900/2900XL/3500XL IOS-Based Switch

You can set only the duplex on the 1900 switch because the ports are all fixed speeds but you can change the speed on the 2900XL and the 3500XL. Here is output from a 2900XL with a speed query on a 10/100 interface:

```
2900XL(config-if)#speed  ?
  10    Force 10 Mbps operation
```

```
  100   Force 100 Mbps operation
  auto  Enable AUTO speed configuration
```

Use the `duplex` command in interface configuration:

```
Todd1900EN(config)#interface f0/26
Todd1900EN(config-if)#duplex  ?
  auto               Enable auto duplex configuration
  full               Force full duplex operation
  full-flow-control  Force full duplex with flow control
  half               Force half duplex operation
 Todd1900EN(config-if)#duplex full
```

Table 2.3 shows the different duplex options available on the 1900/2800 and 2900XL switches.

TABLE 2.3 Duplex Options

Parameter	Definition
`auto`	Sets the port to auto-negotiation mode, which is the default for all 100BaseTX ports.
`full`	Forces the 10Mbps or 100Mbps ports into full-duplex mode.
`full-flow-control`	Works only with 100BaseTX ports. Uses flow control so buffers won't overflow.
`half`	Default for 10BaseT ports. Forces the ports to work only in half-duplex mode.

Use the `show interface` command to view the duplex configuration:

```
Todd1900EN#show interface f0/26
FastEthernet 0/26 is Suspended-no-linkbeat
Hardware is Built-in 100Base-TX
Address is 0030.80CC.7D1A
MTU 1500 bytes, BW 100000 Kbits
802.1d STP State:  Blocking     Forward Transitions:  0
Port monitoring: Disabled
Unknown unicast flooding: Enabled
```

```
Unregistered multicast flooding: Enabled
Description: trunk_to_Building_4
Duplex setting: Full duplex
Back pressure: Disabled
```

The output from a `show interface` on a 2900XL or 3500XL is very close to that of a router:

```
FastEthernet0/1 is down, line protocol is down
  Hardware is Fast Ethernet, address is 0050.2ae5.3041 (bia
    0050.2ae5.3041)
  MTU 1500 bytes, BW 0 Kbit, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive not set
  Auto-duplex , Auto Speed , 100BaseTX/FX
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Queueing strategy: fifo
  Output queue 0/40, 0 drops; input queue 0/75, 0 drops
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     1 packets input, 64 bytes
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 watchdog, 0 multicast
     0 input packets with dribble condition detected
     1 packets output, 64 bytes, 0 underruns
     0 output errors, 0 collisions, 1 interface resets
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
```

Verifying Connectivity

It is important to test the switch IP configuration. You can, of course, use the Ping program, as well as Telnet. The 5000 series also enables you to use the `traceroute` command.

5000 Series Set-Based Switch

Use the IP utilities Ping, Telnet, and Traceroute to test the switch in the network:

```
Todd5000> (enable) ping 172.16.10.10
172.16.10.10 is alive
Todd5000> (enable) telnet  ?
Usage: telnet <host> [port]
       (host is IP alias or IP address in dot notation:
   a.b.c.d)
Todd5000> (enable) traceroute
Usage: traceroute [-n] [-w wait] [-i initial_ttl] [-m max_
   ttl] [-p dest_port] [-q nqueries] [-t tos] host
   [data_size]
(wait = 1..300, initial_ttl = 1..255, max_ttl = 1..255
dest_port = 1..65535, nqueries = 1..1000, tos = 0..255
data_size = 0..1420, host is IP alias or IP address in
dot notation: a.b.c.d)
```

You can use the keystrokes Ctrl+Shift+6, then X, as an escape sequence.

1900/2900XL/3500XL IOS-Based Switch

You can use the Ping program and you can telnet into the switch. Although you can use Traceroute and Telnet with both the 2900XL and the 3500XL, you cannot telnet from the 1900 switch or use Traceroute. You can telnet to any of the switches, as long as a password has been set up.

```
Todd1900EN#ping 172.16.10.10
Sending 5, 100-byte ICMP Echos to 172.16.10.10, time out
   is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max
   0/2/10/ ms
Todd1900EN#telnet
            ^
% Invalid input detected at '^' marker.
```

Physical Troubleshooting

If the Ping test doesn't work, make sure IP addressing and gateways are set up correctly. If they are, and no other part of the network is having

problems, there is a good chance that the problem has to do with the Physical layer.

When testing Physical layer connectivity, it is important to focus the tests on the cabling and on the interfaces. In those instances when it is possible, test the port on the switch by plugging a laptop in directly. Plugging the patch cord into a different port can test the cable inside the wall. Finally, test the NIC by plugging the PC into a different cable run and port.

Erasing the Switch Configuration

The 1900 and 5000 series switches automatically copy their configuration to non-volatile RAM (NVRAM), whereas the 2900 and 3500 series require a manual save. You can delete the configurations if you want to start over.

5000 Series Set-Based Switch

To delete the configurations stored in NVRAM on the 5000 series switch, use the `clear config all` command. The `erase all` command will delete the contents of flash without warning. Be careful! Here is the code:

```
Todd5000> (enable) clear config ?
Usage: clear config all
       clear config <mod_num>
       clear config rmon
       clear config extendedrmon
Todd5000> (enable) clear config all
This command will clear all configuration in NVRAM.
This command will cause ifIndex to be reassigned on the
   next system startup.
Do you want to continue (y/n) [n]? y
........
..................
System configuration cleared.
```

To delete the contents of flash, use the `erase all` command:

```
Todd5000> (enable) erase all
FLASH on Catalyst:
Type            Address             Location
Intel 28F016    20000000            NMP (P3) 8MB SIM

Erasing flash sector...
```

```
Todd5000> (enable)
Todd5000> (enable) show flash
File      Version         Sector   Size    Built
--------- --------------- -------- ------- -------
```

Notice that when you type `erase all` and press Enter, the switch just starts erasing the flash and you can't break out of it. By using a `show flash` command, you can see that the contents of flash are now empty. You might not want to try this on your production switches. You can use the `copy tftp flash` command to reload the software.

1900 IOS-Based Switch

To delete the contents of NVRAM on a 1900 switch, use the `delete NVRAM` command. VLAN Trunk Protocol configuration is not deleted by using `delete VRAM` because it has its own NVRAM. You need to use the command `delete vtp` to clear the VTP configuration:

```
Todd1900EN#delete ?
  nvram  NVRAM configuration
  vtp    Reset VTP configuration to defaults
Todd1900EN#delete nvram
This command resets the switch with factory defaults.  All
   system parameters will revert to their default factory
   settings.  All static and dynamic addresses will be
   removed.
Reset system with factory defaults, [Y]es or [N]o?  Yes
```

2900XL/3500XL IOS-Based Switch

If you attempt to delete something on a 2900 series switch, you're given the option to delete a file from the flash. Oops! Not something you want to do in most cases. Instead, you can use the `erase` command to erase the startup configuration.

```
  2900XL#delete  ?
  flash:  File to be deleted
2900XL#erase  ?
  flash:          Filesystem to be erased
  nvram:          Filesystem to be erased
  startup-config  Erase contents of configuration memory
2900XL#erase startup-config
Erasing the nvram filesystem will remove all files!
  Continue? [confirm]
```

Summary

This chapter covered the different types of Ethernet you can use in an internetwork as well as the distance each type of Ethernet media can run. It's important to remember what you learned here.

Remember that the distance that 10BaseT can run and be within specification is 100 meters (330 feet). The 100 meters includes the following:

- Five meters from the switch to the patch panel
- Ninety meters from the patch panel to the office punch-down block
- Five meters from the punch-down block to the desktop connection

For FastEthernet, the specifications for each type are as follows:

100BaseTX Category 5 UTP wiring; categories 6 and 7 are now available. Category 6 is sometimes referred to as cat 5 plus. Two-pair wiring. 100 meters.

100BaseT4 Four-pair wiring, using UTP category 3, 4, or 5. 100 meters.

100BaseFX Multi-Mode Fiber (MMF) with 62.5-micron fiber-optic core with a 125-micron outer cladding (62.5/125). 400 meters.

For Gigabit Ethernet, the specifications for each type are as follows:

1000BaseCX Copper-shielded twisted-pair. 25 meters.

1000BaseT Copper category 5, four-pair wiring, UTP. 100 meters.

1000BaseSX MMF using 62.5 and 50-micron core, uses a 780-nanometer laser. Up to 260 meters.

1000BaseLX Single-mode fiber that uses a 9-micron core, 1300-nanometer laser. From 3 kilometers to 10 kilometers.

1000BaseZX Single-mode fiber with a 9-micron core or disposition shifted fiber. Up to 100 kilometers.

We showed you how to configure both a set-based switch and a command-line interface (CLI) switch. And we showed you how to set hostnames and

passwords. Finally, you learned how to configure an IP address on each switch and how to verify the configuration.

Exam Essentials

Understand how the set-based and IOS-based command lines are different. Know how to configure the basics in set-based and IOS-based environments. Know how to add a default gateway and IP address, set port speed and duplex, as well as show the status of these.

Understand physical network connectivity. Understand which cable is good for which task and the characteristics of the cable. Know that FastEthernet will use pins 1, 2, 3, and 6 on a UTP cable. Know the limitations of each type of cable.

Understand logical network connectivity. Understand issues with connectivity at layers 1 and 2. Know that a switch allows for full duplex connectivity, whereas a hub does not. Also know that turning on auto-detection for speed forces duplex into auto-detect mode.

Key Terms

Before you take the exam, be sure you're familiar with the following terms:

10BaseT
auto-negotiation
contention media
FastEthernet
Gigabit Ethernet
in-band
switched Ethernet

Written Lab

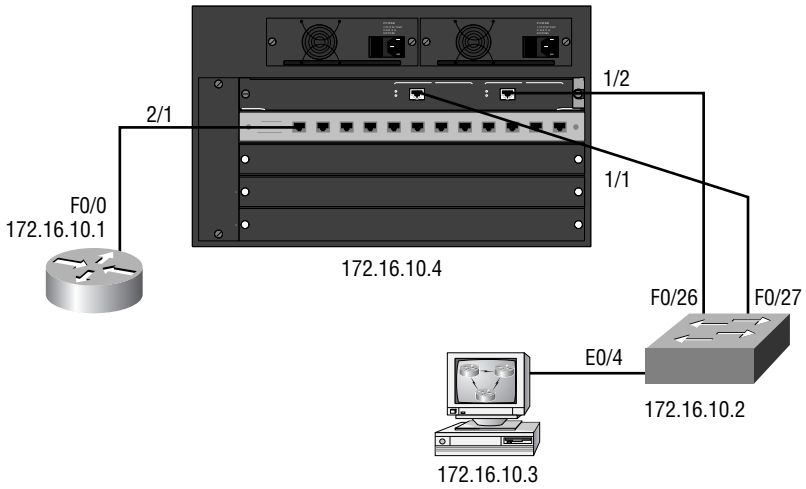
Write the answers to the following questions:

1. 100BaseFX is a point-to-point Ethernet topology that can run up to___ meters.
2. 1000BaseSX uses a 780-meter laser that can run a distance of ___ meters.
3. 100BaseT can run a total distance of ___ meters.
4. What command will set port 3 on card 2 of a 5000 series switch to full duplex?
5. What command will enable you to view the speed and duplex of port 6 on card 3 of a 5000 switch?
6. What command will show you the IP address of a 1900 switch?
7. How do you set the IP address on a 5000 series switch to `172.16.10.17 255.255.255.0`?
8. What command sets the enable password on a 5000 series switch?
9. What three IP commands can be used to test network connectivity of a device?
10. What type of Ethernet topology is suggested at the core layer?

Hands-On Lab

This lab will provide step-by-step instructions for configuring both access layer and distribution layer switches. You'll use a 1900 switch for the access layer and a 5000 series switch for the distribution layer. Figure 2.1 provides the network diagram that will be configured in this lab.

FIGURE 2.1 Access layer to distribution layer configuration



1. Configure the access layer switch by going to the console and pressing K to enter the CLI.
2. Assign the user mode password:

   ```
   enable
   configure terminal
   enable password level 1 cisco
   ```

3. Assign the enable password:

   ```
   enable password level 15 sanfran
   ```

4. (Optional) Assign the enable secret, which will override the enable password:

   ```
   enable secret todd
   ```

5. Set the hostname of the switch:

   ```
   hostname 1900A
   ```

6. Set the IP address of the switch:

   ```
   ip address 172.16.10.2 255.255.255.0
   ```

7. Set the default gateway for the switch:

   ```
   ip default-gateway 172.16.10.1
   ```

8. Set interface 4 to run in full-duplex:

```
interface Ethernet 0/4
duplex full
```

9. Set the description of the interface to Management PC:

```
interface e0/4
description Management_PC
Control-Z
```

10. Type the command to view the current configuration:

```
show running-config
```

11. Verify the IP configuration of the switch:

```
show ip
```

12. Verify the configuration of interface 4:

```
show interface e0/4
```

13. Configure the interface to full-duplex and add a description of Link to 5000A:

```
configure terminal (if needed)
interface fa 0/27
duplex full
description Link_To_5000A
```

14. Configure interface F0/26 to connect to the FastEthernet port 1/2 of the 5000 switch. Set the description and duplex as well:

```
Interface fa0/26
Duplex full
Description Another_Link_to_5000A
```

15. Move your console cable to the 5000 series distribution switch. Set the hostname to be 5000A:

```
enable
set system name 5000A>
```

16. Set the user mode and enable passwords:

    (examples)

```
set password cisco
set enablepass sanfran
```

17. Set the IP address of the 5000A switch:

```
set interface sc0 172.16.10.4 255.255.255.0
```

18. Configure the port speed and duplex of the connection to the access layer switch:

```
set port duplex 1/1 full
set port speed 1/1 100
```

19. Set the description of port 1/1 to Link to Access Layer:

```
set port name 1/1 Link to Access Layer
```

20. Set port 1/2 as the second connection to the access layer switch:

```
Set port duplex 1/2 full
Set port speed 1/2 100
Set port name 1/2 Another Link to Access Layer
```

21. Type the command to view port 1/1:

```
show port 1/1
```

22. Type the command to view the configuration of the 5000 switch:

```
show config
```

23. Test the connections by pinging all devices.

Review Questions

1. Which of the following is true about full-duplex Ethernet?
   - **A.** Full-duplex Ethernet can both transmit and receive simultaneously and use point-to-multipoint connections.
   - **B.** Full-duplex Ethernet can both transmit and receive simultaneously and use point-to-point connections.
   - **C.** Full-duplex Ethernet can only transmit simultaneously and uses point-to-multipoint connections.
   - **D.** Full-duplex Ethernet can only receive simultaneously and uses point-to-point connections.

2. Which of the following is *not* true regarding the 1900 switch?
   - **A.** You can ping from a 1900 switch if configured.
   - **B.** You can ping to a 1900 switch if configured.
   - **C.** You can telnet to a 1900 switch if configured.
   - **D.** You can telnet from a 1900 switch if configured.

3. What command sets interface e0/10 on a 2900 switch to run full-duplex Ethernet?
   - **A.** `full duplex on`
   - **B.** `duplex on`
   - **C.** `duplex full`
   - **D.** `full-duplex`
   - **E.** `set duplex on full`

4. Which command sets a 1900 switch interface to communicate so its buffers will not overflow on a congested link?
   - **A.** `flow on`
   - **B.** `duplex flow control`
   - **C.** `duplex full-flow-control`
   - **D.** `full duplex-flow`

5. If port 2 on card 3 on a 5000 series switch were disabled, what command would enable this interface?

   A. `set enable port 3/2`

   B. `set port enable 3/2`

   C. `set port enable 2/3`

   D. `set enable port 2/3`

6. If you wanted to verify the duplex on a 3500 switch, port 16, what command should you use?

   A. `show port 16`

   B. `show interface 16`

   C. `show interface e0/16`

   D. `show interface f0/16`

   E. `show interface g0/16`

   F. `show interface h0/16`

7. What is the command to set port 4 on card 3 to full-duplex on a 5000 series switch?

   A. `port duplex full 4/3`

   B. `set port duplex 3/4 full`

   C. `set port duplex 4/3 full`

   D. `duplex full`

8. What command would you use to set a description of the Sales printer on card 2, interface 3 for a 5000 switch?

   A. `set port name 2/3 Sales Printer`

   B. `set port name 2/3 Sales_Printer`

   C. `description Sales Printer`

   D. `description Sales_printer`

9. If you wanted to set the hostname on a 5000 series switch to Cat5k>, what command would you use?

   A. `host name cat5k`

   B. `hostname cat5k`

   C. `set prompt cat5k`

   D. `set system name cat5k>`

10. What is the distance that you can run a MMF, 62.5-micron Gigabit Ethernet cable?

    A. 400 meters

    B. 25 meters

    C. 260 meters

    D. 3 kilometers

    E. 10 kilometers

11. What is the distance that a single-mode, 9-micron Gigabit using a 1300-nanometer laser can run?

    A. 400 meters

    B. 25 meters

    C. 260 meters

    D. Up to 10 kilometers

12. What is the distance you can run an MMF with 62.5-micron fiber-optic core with a 125-micron outer cladding (62.5/125) using FastEthernet?

    A. 25 meters

    B. 400 meters

    C. 260 meters

    D. 3 kilometers

13. What is the distance you can run, and stay in spec, from a patch panel to a switch using 10BaseT?

    A. 5 meters

    B. 25 meters

    C. 90 meters

    D. 100 meters

    E. 330 feet

14. If you wanted to set port 3 on card 2 on a 5000 switch to run only 100Mbps, what command would you use?

    A. `set port speed 100 2/3`

    B. `port speed 100 3/2`

    C. `set port duplex 2/3 100`

    D. `set port speed 2/3 100`

15. Which of the following is true regarding a port status light on a switch?

    A. It is used to see whether a loop has occurred on the network.

    B. It is used to identify RTS signaling.

    C. When a device is connected to a port, the port status LED light comes on and stays on.

    D. When a device is connected to a port, the port status LED light comes on and then goes off.

16. If you want to delete the startup configuration on a 1900 switch, what command do you use?

    A. `erase startup-config`

    B. `delete startup-config`

    C. `delete nvram`

    D. `delete startup`

17. If you want to delete the configuration on a 5000 series switch, what command do you use?

    A. `clear config all`

    B. `clear nvram`

    C. `delete nvram`

    D. `erase startup`

18. What command would you use to identify port 3 on a 1900 switch to be Finance Server?

    A. `interface e0/3, description Finance Server`

    B. `interface e0/3, description Finance_Server`

    C. `set port name e0/3 Finance server`

    D. `set port name e0/3 Finance_Server`

19. What is the IEEE specification for FastEthernet?

    A. 802.3

    B. 802.2

    C. 802.3u

    D. 802.3z

20. What is the IEEE specification for Gigabit Ethernet?

    A. 802.3

    B. 802.2

    C. 802.3u

    D. 802.3z

Answers to Written Lab

1. 400
2. 260
3. 100
4. `set port duplex 2/3 full`
5. `show port 3/6`
6. `show ip`
7. `set interface sc0 172.16.10.17 255.255.255.0`
8. `set enablepass`
9. `ping`, `telnet`, and `traceroute`
10. FastEthernet or Gigabit Ethernet

Answers to Review Questions

1. B. Full-duplex Ethernet uses a point-to-point connection between the transmitter of the transmitting station and the receiver of the receiving station.
2. D. You cannot telnet from a 1900 switch console. You can telnet into the switch. You can ping to a 1900 switch and from a 1900 switch console.
3. C. The privileged command `duplex full` sets the duplex of a 2900 interface.
4. C. You can use the command `duplex full-flow-control` on a 1900 switch interface so flow control will be used on that particular interface.
5. B. The 5000 series of switches uses the `set` commands. To set a parameter on a certain interface, use the `set port` command. To enable a port that has been disabled, use the command `set port enable` *`slot/port`*.
6. D. The 3500 switch command-line interface uses the `show interface` *`slot/port`* command, the same as any router that has modular interface cards.
7. B. The 5000 uses the `set port` command to change interface parameters. The `set port duplex` *`slot/port`* command is used to set the duplex of a particular port.
8. A. Unlike the 1900, you do not need to add an underscore when you add a description on an interface with the 5000 series switch. The `set port` command is used to change port parameters, and `set port name` *`slot/port`* `description` is used to identify the port to an administrator. The first answer is the best one.
9. D. Use the command `set system name` to set the hostname on a 5000 series switch.
10. C. The maximum distance a Multi-Mode Fiber, 62.5-micron Gigabit Ethernet link can run is 260 meters.
11. D. Cisco supports up to 10 kilometers for a 1300-nanometer laser run using 9-micron Gigabit Ethernet.

12. B. FastEthernet point-to-point fiber runs can go a maximum distance of 400 meters.

13. A. Although everyone breaks this rule, the specifications state that the patch panel to switch distance can be only 5 meters.

14. D. The `set port` command sets the parameters for individual ports. The `set port speed` *`port/slot speed`* command sets the port speed on a 10/100 port.

15. C. If a device is correctly connected to a port and the device is powered on, the port light-emitting diode (LED) will come on and stay on.

16. C. The command `delete nvram` sets the configuration on a 1900 switch to the factory defaults.

17. A. The command that enables you to delete the configuration on a 5000 series switch is `clear config all`.

18. B. With the 1900 switch, you must use underscores between words. No spaces are allowed in the description of an interface.

19. C. The IEEE committee for FastEthernet is 802.3u.

20. D. The IEEE specification for Gigabit Ethernet is 802.3z.

Chapter

3

VLANs

THE CCNP EXAM TOPICS COVERED IN THIS CHAPTER INCLUDE THE FOLLOWING:

- ✓ **Apply IOS command set to diagnose and troubleshoot a switched network problems**
- ✓ **Describe the different Trunking Protocols**
- ✓ **Configure Trunking on a switch**
- ✓ **Maintain VLAN configuration consistency in a switched network**
- ✓ **Configure the VLAN Trunking Protocol**
- ✓ **Describe the VTP Trunking Protocol**
- ✓ **Describe LAN segmentation using switches**
- ✓ **Configure a VLAN**
- ✓ **Ensure broadcast domain integrity by establishing VLANs**

A virtual local area network (VLAN) is a logical grouping of network users and resources connected to administratively defined ports on a layer 2 switch. By creating VLANs, you are able to create smaller broadcast domains within a switch by assigning different ports in the switch to different subnetworks. A VLAN is treated as its own subnet or broadcast domain. This means that when frames are broadcast, they are switched between ports only within the same VLAN.

By using virtual LANs, you're no longer confined to creating workgroups based on physical locations. VLANs can be organized by location, function, department, or even the application or protocol used, regardless of where the resources or users are located.

In this chapter, you'll learn the following:

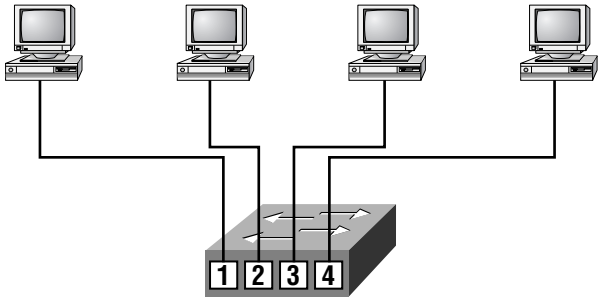
- What a VLAN is
- How to configure VLANs on both set-based and IOS-based switches
- VLAN trunking and VLAN Trunk Protocol (VTP) configurations
  - Trunking enables you to pass information about more than one VLAN on the same link.
  - VTP is used to send VLAN configuration information between switches.
- Frame tagging and identification methods
  - Identification methods both encapsulate a frame and insert a new field in a frame to identify it as it traverses a switched internetwork fabric.

Understanding the Design Benefits of Virtual LANs

Remember that layer 2 switches break up collision domains and that only routers can break up broadcast domains. However, virtual LANs can be used to break up broadcast domains in layer 2 switched networks. Routers are still needed in a layer 2 virtual LAN switched internetwork to enable the different VLANs to communicate with each other.

There are many benefits to creating VLANs in your internetwork. Remember that in a layer 2 switched network, the network is a *flat network*, as shown in Figure 3.1. Every broadcast packet transmitted is seen by every device on the network, regardless of whether the device needs to receive the data.

FIGURE 3.1 A flat network structure



- Each segment has its own collision domain.
- All segments are in the same broadcast domain.

In a flat network, your only security consists of passwords, and all users can see all devices. You cannot stop devices from broadcasting or users from trying to respond to broadcasts. Your security consists of passwords on the servers and other devices.

By creating VLANs, you can solve many of the problems associated with layer 2 switching.

Broadcast Control

Broadcasts occur in every protocol, but how often they occur depends on the protocol, the application(s) running on the internetwork, and how these services are used. VLANs can define smaller broadcast domains, which

means that it is possible to stop application broadcasts to segments that do not use the application.

Although some older applications have been rewritten to reduce their bandwidth needs, there is a new generation of applications that are bandwidth greedy, consuming all they can find. These are multimedia applications that use broadcasts and multicasts extensively. Faulty equipment, inadequate segmentation, and poorly designed firewalls can also add to the problems of broadcast-intensive applications.

These bandwidth-gobbling applications have added a new factor to network design because broadcasts can propagate through the switched network. Routers, by default, send broadcasts only within the originating network, but layer 2 switches forward broadcasts to all segments. This is called a flat network because it is one broadcast domain.

As an administrator, you must make sure the network is properly segmented to keep problems on one segment from propagating through the internetwork. The most effective way of doing this is through switching and routing. Because switches have become more cost-effective, a lot of companies are replacing the hub-and-router network with a pure switched network and VLANs. The largest benefit gained from switches with defined VLANs is that all devices in a VLAN are members of the same broadcast domain and receive all broadcasts. The broadcasts, by default, are filtered from all ports that are on a switch and are not members of the same VLAN.

Every time a VLAN is created, a new broadcast domain is created. VLANs are used to stop broadcasts from propagating through the entire internetwork. Some sort of route processor, a router, layer 3 switches, or Route Switch Modules (RSMs) must be used in conjunction with switches to provide connections between networks (VLANs).

Security

In a flat internetwork, security is implemented by connecting hubs and switches together with routers. Security is then maintained at the router, but this causes three serious security problems:

- Anyone connecting to the physical network has access to the network resources on that physical LAN.
- A user can plug a network analyzer into the hub and see all the traffic in that network.
- Users can join a workgroup just by plugging their workstation into the existing hub.

By using VLANs and creating multiple broadcast groups, administrators now have control over each port and user. Users can no longer just plug their workstation into any switch port and have access to network resources. The administrator controls each port and whatever resources it is allowed to use.

Because groups can be created according to the network resources a user requires, switches can be configured to inform a network management station of any unauthorized access to network resources. If inter-VLAN communication needs to take place, restrictions on a router can also be implemented. Restrictions can also be placed on hardware addresses, protocols, and applications.

Flexibility and Scalability

VLANs also add more flexibility to your network by limiting or adding only the users you want in the broadcast domain regardless of their physical location. Layer 2 switches read frames only for filtering; they do not look at the Network layer protocol. This can cause a switch to forward all broadcasts. However, by creating VLANs, you are essentially creating separate broadcast domains. Broadcasts sent out from a node in one VLAN will not be forwarded to ports configured in a different VLAN. By assigning switch ports or users to VLAN groups on a switch—or a group of connected switches (called a *switch-fabric*)—you have the flexibility to add only the users you want in the broadcast domain regardless of their physical location. This can stop broadcast storms caused by a faulty network interface card (NIC) or an application from propagating throughout the entire internetwork.

When a VLAN gets too big, you can create more VLANs to keep the broadcasts from consuming too much bandwidth. The fewer users in a VLAN, the fewer are affected by broadcasts.

The Collapsed Backbone and the VLAN

To understand how a VLAN looks to a switch, it's helpful to begin by first looking at a traditional collapsed backbone. Figure 3.2 shows a collapsed backbone created by connecting physical LANs to a router.

Each network is attached to the router, and each network has its own logical network number. Each node attached to a particular physical network must match that network number to be able to communicate on the internetwork. Now let's look at what a switch accomplishes. Figure 3.3 shows how switches remove the physical boundary.

FIGURE 3.2 Physical LANs connected to a router

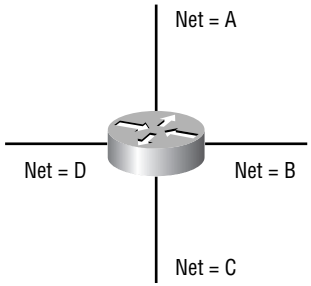
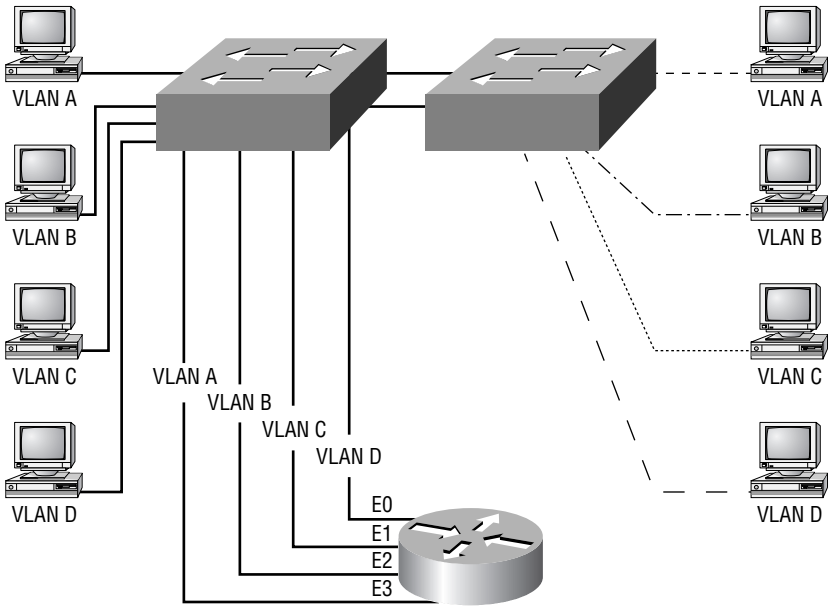


FIGURE 3.3 Switches remove the physical boundary



Switches create greater flexibility and scalability than routers can by themselves because switches define the network VLANs and VLAN port assignments. You can group users into communities of interest, which are known as VLAN organizations.

Because of switches, we don't need routers anymore, right? Wrong. In Figure 3.3, notice that there are four VLANs, or broadcast domains. The nodes within each VLAN can communicate with each other but not with any other VLAN or node in another VLAN. When configured in a VLAN, the

nodes think they are actually in a collapsed backbone, as in Figure 3.2. What do these hosts in Figure 3.2 need to do in order to communicate to a node or host on a different network? They need to go through the router, or other layer 3 device, just as they do when they are configured for VLAN communication, as shown in Figure 3.3. Communication between VLANs, just as in physical networks, must go through a layer 3 device.

Scaling the Switch Block

First introduced in Chapter 1, "The Campus Network," switch blocks represent a switch or group of switches providing access to users. These switches then connect to distribution layer switches, which in turn handle routing issues and VLAN distribution.

To understand how many VLANs can be configured in a switch block, you must understand the following factors:

- Traffic patterns
- Applications used
- Network management
- Group commonality
- IP addressing scheme

Cisco recommends a one-to-one ratio between VLANs and subnets. For example, if you have 2000 users in a building, then you must understand how they are broken up by subnets to create your VLANs. If you had 1000 users in a subnet, which is ridiculous, you would create only 2 VLANs. If you had only 100 users in a subnet, you would create about 20 VLANs or more.

It is actually better to create your broadcast domain groups (VLANs) and then create a subnet mask that fits the need. That is not always possible, and you usually have to create VLANs around an already configured network.

VLANs should not extend past the distribution switch on to the core.

Defining VLAN Boundaries

When building the switch block, you need to understand two basic methods for defining the VLAN boundaries:

- End-to-end VLANs
- Local VLANs

End-to-End VLANs

An *end-to-end VLAN* spans the switch-fabric from end to end; all switches in end-to-end VLANs understand about all configured VLANs. End-to-end VLANs are configured to allow membership based on function, project, department, and so on.

The best feature of end-to-end VLANs is that users can be placed in a VLAN regardless of their physical location. The administrator defines the port the user is connected to as a VLAN member. If the user moves, the administrator defines their new port as a member of their existing VLAN. In accordance with the 80/20 rule, the goal of an administrator in defining end-to-end VLANs is to maintain 80 percent of the network traffic as local, or within the VLAN. Only 20 percent or less should extend outside the VLAN.

Local VLANs

Unlike an end-to-end VLAN, a *local VLAN* is configured by physical location and not by function, project, department, and so on. Local VLANs are used in corporations that have centralized server and mainframe blocks because end-to-end VLANs are difficult to maintain in this situation. In other words, when the 80/20 rule becomes the 20/80 rule, end-to-end VLANs are more difficult to maintain, and so you will want to use a local VLAN.

In contrast to end-to-end VLANs, local VLANs are configured by geographic location; these locations can be a building or just a closet in a building, depending on switch size. Geographically configured VLANs are designed around the fact that the business or corporation is using centralized resources, such as a server farm. The users will spend most of their time utilizing these centralized resources and 20 percent or less on the local VLAN. From what you have read in this book so far, you must be thinking that 80 percent of the traffic is crossing a layer 3 device. That doesn't sound efficient, does it?

Because layer 3 devices are becoming faster and faster, you must design a geographic VLAN with a fast layer 3 device (or devices). The benefit of this design is that it will give the users a deterministic, consistent method of

getting to resources. However, you cannot create this design with a lower-end layer 3 model. This is not for the poor.

Assigning VLAN Memberships

After your VLANs are created, you need to assign switch ports to them. There are two types of VLAN port configurations: static and dynamic. A static VLAN requires less work initially but is more difficult for an administrator to maintain. A dynamic VLAN, on the other hand, takes more work up front but is easier to maintain.

Static VLANs

In a *static VLAN*, the administrator creates a VLAN and then assigns switch ports to it. The association does not change until the administrator changes the port assignment. This is the typical way of creating VLANs and it is the most secure. This type of VLAN configuration is easy to set up and monitor, working well in a network where the movement of users within the network is maintained by basically just locking the network closet doors. Using network management software to configure the ports can be helpful but is not mandatory.

Dynamic VLANs

If the administrator wants to do a little more work up front and add all devices' hardware addresses into a database, hosts in an internetwork can be assigned VLAN assignments dynamically. By using intelligent management software, you can enable hardware (MAC) addresses, protocols, or even applications to create dynamic VLANs. A *dynamic VLAN* will tell the switch port which VLAN it belongs to, based on the MAC address of the device that connects to the port.

For example, suppose MAC addresses have been entered into a centralized VLAN management application. If a node is then attached to an unassigned switch port, the VLAN management database can look up the hardware address and assign and configure the switch port to the correct VLAN. This can make management and configuration easier for the administrator. If a user moves, the switch will automatically assign them into the correct VLAN. However, more administration is needed initially to set up the database than to set up static VLANs, and additional administration is required for upkeep of the database.

Cisco administrators can use the VLAN Membership Policy Server (VMPS) service to set up a database of MAC addresses that can be used for dynamic addressing of VLANs. VMPS is a MAC-address-to-VLAN mapping database.

Configuring Static VLANs

For the Switching exam, Cisco is primarily interested in static VLAN configuration. We'll show you how to configure VLANs on a Catalyst 5000 switch, a Catalyst 1900 switch, and Catalyst 2900/3500 series switches.

It is important to understand the difference between the Catalyst 5000 series VLAN configuration and the IOS-based VLAN configuration.

Catalyst 5000 Series

To configure VLANs on a Catalyst 5000 switch, use the `set vlan` *`vlan# name`* command. Then, after your VLANs are configured, assign the ports to each VLAN:

```
Todd5000> (enable) set vlan 2 name Sales
Vlan 2 configuration successful
```

After the VLAN is configured, use the `set vlan` *`vlan# slot/ports`* command:

```
Todd5000> (enable) set vlan 2 2/1-2
VLAN  Mod/Ports
---- ----------------------
2     1/1-2
      2/1-2

Please configure additional information for VLAN 2.
Todd5000> (enable)
```

The additional information the switch wants you to configure is the VLAN Trunk Protocol (VTP) information. (VTP and trunking are covered in more detail at the end of this chapter, where we will continue with the 5000 switch VLAN configuration.) The 5000 series switch enables you to configure as many ports as you wish to a VLAN at one time. However, the 1900 switch enables you to configure only one interface at a time to a VLAN.

Catalyst 1900 Series

On the 1900 series switch, choose K from the initial user interface menu to begin IOS configuration:

```
1 user(s) now active on Management Console.

          User Interface Menu
```

```
        [M] Menus
        [K] Command Line
        [I] IP Configuration

  Enter Selection:  K

        CLI session with the switch is open.
        To end the CLI session, enter [Exit].
```

To configure VLANs on an IOS-based switch, use the `vlan` *`vlan#`* `name` *`vlan_name`* command:

```
>enable
#configure terminal
Enter configuration commands, one per line. End with CNTL/Z
(config)#hostname 1900EN
1900EN(config)#vlan 2 name sales
1900EN(config)#vlan 3 name marketing
1900EN(config)#vlan 4 name mis
1900EN(config)#exit
```

Catalyst 2900XL/3500XL

Although the 1900EN switch commands are often the same as the ones for the higher-end closet switches, setting up VLANs on new 2900s or 3500s tends to confuse people. The reason is that these switches have a new mode off privileged mode called *VLAN database* configuration mode. This is where everything that is VLAN related will occur. After you know about this mode, though, creating new VLANs is a snap:

```
2900XL# vlan database
2900XL(vlan)# vlan 2 name sales
2900XL(vlan)# vlan 3 name marketing
2900XL(vlan)# exit
```

Remember that a created VLAN is unused until it is mapped to a switch port or ports, and that all ports are always in VLAN 1 unless set otherwise.

After you create the VLANs that you want, you use the `show vlan` command to see the configured VLANs. However, notice that, by default, all

ports on the switch are in VLAN 1. To change that, you need to go to each interface and tell it what VLAN to be a part of:

```
1900EN#show vlan

VLAN Name              Status     Ports
-------------------------------------
1    default           Enabled    1-12, AUI, A, B
2    sales             Enabled
3    marketing         Enabled
4    mis               Enabled
1002 fddi-default      Suspended
1003 token-ring-defau  Suspended
1004 fddinet-default   Suspended
1005 trnet-default     Suspended
-------------------------------------

VLAN Type           SAID   MTU  Parent RingNo BridgeNo Stp  Trans1 Trans2
------------------------------------------------------------------------------
1    Ethernet       100001 1500   0      0      0      Unkn 1002   1003
2    Ethernet       100002 1500   0      1      1      Unkn 0      0
3    Ethernet       100003 1500   0      1      1      Unkn 0      0
4    Ethernet       100004 1500   0      1      1      Unkn 0      0
1002 FDDI           101002 1500   0      0      0      Unkn 1      1003
1003 Token-Ring     101003 1500   1005   1      0      Unkn 1      1002
1004 FDDI-Net       101004 1500   0      0      1      IEEE 0      0
1005 Token-Ring-Net 101005 1500   0      0      1      IEEE 0      0
------------------------------------------------------------------------------
```

You can configure each port to be in a VLAN by using the `vlan-membership` command. You can configure VLANs only port by port (there is no command to assign more than one port to a VLAN at a time):

```
1900EN#configure terminal
Enter configuration commands, one per line. End with CNTL/Z
1900EN(config)#interface e0/2
1900EN(config-if)#v?
vlan-membership
```

```
1900EN(config-if)#vlan-membership ?
  dynamic  Set VLAN membership type as dynamic
  static   Set VLAN membership type as static
1900EN(config-if)#vlan-membership static ?
  <1-1005>  ISL VLAN index
1900EN(config-if)#vlan-membership static 2
1900EN(config-if)#interface e0/4
1900EN(config-if)#vlan-membership static 3
1900EN(config-if)#interface e0/5
1900EN(config-if)#vlan-membership static 4
1900EN(config-if)#exit
1900EN(config)#exit
```

Now, type **show vlan** again to see the ports assigned to each VLAN:

```
1900EN#show vlan

VLAN Name             Status     Ports
---------------------------------------
1    default          Enabled    1, 3, 6-12, AUI, A, B
2    sales            Enabled    2
3    marketing        Enabled    4
4    mis              Enabled    5
1002 fddi-default     Suspended
1003 token-ring-defau Suspended
1004 fddinet-default  Suspended
1005 trnet-default    Suspended
---------------------------------------

VLAN Type           SAID   MTU  Parent RingNo BridgeNo Stp  Trans1 Trans2
------------------------------------------------------------------------------
1    Ethernet       100001 1500   0      0      0      Unkn 1002   1003
2    Ethernet       100002 1500   0      1      1      Unkn 0      0
3    Ethernet       100003 1500   0      1      1      Unkn 0      0
4    Ethernet       100004 1500   0      1      1      Unkn 0      0
1002 FDDI           101002 1500   0      0      0      Unkn 1      1003
1003 Token-Ring     101003 1500   1005   1      0      Unkn 1      1002
1004 FDDI-Net       101004 1500   0      0      1      IEEE 0      0
1005 Token-Ring-Net 101005 1500   0      0      1      IEEE 0      0
------------------------------------------------------------------------------
```

You could also just type **show vlan *vlan#*** to gather information about only one VLAN at a time:

```
1900EN#show vlan 2

VLAN Name              Status     Ports
---------------------------------
2    sales             Enabled    2
---------------------------------

VLAN Type       SAID   MTU  Parent RingNo BridgeNo Stp  Trans1 Trans2
------------------------------------------------------------------------
2    Ethernet   100002 1500   0      1      1      Unkn 0      0
------------------------------------------------------------------------
1900EN#
```

Configuring the interfaces on the 2900 and 3500 is just a bit different. After the VLANs have been created, the interface needs to be made a member of the appropriate VLAN. The command `switchport mode access` is used to tell the port that it will be a member of a single VLAN. It is told what VLAN it is a member of with the command `switchport access vlan` *vlan#*.

```
2900XL(config)# interface fa0/10
2900XL(config-if)# switchport mode access
2900XL(config-if)# switchport access vlan 3
```

Identifying VLANs

VLANs can span multiple connected switches, which (as we stated earlier) Cisco calls a switch-fabric. Switches within the switch-fabric must keep track of frames as they are received on the switch ports, and they must keep track of the VLAN they belong to as the frames traverse the switch-fabric. Switches use frame tagging to perform this function. Switches can then direct frames to the appropriate port.

There are two types of links in a switched environment:

Access link An *access link* is a link that is part of only one VLAN, which is referred to as the native VLAN of the port. Any device attached to an

access link is unaware of a VLAN membership. This device just assumes it is part of a broadcast domain, with no understanding of the physical network. Switches remove any VLAN information from the frame before it is sent to an access link device. Access link devices cannot communicate with devices outside of their VLAN unless the packet is routed through a router.

Trunk link Trunks can carry multiple VLANs. Originally named after the trunks of the telephone system, which carry multiple telephone conversations, a *trunk link* is used to connect switches to other switches, to routers, or even to servers. Trunk links are supported on FastEthernet or Gigabit Ethernet only. To identify the VLAN that a frame belongs to, Cisco switches support two identification techniques: Inter-Switch Link (ISL) and 802.1q. Trunk links are used to transport VLANs between devices and can be configured to transport all VLANs or just a few VLANs. Trunk links still have a native VLAN, and that VLAN is used if the trunk link fails.

Frame Tagging

The switch in an internetwork needs a way to keep track of users and frames as they travel the switch-fabric and VLANs. Frame identification, called *frame tagging*, uniquely assigns a user-defined ID to each frame. This is sometimes referred to as a VLAN ID or color.

Frame tagging is used to identify the VLAN that the packet belongs to. The tag is placed on the frame as it enters the first switch it runs into. As long as the frame does not exit out a non-trunk port, the frame keeps the identifying tag. This enables each switch to see what VLAN the frame belongs to, and each switch that the frame reaches must identify the VLAN ID and then determine what to do with the frame based on the filter table. If the frame reaches a switch that has another trunk link, the frame can be forwarded out the trunk link port. After the frame reaches an exit to an access link, the switch removes the VLAN identifier. The end device will receive the frames without having to understand the VLAN identification.

If you are using NetFlow switching hardware on your Cisco switches, this will enable devices on different VLANs to communicate after taking just the first packet through the router. This means that communication can occur from port to port on a switch, instead of from port to router to port, when traversing VLANs.

VLAN Identification Methods

To keep track of frames traversing a switch-fabric, VLAN identification is used to identify which frames belong to which VLAN. There are multiple trunking methods:

Inter-Switch Link (ISL) Proprietary to Cisco switches, ISL is used for FastEthernet and Gigabit Ethernet links only. It can be used on switch ports and router interfaces as well as server interface cards to trunk a server. Server trunking is good if you are creating functional VLANs and don't want to break the 80/20 rule. The server that is trunked is part of all VLANs (broadcast domains) simultaneously. The users do not have to cross a layer 3 device to access a company-shared server.

IEEE 802.1q Created by the IEEE as a standard method of frame tagging. It actually inserts a field into the frame to identify the VLAN.

LAN Emulation (LANE) Used to communicate with multiple VLANs over ATM.

802.10 (FDDI) Used to send VLAN information over FDDI. Uses a SAID field in the frame header to identify the VLAN. This is proprietary to Cisco devices.

The Cisco Switching exam covers only the ISL and 802.1q methods of VLAN identification.

It is possible for a packet to move from one type of network, such as FDDI, to another, such as Ethernet. Ethernet, FDDI, Token Ring, and ATM have standards enabling the switch to translate one type into a different type. The configuration on the switch requires specifically stating that VLAN 53 is the same thing as ATM ELAN 953, for example. The code for this is derived from translational bridging.

Inter-Switch Link Protocol (ISL)

Inter-Switch Link Protocol (ISL) is a way of explicitly tagging VLAN information onto an Ethernet frame. This tagging information enables VLANs to be multiplexed over a trunk link through an external encapsulation method. By running ISL, you can interconnect multiple switches

and still maintain VLAN information as traffic travels between switches on trunk links.

Cisco created the ISL protocol, and therefore ISL is proprietary to Cisco devices only. If you need a nonproprietary VLAN protocol, use the 802.1q, which is covered next in this chapter.

ISL is an external tagging process, which means that the original frame is not altered but instead is encapsulated with a new 26-byte ISL header and a 4-byte frame check sequence (FCS) field at the end of the frame. Because the frame is encapsulated with information, only ISL-aware devices can read the frame. Token Ring devices can also be connected with the appropriate ports, if VTP version 2 is being used. The size of the frame can be up to 1548 bytes long for Ethernet and 17,878 bytes for Token Ring.

On multi-VLAN (trunk) ports, each frame is tagged as it enters the switch. ISL network interface cards (NICs) enable servers to send and receive frames tagged with multiple VLANs, so the frames can traverse multiple VLANs without going though a router, which reduces latency. This technology can also be used with probes and certain network analyzers. In addition, it makes it easy for users to attach to servers quickly and efficiently without going through a router every time they need to communicate with a resource. Administrators can use the ISL technology to simultaneously include file servers in multiple VLANs, for example.

It is important to understand that ISL VLAN information is added to a frame as soon as that frame enters the switch. The ISL encapsulation is removed from the frame if the frame is forwarded out an access link.

Preventing communication from one VLAN to another might be desirable, but the network design might still require that some devices have access to all VLANs. In addition to configuring a filter on a router, you can install a network card that is ISL or 802.1q capable. This enables an e-mail server or database server to be directly connected to all VLANs without a router being involved.

Standard for Virtual Bridged Local Area Networks (IEEE 802.1q)

Unlike ISL, which uses an external tagging process and encapsulates a frame with a new ISL encapsulation, 802.1q uses an internal tagging process by modifying the existing internal Ethernet frame. To access both links and

trunk links, the frame looks as if it is just a standard Ethernet frame because it is not encapsulated with VLAN information. The VLAN information is added to a field within the frame itself.

Like ISL, the purpose of 802.1q is to carry the traffic of more than one subnet down a single cable. 802.1q tags the frame in a standard VLAN format, which allows for the VLAN implementations of multiple vendors. The standard tag allows for an open architecture and standard services for VLANs and a standard for protocols in the provision of these services. Because adding VLAN information to a frame affects the frame length, two committees were created to deal with this issue: 802.3ac and 802.1q.

The VLAN frame format defined in both the 802.1q and 802.3ac is a 4-byte field that is inserted between the original Ethernet frame Source address field and the Type or Length field. The CRC of the frame must be recomputed whenever the VLAN information is inserted or removed from the frame. The Ethernet frame size can now be up to 1522 bytes if a tag is inserted.

The VLAN Tag Protocol Identifier (TPID) is globally assigned and uses an EtherType field value of 0x81-00. The Tag Control Information (TCI) is a 16-bit value and has three fields contained within:

User Priority A 3-bit field used to assign up to eight layers of priority. The highest priority is 0, and the lowest is 7 (specified in 802.1q).

Canonical Format Indicator (CFI) A 1-bit field that is always a 0 if running an 802.3 frame. This field was originally designed to be used for Token Ring VLANs, but it was never implemented except for some proprietary Token Ring LANs.

VLAN ID (VID) The actual VLAN number that the frame is assigned upon entering the switch (12 bits). The reserved VLAN IDs are as follows:

0x0-00 Null, or no VLAN ID, which is used when only priority information is sent

0x0-01 Default VLAN value of all switches

0x-F-FF Reserved

Because Ethernet frames cannot exceed 1518 bytes, and ISL and 802.1q frames can exceed 1518 bytes, the switch might record the frame as a baby giant frame.

Trunking

Trunk links are point-to-point, 100Mbps or 1000Mbps links between two switches, between a switch and a router, or between a switch and a server. Trunk links carry the traffic of multiple VLANs, from 1 to 1005 at a time. You cannot run trunk links on 10Mbps links.

Cisco switches use the Dynamic Trunking Protocol (DTP) to manage trunk negation in the Catalyst switch engine software release 4.2 or later, using either ISL or 802.1q. DTP is a point-to-point protocol and was created to send trunk information across 802.1q trunks. Dynamic ISL (DISL) was used to support trunk negation on ISL links only before DTP was released in software release 4.1; and before DISL, auto-negotiation of trunk links was not allowed.

A trunk is a port that supports multiple VLANs, but before it became a trunk, it was the member of a single VLAN. The VLAN it is a member of when it becomes a trunk is called a native VLAN. If the port were to lose the trunking ability, it would revert to membership in its native VLAN.

Configuring Trunk Ports

This section shows you how to configure trunk links on the 5000 series, 1900 series, and 2900/3500 series switches.

5000 Switch

To configure a trunk on a 5000 series switch, use the `set trunk` command, and on the IOS-based switch, use the `trunk on` command:

```
Console> (enable) set trunk 2/12 ?
Usage: set trunk <mod_num/port_num>
[on|off|desirable|auto|nonegotiate] [vlans] [trunk_type]
(vlans = 1..1005 An example of vlans is 2-10,1005)
       (trunk_type = isl,dot1q,dot10,lane,negotiate)

Console> (enable) set trunk 2/12 on isl
Port(s) 2/12 trunk mode set to on.
Port(s) 2/12 trunk type set to isl.
Console> (enable) 1997 Mar 21 06:31:54
%DTP-5-TRUNKPORTON:Port 2/12 has become isl trunk
```

Port 2/12 has become a trunk port that uses ISL encapsulation. Notice that we did not specify the VLANs to trunk. By default, all VLANs would

be trunked. Take a look at a configuration in which we specified the VLANs to use:

```
Console> (enable) set trunk 2/12 on 1-5 isl
Adding vlans 1-5 to allowed list.
Please use the 'clear trunk' command to remove
vlans from allowed list.
Port(s) 2/12 allowed vlans modified to 1-1005.
Port(s) 2/12 trunk mode set to on.
Port(s) 2/12 trunk type set to isl.
```

Notice that, even though we told the switch to use VLANs 1–5, it added 1–1005 by default. To remove VLANs from a trunk port, use the `clear vlan` command. We'll do that in a minute.

We need to explain the different options for turning up a trunk port:

`on` The switch port is a permanent trunk port regardless of the other end. If you use the `on` state, you must specify the frame tagging method because it will not negotiate with the other end.

`off` The port becomes a permanent non-trunk link.

`desirable` The port you want to trunk becomes a trunk port only if the neighbor port is a trunk port set to `on`, `desirable`, or `auto`.

`auto` The port wants to become a trunk port but becomes a trunk only if the neighbor port asked the port to be a trunk. This is the default for all ports. However, because `auto` switch ports will never ask (they only respond to trunk requests), two ports will never become a trunk if they are both set to `auto`.

`nonegotiate` Makes a port a permanent trunk port, but because the port does not use DTP frames for communication, there is no negotiation. If you're having DTP problems with a switch port connected to a non-switch device, then use the `nonegotiate` command when using the `set trunk` command. This will enable the port to be trunked, but you won't be sent any DTP frames.

Be careful when using the `nonegotiate` option. It is not unusual to set up switches initially with `auto` or `desirable` trunks and then lock them down with `on`, after the switch-fabric has settled down. If two trunk ports are configured with `auto` or `desirable`, they need to receive the negotiate packets to tell there is another trunk-capable device on the other side. If two trunk ports are both set to `desirable` but `nonegotiate`, no trunk will come up.

1900 Switch

The 1900 switch has the same options but runs only the ISL encapsulation method:

```
1900EN#configure terminal
Enter configuration commands, one per line.
End with CNTL/Z
1900EN(config)#interface f0/26
1900EN(config-if)#trunk ?
  auto         Set DISL state to AUTO
  desirable    Set DISL state to DESIRABLE
  nonegotiate  Set DISL state to NONEGOTIATE
  off          Set DISL state to OFF
  on           Set DISL state to ON
1900EN(config-if)#trunk auto
```

2900XL/3500XL

Setting an interface to become a trunk on a 2900 or 3500 is almost as simple. You place the switch into interface configuration mode and use a variation of the command you used to set an interface to be a member of a particular VLAN. These switches, though, support both ISL and 802.1q through the use of the `switchport trunk encapsulation (isl | dot1q)` command:

```
2900XL(config)# interface fa 0/10
2900XL(config-if)# switchport mode trunk
2900XL(config-if)# switchport trunk encapsulation dot1q
```

Clearing VLANs from Trunk Links

As demonstrated in the preceding sections, all VLANs are configured on a trunk link unless cleared by an administrator. If you do not want a trunk link to carry VLAN information because you want to stop broadcasts on a certain VLAN from traversing the trunk link, or because you want to stop topology change information from being sent across a link where a VLAN is not supported, use the `clear trunk` command.

This section shows you how to clear VLANs from trunk links on both the 5000 and 1900 series of switches.

5000 Series

The command to clear a VLAN from a trunk link is `clear trunk` *`slot/port vlans`*. Here is an example:

```
Console> (enable) clear trunk 2/12 5-1005
Removing Vlan(s) 5-1005 from allowed list.
Port 1/2 allowed vlans modified to 1-4
```

1900 Switch

To delete VLANs from a trunk port on a 1900, use the interface `no trunk-vlan` command:

```
1900EN(config-if)#no trunk-vlan ?
  <1-1005>  ISL VLAN index
1900EN(config-if)#no trunk-vlan 5
1900EN(config-if)#
```

Per Cisco documentation, you can clear up to 10 VLANs at once. The syntax is `no trunk-vlan` *`vlan-list`*. The VLANS must be separated by spaces. Typically, you wouldn't clear more than a few VLANs anyway, because functionally, it makes no difference if they are turned on or not. If you have security, broadcast, or routing update issues, you need to consider clearing VLANs from a trunk link.

2900/3500 Switch

In an effort to increase redundancy, Cisco has a third way of performing this task on the 2900 and 3500 series switches. The command `switchport trunk allowed vlan remove` *`vlan-list`* is used to limit what VLANs can use a particular trunk:

```
2900XL(config)# interface fa 0/10
2900XL(config-if)# switchport trunk allowed vlan remove 2-10,12,15
```

Unlike the 1900, the VLAN list used on the 2900/3500 should not have any spaces in it. Use a hyphen to show a contiguous range of VLANs that are to be excluded and use a comma to separate VLANs that are not contiguous.

Verifying Trunk Links

To verify your trunk ports, use the `show trunk` command. If you have more than one port trunking and want to see statistics on only one trunk port, you can use the `show trunk` *`port_number`* command:

```
Console> (enable) show trunk 2/12
Port      Mode         Encapsulation  Status        Native vlan
--------  -----------  -------------  ------------  -----------
 2/12     on           isl            trunking      1

Port      Vlans allowed on trunk
--------  ------------------------------------------------------
 2/12     1-4

Port      Vlans allowed and active in management domain
--------  ------------------------------------------------------
 2/12     1

Port      Vlans in spanning tree forwarding state and not pruned
--------  ------------------------------------------------------
 2/12     1
Console> (enable)
```

On the 1900 switch, it is the same command, but it can be run only on FastEthernet ports 26 and 27. For some reason, when the `show trunk` command is used, the IOS calls these ports A and B:

```
1900EN#show trunk ?
  A  Trunk A
  B  Trunk B
1900EN#show trunk a
DISL state: Auto, Trunking: On, Encapsulation type: ISL

1900EN#show trunk ?
  A  Trunk A
  B  Trunk B
1900EN#show trunk a ?
  allowed-vlans   Display allowed vlans
  joined-vlans    Display joined vlans
  joining-vlans   Display joining vlans
  prune-eligible  Display pruning eligible vlans
  <cr>
1900EN#show trunk a allowed-vlans
1-4, 6-1004
1900EN#
```

The 2900/3500 series of Catalyst switches continue to do it just a bit differently than the 1900. To view the trunk status of a port on one of these switches, the command `show interface interface_id switchport` needs to be used:

```
Switch# show interface fa0/10 switchport

Name: fa0/10
Switchport: Enabled
Administrative Mode: Trunk
Operational Mode: Trunk
Administrative Trunking Encapsulation: ISL
Operational Trunking Encapsulation: ISL
Negotiation of Trunking: Disabled
Access Mode VLAN: 0 (inactive)
Trunking Native Mode VLAN: 1 (default)
Trunking VLANs Enabled: 1-20, 45, 50-1005
Trunking VLANs Active: 1-3
Pruning VLANs Enabled: 2-1001

Priority for untagged frames: 0
Voice VLAN: none
Appliance trust: none
```

A VLAN that is enabled on the switch is one that the switch has learned exists in the switch-fabric of the LAN. Somewhere out there, a device needs that particular VLAN or it might be configured for future use. An active VLAN is a VLAN in which one or more ports on this switch are members.

Using VLAN Trunk Protocol (VTP)

VLAN Trunk Protocol (VTP) was created by Cisco to manage all the configured VLANs across a switched internetwork and to maintain consistency throughout the network. VTP enables an administrator to add, delete, and rename VLANs. These changes are then propagated to all switches.

VTP provides the following benefits to a switched network:

- Consistent configuration of global VLANs across all switches in the network

- Enabling VLANs to be trunked over mixed networks, for example, Ethernet to ATM LANE or FDDI
- Accurate tracking and monitoring of VLANs
- Dynamic reporting when VLANs are added to all switches
- Plug-and-play VLAN adding to the switched network

To enable VTP to manage your VLANs across the network, you must first create a VTP server. All servers that need to share VLAN information must use the same domain name, and a switch can be in only one domain at a time. This means that a switch can share VTP domain information only with switches configured in the same VTP domain.

A VTP domain can be used if you have more than one switch connected in a network. If all switches in your network are in only one VLAN, then VTP doesn't need to be used. VTP information is sent between switches via a trunk port between the switches.

Switches advertise VTP management domain information, such as the name, as well as a configuration revision number and all known VLANs with any specific parameters.

You can configure switches to receive and forward VTP information through trunk ports but not process information updates nor update their VTP database. This is called VTP transparent mode.

You can set up a VTP domain with security by adding passwords, but remember that every switch must be set up with the same password, which might be difficult. However, if you are having problems with users adding switches to your VTP domain, then a password can be used.

Switches detect the additional VLANs within a VTP advertisement and then prepare to receive information on their trunk ports with the newly defined VLAN in tow. The information would be VLAN ID, 802.10 SAID fields, or LANE information. Updates are sent out as revision numbers that are notification +1. Anytime a switch sees a higher revision number, it knows the information it receives is more current and will overwrite the current database with the new one.

Do you remember the `clear config all` command we talked about in Chapter 2, "Connecting the Switch Block"? Well, guess what? It really doesn't "clear all" after all. It seems that VTP has its own NVRAM, which means that VTP information as well as the revision number would still be present if you perform a `clear config all`. You can clear the revision number by power-cycling the switch.

Real World Scenario

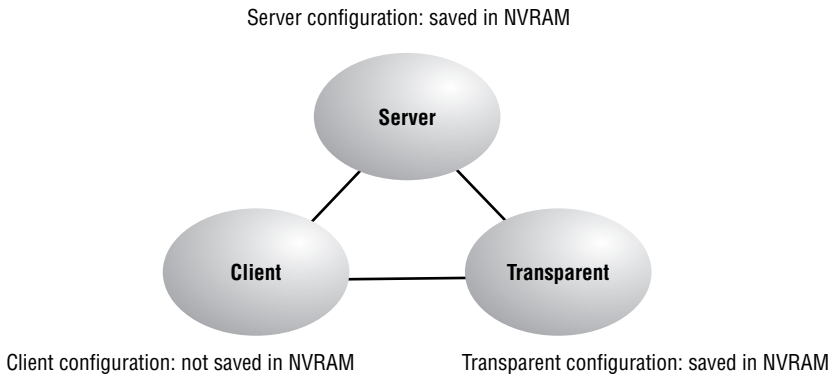
The Threat of High Revision Numbers

Many organizations have discovered the need for physical security when a device with only VLAN 1 but a high configuration revision number is added to the network. If a switch is a part of a test lab and then needs to be placed into production, it is best to clear everything and then power-cycle it. There have been instances of wiped switches erasing the VLAN setup of large organizations because the new device had a higher configuration revision number but had only VLAN 1. If a port belongs to a VLAN and that VLAN is removed, the port shuts down until the VLAN exists again. Adding the VLANs back and propagating them is a snap. The hassle and stress occur with discovering the problem. Using a VTP password is encouraged to prevent people from accidentally causing problems.

VTP Modes of Operation

There are three modes of operation within a VTP domain: server, client, and transparent. Figure 3.4 shows the three VTP modes.

FIGURE 3.4 VTP modes



Server

VTP server mode is the default for all Catalyst switches. You need at least one server in your VTP domain to propagate VLAN information throughout the domain. The following must be completed within server mode:

- Create, add, or delete VLANs on a VTP domain.

- Change VTP information. Any change made to a switch in server mode is advertised to the entire VTP domain.

Global VLANs must be configured on a server. The server will add the VLANs to the switch configuration so every time the switch boots up, the VLAN knowledge will be propagated.

Client

VTP clients receive information from VTP servers and send and receive updates, but they cannot make any changes to the VTP configuration as long as they are clients. No ports on a client switch can be added to a new VLAN before the VTP server notifies the client switch about the new VLAN. If you want a switch to become a server, first make it a client so that it receives all the correct VLAN information and then change it to a server. No global VTP information is kept if the switch loses power.

Transparent

VTP transparent switches do not participate in the VTP domain, but they will still receive and forward VTP advertisements through the configured trunk links. However, for a transparent switch to advertise the VLAN information out the configured trunk links, VTP version 2 must be used. If not, the switch will not forward anything. VTP transparent switches can add and delete VLANs because they keep their own database and do not share it with other switches. Transparent switches are considered locally significant.

VTP Advertisements

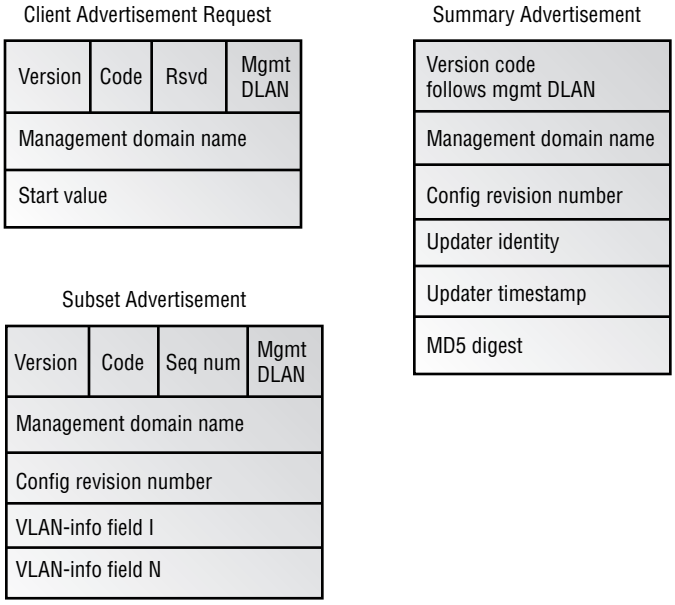
After the different types of VTP switches are defined, the switches can start advertising VTP information between them. VTP switches advertise information they know about only on their trunk ports. They advertise the following:

- Management domain name
- Configuration revision number
- VLANs the switch knows about
- Parameters for each VLAN

The switches use multicast MAC addresses so all neighbor devices receive the frames. A VTP server creates new VLANs, and that information is propagated through the VTP domain.

Figure 3.5 shows the three VTP advertisements: client, summary, and subset.

FIGURE 3.5 VTP advertisement content



The three types of messages are as follows:

Client requests Clients can send requests for VLAN information to a server. Servers will respond with both summary and subset advertisements.

Summary These advertisements are sent out every 300 seconds on VLAN 1 and every time a change occurs.

Subset These advertisements are VLAN specific and contain details about each VLAN.

The summary advertisements can contain the following information:

Management domain name The switch that receives this advertisement must have the name that is in this field or the update is ignored.

Configuration revision number Receiving switches use this to identify whether the update is newer than the one they have in their database.

Updater identity The name of the switch from which the update is sent.

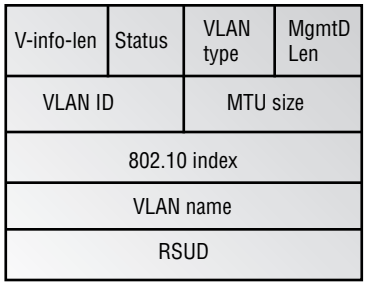
Updater timestamp Might or might not be used.

MD5Digest The key sent with the update when a password is assigned to the domain. If the key doesn't match, the update is ignored.

Subset Advertisements

The subset advertisements contain specific information about a VLAN. After an administrator adds, deletes, or renames a VLAN, the switches are notified that they are about to receive a VLAN update on their trunk links via the VLAN-info field 1. Figure 3.6 shows the VTP subset advertisement inside this field.

FIGURE 3.6 Subset advertisement



The following list includes some of the information that is advertised and distributed in the VLAN-info field 1:

VLAN ID Either ISL or 802.1q

802.10 SAID field that identifies the VLAN ID in FDDI

VTP VTP domain name and revision number

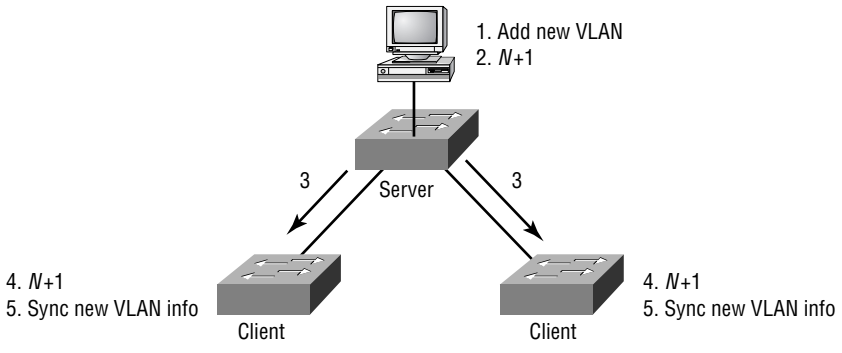
MTU Maximum transmission size for each VLAN

Configuration Revision Number

The revision number is the most important piece in the VTP advertisement. Figure 3.7 shows an example of how a revision number is used in an advertisement.

Figure 3.7 shows a configuration revision number as N. As a database is modified, the VTP server increments the revision number by 1. The VTP server then advertises the database with the new configuration revision number.

FIGURE 3.7 VTP revision number



When a switch receives an advertisement that has a higher revision number, then the switches will overwrite the database in NVRAM with the new database being advertised.

Configuring VTP

There are several options that you need to be aware of before attempting to configure the VTP domain:

1. Consider the version number of the VTP you will run.
2. Decide if the switch is going to be a member of an already existing domain or if you are creating a new one. To add it to an existing domain, find the domain name and password, if used.
3. Choose the VTP mode for each switch in the internetwork.

After everything is configured, the new setup should be verified to ensure that the connections would work properly.

Configure the VTP Version

There are two versions of VTP that are configurable on Cisco switches. Version 1 is the default VTP version on all switches and is typically used. No VTP version configuration is needed if you will be running version 1. Version 1 and version 2 are not compatible, so it is an all-or-nothing configuration for your switches. However, if all your switches are VTP version 2 compatible, changing one switch changes all of them. Be careful if you are not sure whether all your switches are version 2 compatible.

You would configure version 2 for the following reasons:

Token Ring VLAN support To run Token Ring, you must run version 2 of the VTP protocol. This means that all switches must be capable of running version 2.

TLV support Unrecognized type-length-value (TLV) support. If a VTP advertisement is received and has an unrecognized type-length-value, the version 2 VTP switches will still propagate the changes through their trunk links.

Transparent mode Switches can run in transparent mode, which means that they will only forward messages and advertisements, not add them to their own database. In version 1, the switch will check the domain name and version before forwarding, but in version 2, the switches will forward VTP messages without checking the version.

Consistency checks Consistency checks are run when an administrator enters new information in the switches, either with the CLI or other management software. If information is received by an advertisement or read from NVRAM, a consistency check is not run. A switch will check the digest on a VTP message, and if it is correct, no consistency check will be made.

To configure VTP version 2 on a 5000 series, use the `set vtp v2 enable` command:

```
Console> (enable) set vtp v2 enable
This command will enable the version 2 function
in the entire management domain.
All devices in the management domain should
be version2-capable before enabling.
Do you want to continue (y/n) [n]? y
VTP domain  modified
Console> (enable)
```

The 1900 switch uses only VTP version 1. There are no configuration options for VTP versions:

```
1900EN(config)#vtp ?
  client       VTP client
  domain       Set VTP domain name
  password     Set VTP password
  pruning      VTP pruning
  server       VTP server
  transparent  VTP transparent
  trap         VTP trap
```

Setting the 2900 or 3500 to use VTP version 2 is easy, as long as you remember that anything to do with VLAN or VTP administration occurs in VLAN database configuration mode.

```
2900XL# vlan database
2900XL(vlan)# vtp v2-mode
2900XL(vlan)# exit
```

Configure the Domain

After you decide which version to run, set the VTP domain name and password on the first switch. The VTP name can be up to 32 characters long. On the 5000, you can set the VTP domain password (the password is a minimum of 8 characters and a maximum of 64):

```
Console> (enable) set vtp domain ?
Usage: set vtp [domain <name>] [mode <mode>]
[passwd <passwd>]
[pruning <enable|disable>]
[v2 <enable|disable>
       (mode = client|server|transparent
        Use passwd '0' to clear vtp password)
Usage: set vtp pruneeligible <vlans>
       (vlans = 2..1000
        An example of vlans is 2-10,1000)
Console> (enable) set vtp domain Globalnet
VTP domain Globalnet modified
Console> (enable)
```

On the 1900, you don't have a VTP password option:

```
1900EN(config)#vtp domain ?
  WORD  Name of the VTP management domain
1900EN(config)#vtp domain Globalnet ?
  client       VTP client
  pruning      VTP pruning
  server       VTP server
  transparent  VTP transparent
  trap         VTP trap
  <cr>
1900EN(config)#vtp domain Globalnet
1900EN(config)#
```

On the 2900/3500, you have the option of setting a VTP password of 8 to 64 characters:

```
2900XL# vlan database
2900XL(vlan)# vtp domain GlobalNet
2900XL(vlan)# vtp password SwitchesAreFun
```

Configure the VTP Mode

Create your first switch as a server, and then create the connected switches as clients, or whatever you decided to configure them as. You don't have to do this as a separate command as we did; you can configure the VTP information in one line, including passwords, modes, and versions:

```
Console> (enable) set vtp domain
Usage: set vtp [domain <name>] [mode <mode>]
[passwd <passwd>]pruning <enable|disable>]
[v2 <enable|disable>
(mode = client|server|transparent
        Use passwd '0' to clear vtp password)
Usage: set vtp pruneeligible <vlans>
       (vlans = 2..1000
        An example of vlans is 2-10,1000)
Console> (enable) set vtp domain Globalnet mode server
VTP domain Globalnet modified
```

On the 1900, use the `vtp client` command:

```
1900EN(config)#vtp ?
  client       VTP client
  domain       Set VTP domain name
  password     Set VTP password
  pruning      VTP pruning
  server       VTP server
  transparent  VTP transparent
  trap         VTP trap
1900EN(config)#vtp client ?
  pruning  VTP pruning
  trap     VTP trap
  <cr>
1900EN(config)#vtp client
```

The 2900/3500 series uses the same commands as the 1900, just in a different mode:

```
2900XL# vlan database
2900XL(vlan)# vtp client
2900XL(vlan)# vtp server
```

Verify the VTP Configuration

You can verify the VTP domain information by using the commands `show vtp domain` and `show vtp statistics`. However, you cannot run a `show vtp domain` command on a 1900.

The `show vtp domain` command will show you the domain name, mode, and pruning information:

```
Console> (enable) show vtp domain
Domain Name              Domain Index VTP Version Local Mode  Password
-------------------- ------------ ----------- ----------------------
Globalnet       1            2           server
Vlan-count Max-vlan-storage Config Revision Notifications
---------- ---------------- --------------- --------------------------
5          1023             1               disabled

Last Updater    V2 Mode  Pruning  PruneEligible on Vlans
--------------- -------- -------- ----------------------------------
172.16.10.14    disabled disabled 2-1000
Console> (enable)
```

5000 Series

The `show vtp statistics` command shows a summary of VTP advertisement messages sent and received. It also will show configuration errors if detected:

```
Console> (enable) show vtp statistics
VTP statistics:
summary advts received          0
subset  advts received          0
request advts received          0
summary advts transmitted       5
subset  advts transmitted       2
request advts transmitted       0
```

```
No of config revision errors    0
No of config digest errors      0
VTP pruning statistics:
Trunk     Join Transmitted  Join Received  Summary advts received from
                                           non-pruning-capable device
--------  ----------------  -------------  --------------------------
 2/12     0                 0              0
Console> (enable)
```

1900 Series

Here is an example of the same command run on the 1900 switch:

```
1900EN#show vtp statistics
          Receive Statistics                    Transmit Statistics
 -------------------------------  -----------------------------------
 Summary Adverts                0  Summary Adverts             0
 Subset Adverts                 0  Subset Adverts              0
 Advert Requests                0  Advert Requests            56
 Configuration Errors:
   Revision Errors              0
   Digest Errors                0
 VTP Pruning Statistics:
 Port    Join Received    Join Transmitted  Summary Adverts received
                                            with no pruning support
 ----    -------------    ----------------  -----------------------
 A       0                0                 0
 B       0                0                 0
 1900EN#
```

The 2900/3500 get the same output with the `show vtp counters` command.

Adding to a VTP Domain

You need to be careful when adding a new switch into an existing domain. If a switch is inserted into the domain and has incorrect VLAN information, the result could be a VTP database propagated throughout the internetwork with false information.

Before inserting a switch, make sure that you follow these three steps:

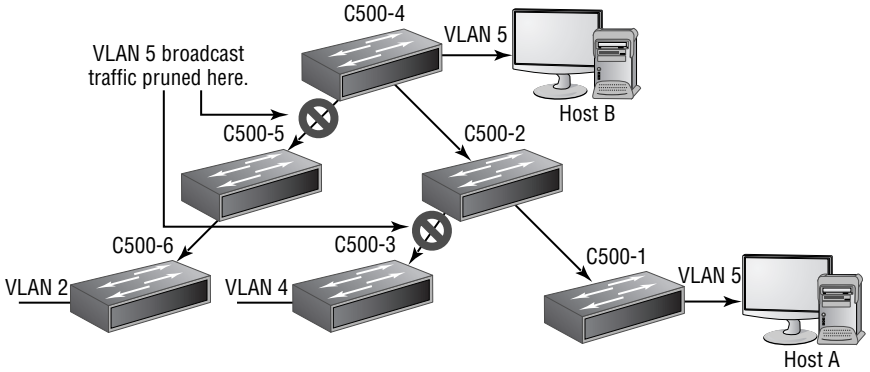
1. Perform a `clear config all` to remove any existing VLAN configuration on a set-based switch. On the 1900, use the `delete nvram` command and erase the startup-config on the 2900/3500.
2. Power-cycle the switch to clear the VTP NVRAM.
3. Configure the switch to perform the mode of VTP that it will participate in. Cisco's rule of thumb is that you create several VTP servers in the domain, with all the other switches set to client mode.

VTP Pruning

To preserve bandwidth, you can configure the VTP to reduce the number of broadcasts, multicasts, and other unicast packets. This is called *VTP pruning*. VTP restricts broadcasts to only trunk links that must have the information. If a trunk link does not need the broadcasts, the information is not sent. VTP pruning is disabled by default on all switches.

Figure 3.8 shows that if a switch does not have any ports configured for VLAN 5 and a broadcast is sent throughout VLAN 5, the broadcast would not traverse the trunk link going to the switch without any VLAN 5 members.

FIGURE 3.8 VTP pruning



VTP pruning limits VLAN traffic to those links that support the VLAN.

Enabling pruning on a VTP server enables pruning for the entire domain, and by default, VLANs 2 through 1005 are eligible for pruning. VLAN 1 can never prune.

Use the following command to set VLANs to be eligible for pruning:

```
Console> (enable) set vtp pruneeligible ?
Usage: set vtp [domain <name>] [mode <mode>]
[passwd <passwd>] [pruning <enable|disable>]
[v2 <enable|disable> (mode = client|server|transparent
        Use passwd '0' to clear vtp password)
Usage: set vtp pruneeligible <vlans>
       (vlans = 2..1000
        An example of vlans is 2-10,1000)
Console> (enable) set vtp pruneeligible 2
Vlans 2-1000 eligible for pruning on this device.
VTP domain Globalnet modified.
```

Notice, once again, that when you enable a VLAN for pruning, by default, it configures all the VLANs. Use the following command to clear the unwanted VLANs:

```
Console> (enable) clear vtp pruneeligible 3-1005
Vlans 1,3-1005 will not be pruned on this device.
VTP domain Globalnet modified.
Console> (enable)
```

To verify the pruned state of a trunk port, use the `show trunk` command.

To set pruning on the 2900/3500, head into VLAN database mode. The command `vtp pruning` enables the pruning process while the command `switchport trunk pruning vlan remove` *`vlan-id`* is used to remove VLANs from the list of pruning-eligible VLANs:

```
2900XL(vlan)# vtp pruning
2900XL(vlan)# exit
2900XL# configure terminal
2900XL(config)# interface fa 0/10
2900XL(config-if)# switchport trunk pruning vlan remove 2-5,10
```

Summary

In this chapter, you learned how to break up broadcast domains in layer 2 switched networks: by creating virtual LANs. When you create VLANs, you are able to create smaller broadcast domains within a switch by assigning different ports in the switch to different subnetworks.

We showed you how to configure VLANs on both set-based and IOS-based switches. It is important to understand how to configure VLANs on both types as well as how to set the configuration of VLANs on individual interfaces.

We also showed you how to configure trunking between links on an access layer switch and a distribution layer switch, where trunking enables you to send information about multiple VLANs down one link, in contrast to an access link that can send information about only one VLAN.

The chapter ended with a discussion of VLAN Trunk Protocol (VTP), which really doesn't have much to do with trunking except that VTP information is sent down trunk links only. VTP is used to update all switches in the internetwork with VLAN information.

Exam Essentials

Understand what a trunk is. Know that a trunk is a link between a switch and another device that allows the traffic from multiple VLANs to cross it. When a packet crosses a trunk, it retains any ISL or `dot1q` information detailing what VLAN the packet belongs to.

Understand the difference between ISL and 802.1q. ISL is a Cisco proprietary VLAN format, whereas 802.1q is a standard. Network cards are made to support both types, which enables PCs and servers to receive and send VLAN-specific traffic. Know that the big difference between the two is that ISL encapsulates the original packet in a new 30-byte frame, whereas 802.1q just adds 4 bytes of header and trailer information.

Know the configuration differences between the different switches. The 5000 series uses the standard `set` commands, whereas the 1900 and 2900/3500 use IOS-type commands. The 2900/3500 switches configure VLAN and VTP configurations in VLAN database configuration mode, as opposed to the global configuration mode that the 1900 uses.

Understand when a VLAN should be used. Know that a VLAN is used to separate broadcast traffic. If a switch has ports 1–10 in VLAN 1 and ports 11–20 in VLAN 2, a packet arriving from a device connected to port 5 can't talk to a device connected to port 15 without some sort of routing engine participating. Know that VLANs can be used for security as well as to break up existing large broadcast domains.

Key Terms

Before you take the exam, be sure you're familiar with the following terms:

access link
dynamic VLAN
end-to-end VLAN
flat network
frame tagging
local VLAN
static VLAN
switch-fabric
trunk link
VLAN database
VTP pruning

Written Lab

Write the answers to the following questions:

1. What commands will create VLAN 35 on a 5000 series switch named Sales using ports 5 through 9 on card 3?
2. What command will set the VTP domain name to Acme and the switch to a VTP client on a set-based switch?
3. What command would you use on a 1900 switch and a set-based switch to see the configured VLANs?
4. What type of frame tagging places a VLAN identifier into the frame header?
5. What type of frame tagging encapsulates the frame with VLAN information?
6. What protocol handles the negotiation of trunk links?
7. How do you configure trunking on a set-based switch, port 1/1, using ISL tagging?
8. What command would you use to clear VLANs 10 through 14 from the trunk link 1/1 on a 5000 switch?

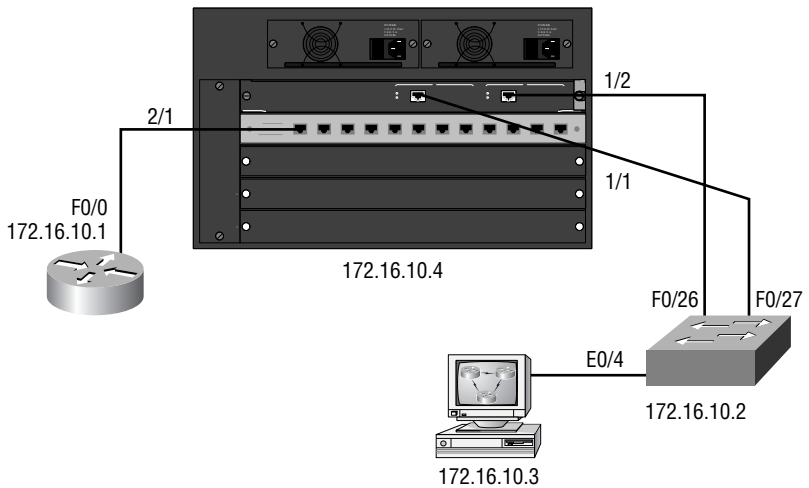
9. What command will display the VTP statistics on a 5000 series switch?

10. If the VTP domain is already configured, how would you set a VTP password on a 5000 switch to "cisco"?

Hands-On Lab

In this lab, you will continue to configure the network used in the hands-on lab in Chapter 2. This lab will configure the network with VTP domain information and trunking. Figure 3.9 is a review of the lab we are configuring.

FIGURE 3.9 Switched internetwork for hands-on lab



1. Start with the 5000 series switch and configure the VTP domain as Routersim:

   ```
   set vtp domain Routersim
   ```

2. The default VTP mode is server, which is what you want the 5000 series switch to be. The 1900 switch will be a VTP client. Create three VLANs on the 5000 series switch:

   - VLAN 1 is the default; it will be used for management.
   - VLAN 2 will be the Sales VLAN and will use IP network 172.16.20.0. Port 2 on card 2 will be used.

- VLAN 3 will be the Mrkt VLAN and will use IP network 172.16.30.0. Ports 3 and 4 on card 2 will be used.
- VLAN 4 will be the Accnt VLAN and will use IP network 172.16.40.0. Ports 5 and 6 on card 2 will be used.

Here is the configuration:

```
Set vlan 2 name Sales
Set vlan 3 name Mrkt
Set vlan 4 name Accnt
Set vlan 2 2/2
Set vlan 3 2/3-4
Set vlan 4 2/5-6
```

3. Type in the commands to verify the VLAN configuration and VTP configuration:

```
show vtp
show vlan
```

4. Because you want VLAN information to be propagated to the 1900 switch, a trunk link needs to be configured between both the switches. Set the trunk link on port 1/1 and port 1/2 of the 5000 switch. These are your connections to the access layer switch (1900A). Remember that the 1900 switch can use only ISL trunking, so the 5000 needs to be configured with ISL trunking:

```
set trunk 1/1 on isl
set trunk 1/2 on isl
```

5. Type the command to view the trunk link:

```
show trunk 1/1
show trunk 1/2
```

6. Connect to the 1900 switch and set the VTP domain name:

```
configure terminal
vtp domain Routersim
```

7. Set the VTP mode to client:

```
vtp mode client
```

8. Before any VLAN information will be propagated through the internetwork, you need to make both interface f0/26 and f0/27 a trunk link:

```
Configure terminal
```

```
Interface f0/27
Trunk on
Interface f0/26
Trunk on
```

9. Verify that the trunk link is working:

```
show trunk a
show trunk b
```

10. Ping the 5000 series switch:

```
ping 172.16.10.4
```

11. Now verify that you have received VLAN information from the 5000 series switch:

```
show vlan
```

You should see all configured VLANs.

12. After you have the trunk link working and have received the VLAN information, you can assign VLANs to individual ports on the switch. Assign ports 1 and 2 to VLAN 2, assign ports 3 and 4 to VLAN 3, and assign ports 5 and 6 to VLAN 4:

```
Configure terminal
Interface e0/1
Vlan-membership static 2
Interface e0/2
Vlan-membership static 2
Interface e0/3
Vlan-membership static 3
Interface e0/5
Vlan-membership static 4
Interface e0/6
Vlan-membership static 4
```

13. Verify the configuration:

```
Show vlan-membership
Show vlan
```

Review Questions

1. Which of the following is a true statement regarding VLANs?
   - **A.** You must have at least two VLANs defined in every Cisco switched network.
   - **B.** All VLANs are configured at the access layer and extend to the distribution layer.
   - **C.** VLANs should extend past the distribution switch on to the core.
   - **D.** VLANs should not extend past the distribution switch on to the core.

2. If you want to configure ports 3/1-12 to be part of VLAN 3, which command is valid on a set-based switch?
   - **A.** `console> (enable) set vlan 3 2/1, 2/2, 2/3, etc.`
   - **B.** `console> (config) vlan 3 set port  3/1-12`
   - **C.** `console> (enable) set vlan 3 3/1-12`
   - **D.** `console>  set vlan 3 3/1-12`
   - **E.** `console> vlan membership 3 3/1-12`

3. What are the two ways that an administrator can configure VLAN memberships? (Choose all that apply.)
   - **A.** DHCP server
   - **B.** Static
   - **C.** Dynamic
   - **D.** VTP database

4. How are local VLANs configured?
   - **A.** By geographic location
   - **B.** By function
   - **C.** By application
   - **D.** Doesn't matter

5. If you want to verify the VTP-configured information on a set-based switch, which of the following commands would you use?

   A. `sh vtp domain`

   B. `sh domain`

   C. `set vtp domain output`

   D. `sho vtp info`

6. What size frames are possible with ISL and 802.1q frames? (Choose all that apply.)

   A. 1518

   B. 1522

   C. 4202

   D. 8190

7. Which of the following is true regarding the Canonical Format Indicator (CFI)? (Choose all that apply.)

   A. It is a 1-bit field that is always a 0 if running an 802.3 frame.

   B. The CFI field was originally designed to be used for Token Ring VLANs, but it was never implemented except for some proprietary Token Ring LANs.

   C. It is not used on any switch but the 5000 series.

   D. It is used with FDDI trunk ports only.

8. Regarding 802.1q, what is the TPID EtherType field always set to?

   A. 17

   B. 6

   C. 0x81-00

   D. 0x2102

9. How are dynamic VLANs configured?

   A. Statically

   B. By an administrator

   C. By using a DHCP server

   D. By using VLAN Management Policy Server

10. If you want to completely clear all configurations on a 1900 switch, what two commands must you type in? (Choose all that apply.)

    A. `clear config`

    B. `delete nvram`

    C. `delete vtp`

    D. `delete start`

11. What do VTP switches advertise on their trunk ports? (Choose all that apply.)

    A. Management domain name

    B. Configuration revision number

    C. VLAN identifiers configured on Cisco routers

    D. VLANs the switch knows about

    E. Parameters for each VLAN

    F. CDP information

12. Which of the following is true regarding VTP?

    A. VTP pruning is enabled by default on all switches.

    B. VTP pruning is disabled by default on all switches.

    C. You can run VTP pruning only on 5000 or higher switches.

    D. VTP pruning is configured on all switches by default if it is configured on just one switch.

13. Which of the following Cisco standards encapsulates a frame and even adds a new FCS field?

A. ISL

B. 802.1q

C. 802.3z

D. 802.3u

14. What does setting the VTP mode to transparent accomplish?

A. Transparent mode will only forward messages and advertisements, not add them to their own database.

B. Transparent mode will forward messages and advertisements and add them to their own database.

C. Transparent mode will not forward messages and advertisements.

D. Transparent mode makes a switch dynamically secure.

15. Which of the following IEEE standards actually inserts a field into a frame to identify VLANs on a trunk link?

A. ISL

B. 802.3z

C. 802.1q

D. 802.3u

16. How long can a VTP domain name be on a 5000 series switch?

A. The VTP name can be up to 23 characters.

B. The VTP name can be up to 32 characters.

C. The VTP name can be up to 48 characters.

D. The VTP name can be up to 80 characters.

17. If you want to view the trunk status on port 27 of a 1900 switch, which command would you use?

A. `show port 27`

B. `show trunk`

C. `show trunk B`

D. `show trunk f0/27`

E. `show trunk e0/27`

18. VTP provides which of the following benefits to a switched network? (Choose all that apply.)

    A. Multiple broadcast domains in VLAN 1

    B. Management of all switches and routers in an internetwork

    C. Consistent configuration of VLANs across all switches in the network

    D. Allowing VLANs to be trunked over mixed networks, for example, Ethernet to ATM LANE or FDDI

    E. Tracking and monitoring of VLANs accurately

    F. Dynamic reporting of added VLANs to all switches

    G. Plug-and-play VLAN adding

    H. Plug-and-play configuration

19. Which of the following is true regarding VTP?

    A. Changing the VTP version on one switch changes all switches in a domain.

    B. If you change the VTP version on one switch, you must change the version on all switches.

    C. VTP is on by default with a domain name of Cisco on all Cisco switches.

    D. All switches are VTP clients by default.

20. Which of the following is true regarding trunk links?

    A. They are configured by default on all switch ports.

    B. They work only with a type of Ethernet network and not with Token Ring, FDDI, or ATM.

    C. You can set trunk links on any 10Mbps, 100Mbps, and 1000Mbps ports.

    D. You must clear the unwanted VLANs by hand.

Answers to Written Lab

1. `set vlan 35 name Sales`
   `set vlan 35 3/5-9`
2. `set vtp domain Acme mode client`
3. `show vlan`
4. 802.1q
5. ISL
6. Dynamic Trunk Protocol (DTP)
7. `set trunk 1/1 on isl`
8. `clear trunk 1/1 10-14`
9. `show vtp statistics`
10. `set vtp passwd cisco`

Answers to Review Questions

1. D. VLANs should not pass through the distribution layer. The distribution layer devices should route between VLANs.
2. C. The set-based switches can configure multiple ports to be part of a VLAN at the same time. The command is `set vlan` *`vlan# slot/ports`*.
3. B, C. Static VLANs are set port by port on each interface or port. Dynamic VLANs can be assigned to devices via a server.
4. A. Local VLANs are created by location—for example, an access closet.
5. A. The command `show vtp domain` will provide the switch's VTP mode and the domain name.
6. A, B. ISL encapsulates frames with another frame encapsulation type. This means that a data frame can extend past the regular frame size of 1518 bytes up to 1548 bytes, whereas 802.1q frames can be up to 1522 bytes.
7. A, B. The CFI field is not used often, and only in proprietary Token Ring LANs. It will always be a 0 unless a programmer specifically programs it to be different.
8. C. The EtherType file will always be a 0x81-00 when 802.1q frame tagging is used.
9. D. A VLAN Management Policy Server (VMPS) must be configured with the hardware addresses of all devices on your internetwork. Then the server is allowed to hand out VLAN assignments configured by the administrator into the VMPS database.
10. B, C. The command `delete nvram` deletes the configuration of the switch but not the VTP configuration. To delete the VTP information configured on the switch, use the `delete vtp` command.
11. A, B, D, E. VLAN Trunk Protocol is used to update switches within a domain about configured VLANs. This includes the management domain name and configuration revision number so that receiving switches know if new VLAN information (including configured parameters) has been added to the VTP database and all the VLANs the switch knows about.

12. B. VTP pruning stops VLAN information from traversing a trunk link if it would be discarded on the remote end because no VLANs are configured on the switch.

13. A. Inter-Switch Link (ISL) encapsulates a new header and trailer to an existing data frame.

14. A. VTP transparent switches do not update their VTP database with VLAN information received on trunk links. However, they will forward these updates.

15. C. 802.1q does not encapsulate a data frame as ISL does. Instead, it puts a new field into the existing frame to identify the VLAN that the packet belongs to.

16. B. VTP domain names can be up to 32 characters and must be the same on all switches with which you want to share VLAN information.

17. C. The 1900 switches use port A to reference interface 0/26 and B to reference interface 0/27.

18. B, C, D, E, F, G, H. VTP does not have anything to do with breaking up or configuring broadcast domains. All answers except A are correct.

19. A. If you change the VTP version on one switch, all other switches will be changed automatically if they support the new version.

20. D. Trunk links, by default, are assigned to forward all VLANs. You must delete these by hand if you don't want all VLANs to be sent down a trunk link.

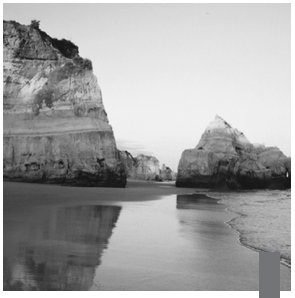
Chapter

4

Layer 2 Switching and the Spanning Tree Protocol (STP)

THE CCNP EXAM TOPICS COVERED IN THIS CHAPTER INCLUDE THE FOLLOWING:

- ✓ **Describe Spanning Tree**
- ✓ **Configure the switch devices to improve Spanning Tree Convergence in the network**
- ✓ **Provide physical connectivity between two devices within a switch block**
- ✓ **Provide connectivity from an end user station to an access layer device**



In this chapter, we'll explore the three distinct functions of layer 2 switching: address filtering, forward/filter decision-making, and loop avoidance. We will probe the issue of loop avoidance in depth and discuss how the Spanning Tree Protocol (STP) works to stop network loops from occurring on your layer 2 network.

It is very important to have a clear understanding of the Spanning Tree Protocol. This chapter will continue the discussion of layer 2 switching started in Chapter 1, "The Campus Network." We'll discuss how network loops occur in a layer 2 network and then provide an introduction to STP, including the different components of STP and how to configure STP on layer 2 switched networks. By the end of this chapter, you will know how to use STP to stop network loops, broadcast storms, and multiple frame copies. In Chapter 5, "Using Spanning Tree with VLANs," we'll continue discussing STP and provide the more complex and advanced configurations used with it.

It is typical these days to create a network with redundant links. This provides consistent network availability when a network outage occurs on one link. However, loop avoidance is needed, and STP provides this function. It is possible to load-balance over the redundant links as well; we'll cover load-balancing in Chapter 5.

Layer 2 LAN Switching

You can think of layer 2 switches as bridges with more ports. Remember from Chapter 1 that layer 2 switching is hardware based, which means it uses the Media Access Control (MAC) address from the hosts' network interface cards (NICs) to filter the network. You should also remember how

switches use application-specific integrated circuits (ASICs) to build and maintain filter tables.

However, there are some differences between bridges and switches that you should be aware of. This section outlines those differences and then discusses the three functions of layer 2 switching.

Comparing Bridges to Switches

The following list describes the differences between bridges and switches. Table 4.1 provides an overview of that comparison.

- Bridges are considered software based. Switches are hardware based because they use an ASICs chip to help make filtering decisions.
- Bridges can have only one spanning-tree instance per bridge. Switches can have many. (Spanning tree is covered later in this chapter.)
- Bridges can have up to only 16 ports. A switch can have hundreds.

TABLE 4.1 Comparison of Bridges and Switches

	Bridges	Switches
Filtering	Software based	Hardware based
Spanning tree numbers	One spanning tree instance	Many spanning tree instances
Ports	16 ports maximum	Hundreds of ports available

You probably won't go out and buy a bridge, but it's important to understand how bridges are designed and maintained because layer 2 switches function in a similar fashion.

Three Switch Functions at Layer 2

There are three distinct functions of layer 2 switching:

Address learning Layer 2 switches and bridges remember the source hardware address of each frame received on an interface and enter it into a MAC database.

The forwarding and filtering decision When a frame is received on an interface, the switch looks at the destination hardware address and looks up the exit interface in the MAC database.

Loop avoidance If multiple connections between switches are created for redundancy, network loops can occur. STP is used to stop network loops and allow redundancy.

These functions of the layer 2 switch—address learning, forward and filtering decisions, and loop avoidance—are discussed in detail next.

Address Learning

The layer 2 switch is responsible for *address learning*. When a switch is powered on, the MAC filtering table is empty. When a device transmits and a frame is received on an interface, the switch takes the source address and places it in the MAC filter table. It remembers what interface the device is located on. The switch has no choice but to flood the network with this frame because it has no idea where the destination device is located.

If a device answers and sends a frame back, then the switch will take the source address from that frame, place the MAC address in the database, and associate this address with the interface on which the frame was received. Because the switch now has two MAC addresses in the filtering table, the devices can now make a point-to-point connection and the frames will be forwarded only between the two devices. This is what makes layer 2 switches better than hubs. In a hub network, all frames are forwarded out all ports every time.

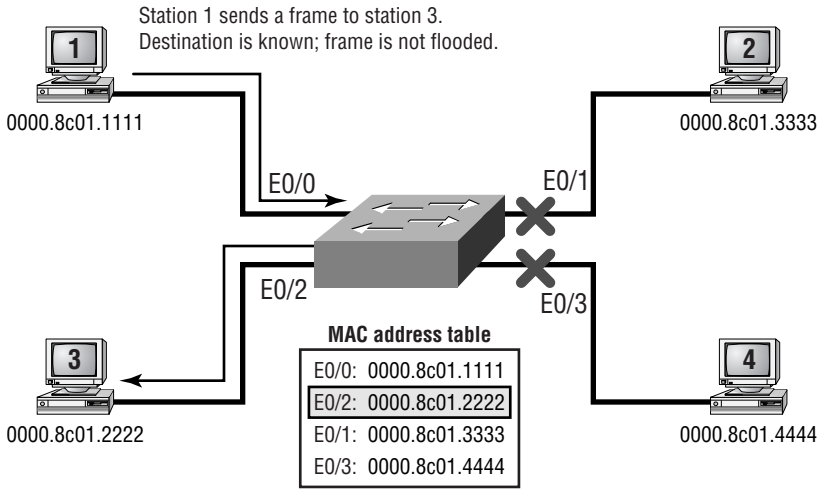
Figure 4.1 shows the procedures for building a MAC database.

In the figure, four hosts are attached to a switch. The switch has nothing in the MAC address table when it is powered on. The figure shows the switch's MAC filter table after each device has communicated with the switch. The following steps show how the table is propagated:

1. Station 1 sends a frame to station 3. Station 1 has a MAC address of 0000.8c01.1111. Station 3 has a MAC address of 0000.8c01.2222.
2. The switch receives the frame on Ethernet interface 0/0, examines the source and destination MAC addresses, and places the source address in the MAC address table.
3. Because the destination address is not in the MAC database, the frame is forwarded out all interfaces.

4. Station 3 receives the frame and responds to station 1. The switch receives this frame on interface E0/2 and places the source hardware address in the MAC database.
5. Station 1 and station 3 can now make a point-to-point connection, and only the two devices will receive the frames. Stations 2 and 4 will not see the frames.

FIGURE 4.1 How switches learn hosts' locations



If the two devices do not communicate with the switch again within a certain time limit, the switch will flush the entries from the database to keep the database as current as possible.

Forwarding/Filtering Decision

The layer 2 switch also uses the MAC filter table to both forward and filter frames received on the switch. This is called the *forwarding and filtering decision*. When a frame arrives at a switch interface, the destination hardware address is compared to the forward/filter MAC database. If the destination hardware address is known and listed in the database, the frame is sent out only on the correct exit interface. The switch does not transmit the frame out of any interface except for the destination interface. This preserves bandwidth on the other network segments. This is called frame filtering.

If the destination hardware address is not listed in the MAC database, the frame is flooded out all active interfaces except the interface on which

the frame was received. If a device answers, the MAC database is updated with the device location (interface).

Broadcast and Multicast Frames

Remember, the layer 2 switches forward all broadcasts by default. The forwarding/filtering decision is a bit different because broadcast packets are designed to go to every device that is listening and multicasts are for every device listening for a particular type of packet. Whereas the MAC address of a given device is normally determined by the MAC address that is burned into the network card, broadcasts and multicasts need some way of targeting multiple devices.

A broadcast targets every device on the subnet by setting all the bits in the destination MAC address to 1. Thus, the 48-bit destination MAC address, which uses hexadecimal notation, looks like FFFF.FFFF.FFFF. Every device is trained to look for frames destined to its MAC address and frames destined to every MAC address. An example of a packet that needs to be addressed to every device that can hear is an ARP request.

A multicast is a slightly different animal in that it wants to go to every device that is participating in a certain process. If five routers are using the EIGRP routing protocol and one sends out an update, it sends the update to the multicast IP address 224.0.0.10. Each router is listening for any packet with that IP address as its destination, but devices don't look at the IP address when the frame is received—they look at the MAC address. There is a special format that MAC addresses follow when the packet is part of a multicast process. This process is covered in detail in Chapter 9, "Configuring Multicast."

When a switch receives these types of frames, the frames are then quickly flooded out all active ports of the switch by default. To have broadcasts and multicasts forwarded out only a limited number of administratively assigned ports, you create virtual LANs, which were discussed in Chapter 3, "VLANs."

Loop Avoidance

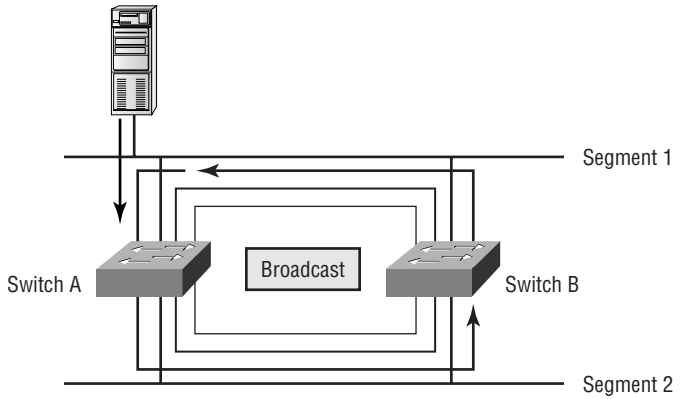
Finally, the layer 2 switch is responsible for *loop avoidance*. It's a good idea to use redundant links between switches. They help stop complete network failures if one link fails. Even though redundant links are extremely helpful, they cause more problems than they solve. In this section, we'll discuss some of the most serious problems:

- Broadcast storms
- Multiple frame copies
- Multiple loops

Broadcast Storms

If no loop avoidance schemes are put in place, the switches will flood broadcasts endlessly throughout the internetwork. This is sometimes referred to as a broadcast storm. Figure 4.2 shows how a broadcast might be propagated throughout the network.

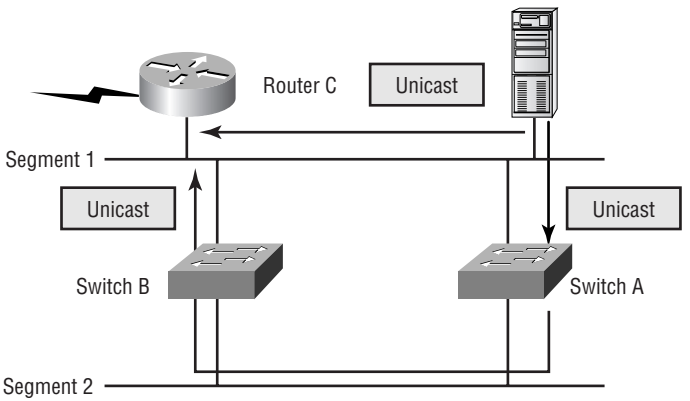
FIGURE 4.2 Broadcast storms



Multiple Frame Copies

Another problem is that a device can receive multiple copies of the same frame because the frame can arrive from different segments at the same time. Figure 4.3 shows how multiple frames can arrive from multiple segments simultaneously.

FIGURE 4.3 Multiple frame copies



The MAC address filter table will be confused about where a device is located because the switch can receive the frame from more than one link. It is possible that the switch can't forward a frame because it is constantly updating the MAC filter table with source hardware address locations. This is called thrashing the MAC table.

Multiple Loops

One of the biggest problems is multiple loops generating throughout an internetwork. This means that loops can occur within other loops. If a broadcast storm were to then occur, the network would not be able to perform packet switching.

To solve these three problems, the Spanning Tree Protocol was developed.

Spanning Tree Operation

In layer 3 devices, which are typically routers, the routing protocols are responsible for making sure routing loops do not occur in the network. What is used to make sure network loops do not occur in layer 2 switched networks? That is the job of the *Spanning Tree Protocol (STP)*.

Digital Equipment Corporation (DEC), which was purchased by Compaq before the merger with Hewlett-Packard, was the original creator of STP. The IEEE created its version of STP, called 802.1d, using the DEC version as the basis. By default, all Cisco switches run the IEEE 802.1d version of STP, which is not compatible with the DEC version.

The big difference between the two types of STP from an administrative point of view is the range of values that can be set for the priority. A bridge using DEC STP can be set as high as 255, and a switch using IEEE STP can be set as high as 65535. If the two could be used together, a bridge set as a very low priority on DEC would stand a good chance of becoming the root in an IEEE STP network.

The big picture is that STP stops network loops from occurring on your layer 2 network (bridges or switches). STP is constantly monitoring the network to find all links and to make sure loops do not occur by shutting down redundant links.

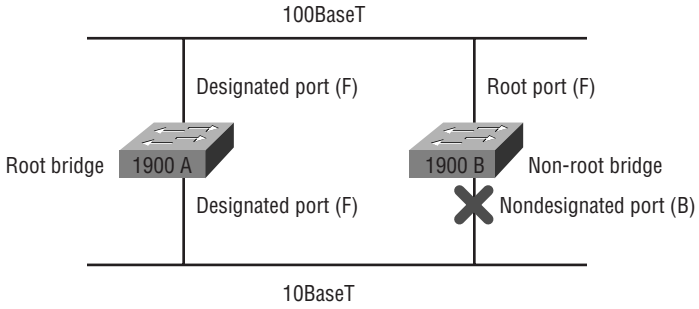
The Spanning Tree Protocol executes an algorithm called the spanning-tree algorithm. This algorithm chooses a reference point in the network and calculates the redundant paths to that reference point. After it finds all the

links in the network, the spanning-tree algorithm chooses one path on which to forward frames and shuts down the other redundant links to stop any network loops from occurring in the network. It does this by electing a root bridge that will decide on the network topology.

There can be only one *root bridge* in any given network. The root bridge ports are called designated ports, and designated ports operate in what is called forwarding state. Forwarding state ports send and receive traffic.

If you have other switches in your network, as shown in Figure 4.4, they are called non-root bridges. However, the port that has the lowest cost to the root bridge is called a root port and sends and receives traffic. The cost is determined by the bandwidth of a link.

FIGURE 4.4 Spanning tree operations



Ports that forward traffic away from the root bridge are called the *designated ports*. Because the root can forward traffic only away from itself, all its ports are designated ports. The other port or ports on the bridge are considered *nondesignated ports* and will not send or receive traffic. This is called blocking mode.

This section will cover exactly how a group of switches will determine the best path throughout the network and how you can modify the results. This section will cover port selection and link cost values as well as the different spanning tree states a particular port might be in.

Selecting the Best Path

Using spanning tree, a group of switches will determine the best path from any point A to any point B. To do this, all the switches need to communicate and each switch needs to know what the network looks like. In order to know what links should be dynamically disabled, a root bridge must be selected and each switch needs to determine the type of each port.

Selecting the Root Bridge

Switches or bridges running STP exchange information with what are called *Bridge Protocol Data Units (BPDUs)*. BPDUs are used to send configuration messages by using multicast frames. The bridge ID of each device is sent to other devices using BPDUs.

The *bridge ID* is used to determine the root bridge in the network and to determine the root port. The bridge ID is 8 bytes long and includes the priority and the MAC address of the device. The priority on all devices running the IEEE STP version is 32768 by default. The lower the bridge ID, the more likely a device is to become the root bridge.

To determine the root bridge, the switches in the network will compare the bridge IDs they receive via the BPDUs. Whichever switch has the lowest bridge ID will become the root bridge. If two switches or bridges have the same priority value, then the MAC address is used to determine which has the lowest ID.

For example, if two switches, A and B, both use the default priority of 32768, the MAC address will be used. If switch A's MAC address is 0000.0c00.1111 and switch B's MAC address is 0000.0c00.2222, switch A would become the root bridge.

Because each switch comes with a burned-in MAC address, if the switches use the default priority, then the one with the lowest MAC address will become the root bridge. This means that this device will have a large number of packets passing through it. If you have a 6509 and have spent lots of money on the fabric upgrades to a 256Gb backplane, the last thing you want is for a 1900 in a closet to become the root bridge. For this reason, it is strongly recommended that you lower the number on the priority for core switches. Chapter 5 gives more information on dealing with designs.

The following network analyzer output shows a BPDU broadcasted on a network. BPDUs are sent out every two seconds by default. That might seem like a lot of overhead, but remember that this is only a layer 2 frame, with no layer 3 information in the packet:

```
Flags:          0x80  802.3
Status:         0x00
Packet Length:64
Timestamp:      19:33:18.726314 02/28/2002
```

```
802.3 Header
  Destination:  01:80:c2:00:00:00
  Source:       00:b0:64:75:6b:c3
  LLC Length:   38
802.2 Logical Link Control (LLC) Header
  Dest. SAP:    0x42  802.1 Bridge Spanning Tree
  Source SAP:   0x42  802.1 Bridge Spanning Tree
  Command:      0x03  Unnumbered Information
802.1 - Bridge Spanning Tree
  Protocol Identifier:  0
  Protocol Version ID:  0
  Message Type:         0  Configuration Message
  Flags:                %00000000
  Root Priority/ID:     0x8000  /  00:b0:64:75:6b:c0
  Cost Of Path To Root: 0x00000000  (0)
  Bridge Priority/ID:   0x8000  / 00:b0:64:75:6b:c0
  Port Priority/ID:     0x80  /  0x03
  Message Age:                        0/256 seconds
   (exactly 0seconds)
  Maximum Age:                        5120/256 seconds
   (exactly 20seconds)
  Hello Time:                        512/256 seconds
   (exactly 2seconds)
  Forward Delay:                       3840/256 seconds
   (exactly 15seconds)
Extra bytes (Padding):
  ........             00 00 00 00 00 00 00 00
Frame Check Sequence:  0x2e006400
```

Notice the cost of path to root. It is zero because this switch is actually the root bridge. We'll discuss path costs in more detail in the upcoming section, "Selecting the Designated Port."

The preceding network analyzer output also shows the BPDU timers, which are used to prevent bridging loops because the timers determine how long it will take the spanning tree to converge after a failure.

BPDUs are susceptible to propagation delays, which happen because of packet length, switch processing, bandwidth, and utilization problems. This can create an unstable network because temporary loops might occur in the network when BPDUs are not received on time to the remote switches in the network. The STP uses timers to force ports to wait for the correct topology information.

As you can see in the output, the hello time is exactly 2 seconds, the maximum age is exactly 20 seconds, and the forward delay is exactly 15 seconds.

When a switch first boots up, the only MAC address it knows is its own, so it advertises itself as the root. As it collects BPDUs, it will acknowledge another device as the root, if necessary. When a switch receives a BPDU advertising a device as root, with a better bridge ID than the current root is using, the switch caches this information and waits. It will wait the duration of the MaxAge timer before using the new root, allowing other switches in the network to also receive the BPDU. This reduces the possibility of loops.

Selecting the Root Port

After you have selected the root bridge, all switches must become buddies with the root bridge. Each switch listens to BPDUs on all active ports, and if more than one BPDU is received, the switch knows it has a redundant link to the root bridge. The switch has to determine which port will become the root port and which port will be put into blocking state.

To determine the port that will be used to communicate with the root bridge, the path cost is determined. The path cost is an accumulated total cost based on the bandwidth of the links. Table 4.2 shows the typical costs associated with the different Ethernet networks.

TABLE 4.2 STP Link Cost

Speed	New IEEE Cost	Original IEEE Cost
10Gbps	2	1
1Gbps	4	1
100Mbps	19	10
10Mbps	100	100

The IEEE 802.1d specification has recently been revised to handle the new higher-speed links, hence the different costs shown in Table 4.2.

Included in the BPDUs that a switch sends out is the cost of getting a frame to the root bridge. A neighboring device will receive this information, add the cost of the link the BPDU arrived on, and that becomes the cost for the neighboring device. For example, switch A sends out a BPDU to switch B saying that A can reach the root with a path cost of 38. The BPDU travels

across a gigabit link between switch A and B. B receives the BPDU giving the cost of 38 and adds the cost of the link the BPDU arrived on, which is 4. Switch B knows that it can reach the root by sending frames through switch A with a total path cost of 42.

After the cost is determined for all links to the root bridge, the switch will decide which port has the lowest cost. The lowest-cost port is put into forwarding mode, and the other ports are placed in blocking mode. If there are equal-cost paths, the port with the lowest port ID will be put into the forwarding state. In the previous example, if switch B had two paths to the root, both with a cost of 42, the switch needs some other way of figuring out which single path will be used. If switch A is accessed via gigabit port 0/3 and switch C is accessed via gigabit port 0/7, switch B will send frames via switch A because it is attached to the lower numerical port number.

Selecting the Designated Port

A designated port is one that is active and forwarding traffic, but doesn't lead to the root. Often, a designated port on one switch connects to the root port on another switch, but it doesn't have to. Because the root bridge doesn't have any ports that lead to itself and because its ports are never dynamically turned off, all its ports are labeled as designated ports.

The selection of a designated port is fairly easy. If there are two switches that have equal-cost paths to get to the root and are connected to each other, there must be some way of resolving the topological loop that exists. The switches simply examine the bridge IDs, and whichever device has the lower bridge ID is the one that will be responsible for forwarding traffic from that segment. Figure 4.4, shown earlier, illustrates this point.

Spanning Tree Port States

The ports on a bridge or switch running the STP can transition through four states:

Blocking Won't forward frames; listens to BPDUs. All ports are in blocking state by default when the switch is powered on.

Listening Listens to BPDUs to make sure no loops occur on the network before passing data frames.

Learning Learns MAC addresses and builds a filter table, but does not forward frames.

Forwarding Bridge port is able to send and receive data. A port will never be placed in forwarding state unless there are no redundant links or the port determines that it has the best path to the root bridge.

An administrator can put a port in disabled state, or if a failure with the port occurs, the switch will put it into disabled state.

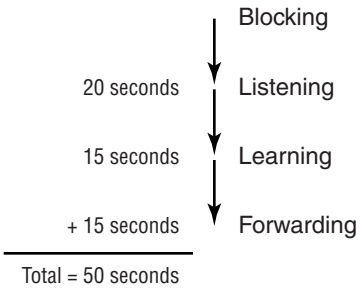
Typically, switch ports are in either blocking or forwarding state. A forwarding port is a port that has been determined to have the lowest cost to the root bridge. However, if the network has a topology change because of a failed link, or the administrator adds a new switch to the network, the ports on a switch will be in listening and learning states.

Blocking ports are used to prevent network loops. After a switch determines the best path to the root bridge, all other ports may be placed in the blocking state. Blocked ports will still receive BPDUs.

If a switch determines that a blocked port should now be the designated port, it will go to listening state. It will check all BPDUs heard to make sure that it won't create a loop after the port goes to forwarding state.

Figure 4.5 shows the default STP timers and their operation within STP.

FIGURE 4.5 STP default timers



Notice the time from blocking to forwarding. Blocking to listening is 20 seconds. Listening to learning is another 15 seconds. Learning to forwarding is 15 seconds, for a total of 50 seconds. However, the switch could go to disabled if the port is administratively shut down or the port has a failure.

Convergence

Convergence occurs when bridges and switches have transitioned to either the forwarding or blocking state. No data is forwarded during this time. Convergence is important in making sure that all devices have the same database.

The problem with convergence is the time it takes for all devices to update. Before data can start to be forwarded, all devices must be updated. The time

it usually takes to go from blocking to forwarding state is 50 seconds. Changing the default STP timers is not recommended, but the timers can be adjusted if they need to be. The time it takes to transition a port from the listening state to the learning state or from the learning state to the forwarding state is called the forward delay.

Real World Scenario

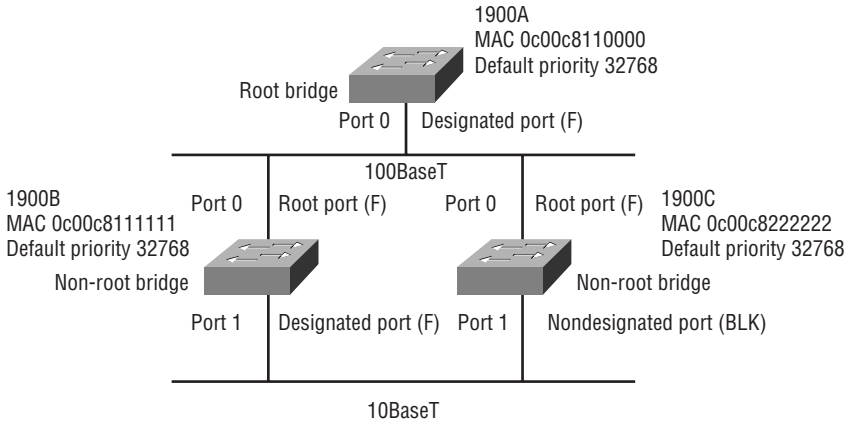
Sizing the Network

Each device will use the timers configured on the root bridge. If the timers need to be changed, Cisco recommends that they not be changed directly. Instead, first experiment with the `spantree diameter` option. It will set the timers based on the size of the switched network. The larger the network, the more time is allowed for propagation, which increases the timers. The default diameter is seven switches across. Setting the diameter smaller than your actual network size increases the chance of broadcast storms.

Spanning Tree Example

In Figure 4.6, the three switches all have the same priority of 32768. However, notice the MAC address of each switch. By looking at the priority and MAC addresses of each switch, you should be able to determine the root bridge.

FIGURE 4.6 Spanning tree example



Because 1900A has the lowest MAC address and all three switches use the default priority, 1900A will be the root bridge.

To determine the root ports on switches 1900B and 1900C, you need to look at the cost of the link connecting the switches. Because the connection from both switches to the root switch is from port 0 using a 100Mbps link, that has the best cost and both switches' root port will then be port 0.

Use the bridge ID to determine the designated ports on the switches. The root bridge always has all ports as designated. However, because both 1900B and 1900C have the same cost to the root bridge and because switch 1900B has the lowest bridge ID, the designated port will be on switch 1900B. Because 1900B has been determined to have the designated port, switch 1900C will put port 1 in blocking state to stop any network loop from occurring.

LAN Switch Types

LAN switching is used to forward or filter frames based on their hardware destination. There are three methods in which frames can be forwarded or filtered. Each method has its advantages and disadvantages, and by understanding the different LAN switch methods available, you can make smart switching decisions.

Here are the three switching modes:

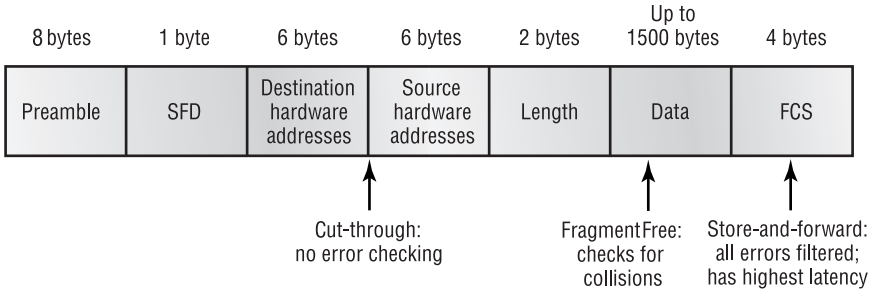
Store-and-forward With the *store-and-forward* mode, the complete data frame is received on the switch's buffer, a cyclic redundancy check (CRC) is run, and then the destination address is looked up in the MAC filter table.

Cut-through With the *cut-through* mode, the switch waits for only the destination hardware address to be received and then looks up the destination address in the MAC filter table.

FragmentFree *FragmentFree* is the default mode for the Catalyst 1900 switch; it is sometimes referred to as modified cut-through. The switch checks the first 64 bytes of a frame for fragmentation (because of possible collisions) before forwarding the frame.

Figure 4.7 shows the different points where the switching mode takes place in the frame. The different switching modes are discussed in detail next.

FIGURE 4.7 Different switching modes within a frame



Store-and-Forward

With the store-and-forward switching method, the LAN switch copies the entire frame onto its onboard buffers and computes the CRC. Because it copies the entire frame, latency through the switch varies with frame length.

The frame is discarded if it contains a CRC error, if it's too short (fewer than 64 bytes including the CRC), or if it's too long (more than 1518 bytes including the CRC). If the frame doesn't contain any errors, the LAN switch looks up the destination hardware address in its forwarding or switching table and determines the outgoing interface. It then forwards the frame toward its destination. This is the mode used by the Catalyst 5000 series switches, and it cannot be modified on the switch.

Cut-Through (Real Time)

With the cut-through switching method, the LAN switch copies only the destination address (the first 6 bytes following the preamble) onto its onboard buffers. It then looks up the hardware destination address in the MAC switching table, determines the outgoing interface, and forwards the frame toward its destination. A cut-through switch provides reduced latency because it begins to forward the frame as soon as it reads the destination address and determines the outgoing interface.

Some switches can be configured to perform cut-through switching on a per-port basis until a user-defined error threshold is reached. At that point, they automatically change over to store-and-forward mode so they will stop

forwarding the errors. When the error rate on the port falls below the threshold, the port automatically changes back to cut-through mode.

FragmentFree (Modified Cut-Through)

FragmentFree is a modified form of cut-through switching. In FragmentFree mode, the switch waits for the collision window (64 bytes) to pass before forwarding. If a packet has an error, it almost always occurs within the first 64 bytes. FragmentFree mode provides better error checking than the cut-through mode, with practically no increase in latency. This is the default switching method for the 1900 switches.

Configuring Spanning Tree

The configuration of spanning tree is pretty simple unless you want to change your timers or add multiple spanning tree instances; then it can get complex. The timers and more advanced configurations are covered in Chapter 5.

STP is enabled on all Cisco switches by default. However, you might want to change your spanning tree configuration to have many spanning tree instances. This means that each VLAN can be its own spanning tree. This is known as Per-VLAN spanning tree.

To enable or disable spanning tree on a set-based switch, use the `set spantree` *`parameter`* command. This is performed on a VLAN-by-VLAN basis rather than a port-by-port configuration:

```
Todd5000> (enable) set spantree disable 1-1005
Spantrees 1-1005 disabled.

Todd5000> (enable) set spantree enable 1-1005
Spantrees 1-1005 enabled.
```

The preceding configuration shows the disabling of spanning tree on an individual VLAN basis. To enable spanning tree on an individual VLAN basis, use `set spantree enable` *`VLAN(s)`*. Cisco recommends that you do not disable spanning tree on a switch, particularly on uplinks where a loop can occur.

Real World Scenario

Detecting Loops

On switches that have a CPU usage indicator, this is sometimes also called "the spanning tree loop indicator." It's relatively rare to see the CPU usage indicator get much past 20 percent utilization for more than a few seconds at a time. If network connectivity has been lost and you suspect a spanning tree loop is the culprit, take a look at the CPU usage indicator. If utilization reaches 70 percent or higher, when the switch never sees that level of usage during normal operation, that's a good indicator of a spanning tree loop.

On a chassis with a Supervisor Engine III or III F with a NFFC or NFFC II, you cannot enable spanning tree on a per-VLAN basis. You must enable spanning tree on every VLAN by using the `set spantree enable all` command.

To enable or disable spanning tree on a Cisco 1900 IOS-based switch, use the `spantree` command or the `no spantree` command. With a 2900/3500, use the `spanning-tree` command to enable and `show spanning-tree` to view the configuration. The following configuration shows how to enable and disable spanning tree on a 1900 switch:

```
1900A#configure terminal
Enter configuration commands, one per line. End with CNTL/Z
1900A(config)#spantree ?
  <1-1005>  ISL VLAN index

1900A(config)#no spantree 1
1900A#show spantree 1
Error: STP is not enabled for VLAN 1

1900A#configure terminal
Enter configuration commands, one per line. End with CNTL/Z
1900A(config)#spantree 1
1900A#show spantree 1
```

```
VLAN1 is executing the IEEE compatible Spanning Tree
  Protocol
   Bridge Identifier has priority 32768, address
   0030.80CC.7B40
   Configured hello time 2, max age 20, forward delay 15
   Current root has priority 32768, address 0030.80CC.7B40
   Root port is N/A, cost of root path is 0
   Topology change flag not set, detected flag not set
   Topology changes 0, last topology change occurred
   0d00h00m00s ago
   Times:  hold 1, topology change 8960
           hello 2, max age 20, forward delay 15
   Timers: hello 2, topology change 35, notification 2
Port Ethernet 0/1 of VLAN1 is Forwarding
   [output cut]
```

Notice in the preceding output that the `no spantree 1` command turned off spanning tree for VLAN 1. Typing `spantree 1` (`spant 1` for short) turned the Spanning Tree Protocol back on for VLAN 1. The `show spantree 1` command displays the STP information for VLAN 1. Notice that the bridge ID, MAC address, and timers are displayed.

To see the spanning tree configuration and whether it is active on a Catalyst 5000 set-based switch, use the `show spantree` command as shown here:

```
Todd5000> (enable) show spantree
VLAN 1
Spanning tree enabled
Spanning tree type          ieee

Designated Root             00-e0-34-88-fc-00
Designated Root Priority    32768
Designated Root Cost        0
Designated Root Port        1/0
Root Max Age   20 sec    Hello Time 2  sec   Forward Delay 15 sec

Bridge ID MAC ADDR          00-e0-34-88-fc-00
Bridge ID Priority          32768
Bridge Max Age 20 sec    Hello Time 2  sec   Forward Delay 15 sec
```

```
Port   Vlan  Port-State    Cost  Priority Fast-Start Group-Method
-----  ----  ------------  -----  --------  ----------  -----
 1/1   1     forwarding      19      32     disabled
 1/2   1     not-connected   19      32     disabled
 2/1   1     not-connected  100      32     disabled
 2/2   1     not-connected  100      32     disabled
 2/3   1     not-connected  100      32     disabled
 2/4   1     not-connected  100      32     disabled
 2/5   1     not-connected  100      32     disabled
<Output truncated>
```

By default, the `show spantree` command provides information about VLAN 1. You can gather spanning tree information about other VLANs by using the `show spantree` *`vlan#`* command.

The `show spantree` command will provide you the following information:

Designated root The MAC address of the root bridge.

Designated root priority The priority of the root bridge. All bridges have a default of 32768.

Designated root cost The cost of the shortest path to the root bridge.

Designated root port The port that is chosen as the lowest cost to the root bridge.

Root timers The timers received from the root bridge.

Bridge ID MAC address This bridge's ID. This plus the bridge priority make up the bridge ID.

Bridge ID priority The priority set; the preceding bridge output is using the default of 32768.

Bridge timers The timers used by this bridge.

Ports in the spanning tree Not all available ports are displayed in the preceding output. However, this field does show all ports participating in this spanning tree. It also shows whether they are forwarding.

Although the command abbreviation `show span` works on all the switches, you will get much different output if you use it on the 5000 series. This is because a SPAN (Switch Port ANalyzer) is the port used to connect to a sniffer. On the 5000, abbreviate `spantree` to no less than `spant` to avoid this.

Summary

This chapter covered layer 2 switching. You learned how redundant links can be used to provide redundancy in a network but also how they can cause problems.

The Spanning Tree Protocol was discussed at length, including how it can be used to stop network loops, broadcast storms, and multiple frame copies.

We discussed STP configuration and showed you some examples. However, we showed you only how to turn spanning tree off and on. In Chapter 5, we'll show you how to use STP to create complex configurations on the switch.

Exam Essentials

Understand that the Spanning Tree Protocol controls the switched network topology. Without STP, switches would often have multiple paths to get to a given destination. Packet duplication due to the multiple paths would lead to broadcast storms and general instability.

Understand the importance of the root bridge. The root bridge is the center of the spanning tree universe; all STP calculations are based on which device is the root. Switches figure out which is the shortest path to the root and disable ports that promote redundancy.

Know the different types of ports. Know that a root port is the port on a switch that has the least-cost path to the root bridge. A designated port is a port that is active but does not lead to the root. All the ports on the root bridge are active and are designated ports.

Understand the method of breaking ties. Whenever there is a tie, there is always a method of breaking it. It is important to remember that usually, a lower number is better. If two switches have the same priority value, the MAC address will break the tie. If two ports on a single switch can reach the root with paths of the same cost, then the lowest-numbered one is used.

Key Terms

Before you take the exam, be sure you're familiar with the following terms:

address learning	FragmentFree
bridge ID	loop avoidance
Bridge Protocol Data Units (BPDUs)	nondesignated ports
cut-through	root bridge
designated ports	Spanning Tree Protocol (STP)
forwarding and filtering decision	store-and-forward

Written Lab

Write the answers to the following questions:

1. What command will show you whether a port is in forwarding mode?
2. What command would you use to disable spanning tree for VLAN 5 on a set-based switch?
3. What command will enable spanning tree for VLAN 6 on a 1900 switch?
4. What is a switch's priority by default?
5. What is used to determine a bridge ID?
6. What is the default hello time of a BPDU?
7. What is the amount of time it takes for a switch port to go from blocking state to forwarding state?

8. What are the four states of a bridge port?

9. What are the two parameters used to determine which port will be forwarding data and which ports will be blocking on a switch with redundant links?

10. True/False: A bridge must forward all broadcasts out all ports except for the port that initially received the broadcast.

Review Questions

1. Which LAN switch method runs a CRC on every frame?
   - **A.** Cut-through
   - **B.** Store-and-forward
   - **C.** FragmentCheck
   - **D.** FragmentFree

2. Which LAN switch type checks only the hardware address before forwarding a frame?
   - **A.** Cut-through
   - **B.** Store-and-forward
   - **C.** FragmentCheck
   - **D.** FragmentFree

3. What is true regarding the STP blocked state of a port? (Choose all that apply.)
   - **A.** No frames are transmitted or received on the blocked port.
   - **B.** BPDUs are sent and received on the blocked port.
   - **C.** BPDUs are still received on the blocked port.
   - **D.** Frames are sent or received on the blocked port.

4. Layer 2 switching provides which of the following? (Choose all that apply.)
   - **A.** Hardware-based bridging (MAC)
   - **B.** Wire speed
   - **C.** High latency
   - **D.** High cost

5. What is used to determine the root bridge in a network? (Choose all that apply.)

A. Priority

B. Cost of the links attached to the switch

C. MAC address

D. IP address

6. What is used to determine the designated port on a bridge?

A. Priority

B. Cost of the links attached to the switch

C. MAC address

D. IP address

7. What are the four port states of an STP switch?

A. Learning

B. Learned

C. Listened

D. Heard

E. Listening

F. Forwarding

G. Forwarded

H. Blocking

I. Gathering

8. What are the three distinct functions of layer 2 switching?

A. Address learning

B. Routing

C. Forwarding and filtering

D. Creating network loops

E. Loop avoidance

F. IP addressing

9. Which of the following is true regarding BPDUs?

   A. BPDUs are used to send configuration messages by using IP packets.

   B. BPDUs are used to send configuration messages by using multicast frames.

   C. BPDUs are used to set the cost of STP links.

   D. BPDUs are used to set the bridge ID of a switch.

10. If a switch determines that a blocked port should now be the designated port, what state will the port go into?

    A. Unblocked

    B. Forwarding

    C. Listening

    D. Listened

    E. Learning

    F. Learned

11. What is the difference between a bridge and a layer 2 switch? (Choose all that apply.)

    A. There can be only one spanning tree instance per bridge.

    B. There can be many different spanning tree instances per switch.

    C. There can be many spanning tree instances per bridge.

    D. There can be only one spanning tree instance per switch.

12. What is the difference between a bridge and a layer 2 switch? (Choose all that apply.)

    A. Switches are software based.

    B. Bridges are hardware based.

    C. Switches are hardware based.

    D. Bridges are software based.

13. What does a switch do when a frame is received on an interface and the destination hardware address is unknown or not in the filter table?

    A. Forwards the switch to the first available link

    B. Drops the frame

    C. Floods the network with the frame looking for the device

    D. Sends back a message to the originating station asking for a name resolution

14. Which LAN switch type waits for the collision window to pass before looking up the destination hardware address in the MAC filter table and forwarding the frame?

    A. Cut-through

    B. Store-and-forward

    C. FragmentCheck

    D. FragmentFree

15. What is the default LAN switch type on a 1900 switch?

    A. Cut-through

    B. Store-and-forward

    C. FragmentCheck

    D. FragmentFree

16. How is the bridge ID of a switch communicated to neighbor switches?

    A. IP routing

    B. STP

    C. During the four STP states of a switch

    D. Bridge Protocol Data Units

    E. Broadcasts during convergence times

17. How is the root port on a switch determined?

    A. The switch determines the highest cost of a link to the root bridge.

    B. The switch determines the lowest cost of a link to the root bridge.

    C. By sending and receiving BPDUs between switches. The fastest BPDU transfer rate on an interface becomes the root port.

    D. The root bridge will broadcast the bridge ID, and the receiving bridge will determine what interface this broadcast was received on and make this interface the root port.

18. How many root bridges are allowed in a network?

    A. 10

    B. 1

    C. 1 for each switch

    D. 20

19. What could happen on a network if no loop avoidance schemes are put in place? (Choose all that apply.)

    A. Faster convergence times.

    B. Broadcast storms.

    C. Multiple frame copies.

    D. IP routing will cause flapping on a serial link.

20. What is the default priority of STP on a switch?

    A. 32768

    B. 3276

    C. 100

    D. 10

    E. 1

Answers to Written Lab

1. `show spantree`. This command will display the spanning tree information of a VLAN and all the ports' participation in STP.
2. `set spantree disable 5`. The `set spantree` command is used to enable or disable spanning tree for a VLAN.
3. `spantree 6`. This command is used to turn on spanning tree for a VLAN. You can disable STP for an interface with the `no spantree` command.
4. 32768. This is the default priority on all switches and bridges.
5. Bridge priority and then MAC address. If the priorities of the switches are set the same, the MAC address would be used to determine the root bridge.
6. Two seconds. Every two seconds, BPDUs are sent out all forwarding ports.
7. Fifty seconds. From blocking to listening is 20 seconds, from listening to learning is 15 seconds, and from learning to forwarding is another 15 seconds.
8. Blocking, listening, learning, forwarding. Each state is used to stop network loops from occurring on redundant links.
9. The path cost and port ID are used to determine the designated port and nondesignated ports.
10. True. Bridges forward all frames that are received and are broadcasts or are not in the filter table.

Answers to Review Questions

1. B. Store-and-forward LAN switching checks every frame for CRC errors. It has the highest latency of any LAN switch type.
2. A. The cut-through method does no error checking and has the lowest latency of the three LAN switch types. Cut-through checks only the hardware destination address before forwarding the frame.
3. A, C. BPDUs are still received on a blocked port, but no forwarding of frames and BPDUs are allowed.
4. A, B. Layer 2 switching uses ASICs to provide frame filtering and is considered hardware based. Layer 2 switching also provides wire-speed frame transfers, with low latency.
5. A, C. Layer 2 devices running the STP use the priority and MAC address to determine the root bridge in a network.
6. B. To determine the designated ports, switches use the cost of the links attached to the switch.
7. A, E, F, H. The four states are blocking, listening, learning, and forwarding. Disabled is a fifth state.
8. A, C, E. Layer 2 features include address learning, forwarding and filtering of the network, and loop avoidance.
9. B. Bridge Protocol Data Units are used to send configuration messages to neighbor switches. This includes the bridge IDs.
10. C. A blocked port will always listen for BPDUs to make sure that a loop will not occur when the port is put into forwarding state.
11. A, B. Unlike a bridge, a switch can have many different spanning tree instances. Bridges can have only one.
12. C, D. Bridges are considered software based, and switches are considered hardware based.
13. C. Switches forward all frames that have an unknown destination address. If a device answers the frame, the switch will update the MAC address table to reflect the location of the device.

14. D. FragmentFree looks at the first 64 bytes of a frame to make sure a collision has not occurred. It is sometimes referred to as modified cut-through.

15. D. By default, 1900 switches use the FragmentFree LAN switch type. The 1900 can use the store-and-forward method.

16. D. The bridge ID is sent via a multicast frame inside a BPDU update.

17. B. Root ports are determined by using the lowest cost of a link to the root bridge.

18. B. Only one root bridge can be used in any network.

19. B, C. Broadcast storms and multiple frame copies are typically found in a network that has multiple links to remote locations without some type of loop avoidance scheme.

20. A. The default priorities on all switches are 32768.

Chapter

5

Using Spanning Tree with VLANs

THE CCNP EXAM TOPICS COVERED IN THIS CHAPTER INCLUDE THE FOLLOWING:

- ✓ **Describe Spanning Tree**
- ✓ **Configure the switch devices to improve Spanning Tree Convergence in the network**
- ✓ **Identify Cisco Enhancement that improve Spanning Tree Convergence**
- ✓ **Configure a switch device to Distribute Traffic on Parallel Links**
- ✓ **Describe LAN segmentation using switches**

Redundancy is the ability to provide an immediate backup solution to a fault in the network that might otherwise cause a network or component service outage. When you're building a redundant network—which is a network with redundant power, hardware, links, and other network-critical components—network loops can occur. The Spanning Tree Protocol (STP) was created to overcome the problems associated with transparent bridging at layer 2.

This chapter will focus on providing link redundancy by using STP and the IEEE 802.1d algorithm used to support STP. The Spanning Tree Protocol uses timers to make the network stable. You'll learn how to manage the different STP timers to maximize the efficiency of your network.

Creating VLAN Standards

Cisco and the IEEE do not see everything eye-to-eye when it comes to using spanning tree and VLANs. Per-VLAN Spanning Tree (PVST) is a Cisco proprietary implementation of STP. PVST uses Inter-Switch Link (ISL) routing and runs a separate instance of STP for each and every VLAN.

The IEEE uses what is called Common Spanning Tree (CST), which is defined with IEEE 802.1q. The IEEE 802.1q defines one spanning tree instance for all VLANs. As of this writing, the IEEE also has a draft standard called 802.1s that will allow multiple spanning tree instances, but it is not a finished standard. This chapter will talk about what Cisco allows in that area. You can review the draft at `www.ieee802.org/1/pages/802.1s.html`.

There is one more implementation of STP, and that is called PVST+. Because it ends with a plus sign, it must be better, right? Well, maybe. What

it does is allow CST information to be passed into PVST. Cisco thinks it would be easier if you simply had all Cisco switches; then you wouldn't even have to think about this issue.

The following list includes a brief explanation of each STP implementation:

Per-VLAN Spanning Tree (PVST) Default for Cisco switches, it runs a separate instance of spanning tree for each VLAN. Makes smaller STP implementations for easier convergence.

Common Spanning Tree (CST) The 802.1q standard, it runs one large STP on the entire network regardless of the number of VLANs. Problems with convergence can occur in large networks.

Per-VLAN Spanning Tree+ (PVST+) Allows Cisco switches to communicate with CST switches.

In the rest of this section, we'll go into more detail about each type of STP implementation and its use with VLANs.

Per-VLAN Spanning Tree (PVST)

The STP protocol does not scale well with large switched networks. In large switched networks, delays can occur in receiving Bridge Protocol Data Units (BPDUs). These delays can cause instability in the STP database. Delays in larger switched networks can also cause convergence time problems, which means that the network will not be forwarding frames.

To solve late BPDUs and convergence problems, Cisco created a separate instance of *Per-VLAN Spanning Tree (PVST)*. It makes smaller STP implementations, which are easier for the switches to manage. Also, with PVST, each VLAN has a unique Spanning Tree Protocol topology for its root, port cost, path cost, and priority.

By running PVST, you still provide a loop-free network, but it is based within each VLAN. Each switch will have a spanning tree process running for each VLAN. If a switch has five VLANs that it knows about, then it will have five instances of spanning tree running. The benefits of having a PVST are listed here:

- It reduces the STP recalculation time when the switched network is converging.
- The spanning tree topology is smaller because all links will not support all VLANs.

- It makes the switched network easier to scale.
- Recovery is faster than with a large network that has one STP instance.
- It allows administrative control of forwarding paths on a subnet basis.
- It allows for load balancing over redundant links when VLAN priorities are established for those links.

However, there are some disadvantages of using a spanning-tree-per-instance implementation:

- The utilization on the switch is a factor because it needs to manage all the STP instances.
- You must take into consideration that the trunk links have to support all the VLAN STP information as well.
- It requires ISL.
- PVST is a Cisco proprietary protocol.

Common Spanning Tree (CST)

The IEEE 802.1q is referred to as the *Common Spanning Tree (CST)*. It is also called the Mono-Spanning Tree because it uses only one spanning tree instance regardless of the size of the switched layer 2 network.

The CST runs on all VLANs by default, and all switches are involved in the election process to find the root bridge. The switches then form an association with that root bridge. Typically, using CST does not allow for optimization of the root bridge placement.

There are some advantages to CST. With one STP instance, there are fewer BPDUs consuming bandwidth. Because there is only one instance of STP in the network, there is less STP processing performed by the switches.

However, the disadvantages typically outweigh the advantages in a larger network. With a single root bridge, the path that has been calculated as the best cost to the root bridge might not be the most efficient for some users to send their data. Another disadvantage of CST is that the STP topology increases in size to make sure all ports in the network are found. This can cause delays in the updates and convergence times if the network topology is too large.

Per-VLAN Spanning Tree+ (PVST+)

Per-VLAN Spanning Tree+ (PVST+) is an extension of the PVST standard. Starting with the Catalyst software 4.1 or later, PVST+ is supported on Cisco Catalyst switches. This enables Cisco switches to support the IEEE 802.1q standard. Basically, the PVST+ extension of the PVST protocol provides support for links across an IEEE 802.1q CST region.

PVST+ also supports the Cisco default PVST and adds checking mechanisms to make sure there are no configuration problems on trunked ports and VLAN IDs across switches. PVST+ is plug-and-play compatible with PVST with no configuration necessary. To provide support for the IEEE 802.1q standard, Cisco's existing PVST has been modified with additional features enabling it to support a link across the IEEE 802.1q Common Spanning Tree region.

PVST+ includes the following features:

- Provides notification of inconsistencies related to port trunking or VLAN identification across the switches.
- Adds mechanisms to ensure that there is no unknown configuration.
- Tunnels PVST BPDUs through the 802.1q VLAN region as multicast data.
- Provides compatibility with IEEE 802.1q's CST and Cisco's PVST protocols.
- Interoperates with 802.1q-compliant switches using CST through 802.1q trunking. A CST BPDU is transmitted or received with an IEEE standard bridge group MAC address.
- Blocks ports that receive inconsistent BPDUs in order to prevent forwarding loops.
- Notifies users via Syslog messages about all inconsistencies.

Scaling the Spanning Tree Protocol

The STP prevents loops in layer 2 switched networks and is basically plug-and-play. However, it might be advantageous to change some of the default timers and settings to create a more stable environment.

In this section, we'll discuss how to scale the STP protocol on a large, switched internetwork. It is important to understand how to provide proper placement of the root bridge to create an optimal topology. If the root bridge is automatically chosen through an election, which is the default, the actual path that the frames can take might not be the most efficient. As the administrator, you can then change the root placement to create a more optimal path. However, it's possible that your changes could cause more damage instead—but hopefully you'll have thought out your network design before making any changes.

To change the root placement, you need to do the following:

- Determine the root device.
- Configure the device.
- Set the port cost.
- Set the port priorities.
- Change the STP timers.

Determining the Root

Determining the root device is the most important decision that you make when configuring the STP protocol on your network. If you place the root in the wrong place in your network, it will be difficult to scale the network, and really, that is what you are trying to do: create a scalable layer 2 switched internetwork.

However, by placing the root switch as close as possible to the center of your network, more optimal and deterministic paths can be easily chosen. You can choose the root bridge and secondary and backup bridges as well. Secondary bridges are very important for network stability in case the root bridge fails. Choosing the root is typically the best thing to do, but if that root goes down for maintenance, spanning tree will select a new root—and because all other switches have the same priority, it might be a switch you wouldn't usually want to be the root bridge.

Because the root bridge should be close to the center of the network, the device will typically be a switch that a lot of traffic passes through, such as a distribution layer switch, a core layer switch, or one that does routing or multi-layer switching. An access layer switch would not usually be chosen.

After the root bridge has been chosen and configured, all the connected switches must determine the best path to the root bridge. The STP uses

several different costs in determining the best path to the root bridge:

- Port cost
- Path cost
- Port priority

When a BPDU is sent out a switch port, the BPDU is assigned a port cost. The path cost, which is the sum of all the port costs, is then determined. The STP will first look at the path cost to figure out the forwarding and blocking ports. If the path costs are equal on two or more links to the root bridge, the port ID is used to determine the root port. The port with the lowest port ID is determined to be the forwarding port. You can change the port used by changing the port priority, but Cisco doesn't recommend this. However, we'll show you how to do it later in this section (so you can have some fun on a rainy Saturday).

Configuring the Root

After you choose the best switch to become your root bridge, you can use the Cisco command-line interface (CLI) to configure the STP parameters in a switched network.

The command to configure the STP is `set spantree`. The following switch output (from our Catalyst 5000) shows the different command parameters you can use when configuring the STP. We are interested in the `set spantree root` and `set spantree root secondary` commands at this point:

```
Todd5000> (enable) set spantree ?
Set spantree commands:
-----------------------------------------------------------------------
set spantree backbonefast       Enable or disable fast convergence
set spantree disable            Disable spanning tree
set spantree enable             Enable spanning tree
set spantree fwddelay           Set spantree forward delay
set spantree hello              Set spantree hello interval
set spantree help               Show this message
set spantree maxage             Set spantree max aging time
set spantree multicast-address  Set multicast address type for trbrf's
set spantree portcost           Set spantree port cost
set spantree portfast           Set spantree port fast start
set spantree portpri            Set spantree port priority
```

```
set spantree portstate          Set spantree logical port state
set spantree portvlancost       Set spantree port cost per vlan
set spantree portvlanpri        Set spantree port vlan priority
set spantree priority           Set spantree priority
set spantree root               Set switch as primary or secondary root
set spantree uplinkfast         Enable or disable uplinkfast groups
Todd5000> (enable)
```

The `set spantree root` command sets the primary root bridge for a specific VLAN, or even for all your VLANs. The `set spantree root secondary` command enables you to configure a backup root bridge.

In the following switch output, notice the options that are available with the `set spantree root` command:

```
Todd5000> (enable) set spantree root ?
Usage: set spantree root [secondary] <vlans> [dia <network_diameter>]
                         [hello <hello_time>]
       (vlans = 1..1005, network_diameter = 2..7, hello_time = 1..10)
```

Table 5.1 shows the parameters available with the `set spantree` command and their definitions.

TABLE 5.1 `set spantree root` Parameters

Parameter	Definition
`root`	Designation to change the switch to the root switch. The `set spantree root` command changes the bridge priority from 32768 to 8192.
`secondary`	Designation to change the switch to a secondary root switch if the primary fails. This automatically changes the bridge priority from a default of 32768 to 16384.
`vlan_list`	Optional command that changes the STP parameters on a specified VLAN. If no VLAN is specified, then it changes only VLAN 1 by default. You can change the parameters for VLANs 1–1005.

TABLE 5.1 `set spantree root` Parameters *(continued)*

Parameter	Definition
`dia` *network diameter*	Another optional command that specifies the maximum number of bridges between any two points where end stations attach. You can set these parameters from 2 to 7. Figure the network diameter by starting at the root bridge and counting the number of bridges in the VLAN. The root bridge is 1, so if you have only one more switch, set the network diameter to 2. This changes the timers in the VLAN to reflect the new diameter.
`hello` *hello time*	Optional command that specifies in seconds the duration between configuration messages from the root switch. You can set this anywhere from 1 to 10 seconds (2 is the default).

The following switch output is an example of using the `set spantree root` command:

```
Todd5000> (enable) set spantree root 1-4 dia 2
VLANs 1-2 bridge priority set to 8192.
VLANs 1-2 bridge max aging time set to 10.
VLANs 1-2 bridge hello time set to 2.
VLANs 1-2 bridge forward delay set to 7.
Switch is now the root switch for active VLANs 1-4.
Todd5000> (enable)
```

The `set spantree root` command tells the switch to change the bridge priority to 8192, which will automatically change the switch to the root bridge. The `1-4` represents the VLANs for which the STP will change the parameters, and the `dia 2` is the network diameter. To figure the network diameter, we simply counted the number of switches from the root, including the root bridge, which in our example equals 2.

Notice the output after the command. The bridge priority was changed to 8192, the maximum age time was changed to 10, hello time is still 2 seconds, and the forward delay was set to 7 seconds. If the network diameter is set, the STP will set the timers to what it would consider efficient for that size network.

Real World Scenario

When a Root Isn't the Root

Using the `set spantree root` command is great when the organization is very centralized. But in a decentralized environment, you might use this command only to find that a coworker set the priority of a different switch to a lower value by using the `set spantree priority` command. This will result in the switch you configured being no more than the backup root bridge. When setting a particular switch to become the root, always make sure that the switch you configured knows it's the root and that other switches know it as well. I find it useful to check one last time as I finish, just to make sure everything is well.

You can verify your STP configuration with the `show spantree` command. If you type the command **`show spantree`** with no parameters, it will show you the spanning tree configuration for all VLANs. You can type **`show spantree`** ***`vlan`*** to see the parameters for just a particular VLAN. The following switch output shows the spanning tree information for VLAN 1:

```
Todd5000> (enable) show spantree 1
VLAN 1
Spanning tree enabled
Spanning tree type          ieee

Designated Root             00-e0-34-88-fc-00
Designated Root Priority    8192
Designated Root Cost        0
Designated Root Port        1/0
Root Max Age   10 sec    Hello Time 2  sec   Forward Delay 7  sec

Bridge ID MAC ADDR          00-e0-34-88-fc-00
Bridge ID Priority          8192
Bridge Max Age 10 sec    Hello Time 2  sec   Forward Delay 7  sec
```

```
Port      Vlan  Port-State      Cost   Priority  Fast-Start
--------- ----  -------------   -----  --------  ----------
 1/1      1     forwarding       19      32      disabled
 1/2      1     forwarding       19      32      disabled
 2/1      1     not-connected    100     32      disabled
 2/2      1     not-connected    100     32      disabled
 2/3      1     not-connected    100     32      disabled
 2/4      1     not-connected    100     32      disabled
 2/5      1     not-connected    100     32      disabled
<Output truncated>
```

Notice that the bridge IP priority is set to 8192; the designated root and bridge ID MAC address are the same because this is the root bridge. The port states are both 19, which is the default for 100Mbps. Because both ports are in forwarding state, the 1900 switch must have one of its FastEthernet ports in blocking mode. Let's take a look by using the `show spantree` command on the 1900 CLI:

```
Port FastEthernet 0/26 of VLAN1 is Blocking
   Port path cost 10, Port priority 128
   Designated root has priority 8192, address   00E0.3488.FC00
   Designated bridge has priority 8192, address   00E0.3488.FC00
   Designated port is 2, path cost 0
   Timers: message age 10, forward delay 7, hold 1

Port FastEthernet 0/27 of VLAN1 is Forwarding
   Port path cost 10, Port priority 128
   Designated root has priority 8192, address   00E0.3488.FC00
   Designated bridge has priority 8192, address   00E0.3488.FC00
   Designated port is 1, path cost 0
   Timers: message age 10, forward delay 7, hold 1
```

Notice that port f0/26 is in blocking mode and port f0/27 is in forwarding mode. If we want port f0/26 to be in forwarding mode and f0/27 in blocking mode, we can set the port costs to help the switch determine the best path to use. Note that we are not saying you should do this; we just wanted to show you how.

Setting the Port Cost

The parameters in this next set are used to enable the network administrator to influence the path that spanning tree chooses when setting the port priority, port cost, and path cost.

Cisco does not recommend changing these settings unless it's absolutely necessary. However, the best way to get a good understanding of how the STP works is by changing the defaults. We do not recommend trying any of this on a production network unless you have permission from the network manager, who understands that you can bring the network down by doing so.

By changing the port cost, you can change the port ID, which means it can be a more desirable port to STP. Remember that STP uses the port ID only if there is more than one path to the root bridge and they are of equal cost. Path cost is the sum of the costs between a switch and the root bridge. The STP calculates the path cost based on the media speed of the links between the switch and the port cost of each port forwarding the frames. In our lab, both links are 100Mbps, so the port ID is important and will be used.

To change the path used between a switch and the root bridge, first calculate the current path cost. Then change the port cost of the port you want to use, making sure that you keep in mind the alternate paths if the primary path fails before making any changes to your switch. Remember that ports with a lower port cost are more likely to be chosen; this doesn't mean they always will be chosen.

To change the port cost of a port on a 5000 series switch, use the `set spantree portcost` command:

```
Todd5000> (enable) set spantree portcost ?
Usage: set spantree portcost <mod_num/port_num> <cost>
       set spantree portcost <trcrf> <cost>
       (cost = 1..65535)
```

The parameters to set the cost of a port are the module and port number and the cost you want to configure. The following example shows how to set the port cost on port 1/1 from the default of 19 to 10:

```
Todd5000> (enable) set spantree portcost 1/1 10
Spantree port 1/1 path cost set to 10.
```

You would verify the change with the `show spantree` command. However, because both ports are in forwarding mode, the preceding command will not change the switch's STP parameters. Notice in the following switch output that both ports are forwarding, but the costs of the ports are different:

```
Port      Vlan  Port-State     Cost   Priority  Fast-Start
--------- ----  -------------  -----  --------  ----------
 1/1       1    forwarding      10       32     disabled
 1/2       1    forwarding      19       32     disabled
```

Remember that a root switch will be forwarding on all active ports, so the port IDs are irrelevant to the switch. However, the 1900 must then choose a port to perform blocking on the interface with the lowest cost.

To change the port cost on a 1900 CLI-based switch, use the `spantree cost` interface command. The cost value can be any number from 1 to 65535; however, you cannot make it less than the path cost of both links. For example, notice in the following switch output that we tried to set port f0/26 to a lower number than the default of 10. The switch would not allow us to do that because both f0/26 and f0/27 are running the default of 10. What we need to do is to raise the port priority of the port we don't want STP to use for forwarding. Notice that we changed the cost of port f0/27 to 20. This should make the f0/26 port a more desirable path:

```
1900A#configure terminal
Enter configuration commands, one per line. End with CNTL/Z
1900A(config)#interface f0/26
1900A(config-if)#spantree cost 5
Error: Option 1 path cost should be greater
       than or equal to option 2 path cost 10
1900A(config-if)#interface f0/27
1900A(config-if)#spantree cost 20
1900A(config-if)#
```

To verify the port priorities, use the `show spantree` command:

```
Port FastEthernet 0/26 of VLAN1 is Forwarding
   Port path cost 10, Port priority 128
   Designated root has priority 8192, address   00E0.3488.FC00
   Designated bridge has priority 8192, address   00E0.3488.FC00
   Designated port is 2, path cost 0
   Timers: message age 10, forward delay 7, hold 1

Port FastEthernet 0/27 of VLAN1 is Blocking
   Port path cost 20, Port priority 128
   Designated root has priority 8192, address   00E0.3488.FC00
   Designated bridge has priority 8192, address   00E0.3488.FC00
   Designated port is 1, path cost 0
   Timers: message age 10, forward delay 7, hold 1
1900A#
```

In the preceding switch output, notice that port f0/26 is now forwarding and port f0/27 is now blocking. In the output, the port path cost is 10 for f0/26 and 20 for f0/27. This is a pretty simple and straightforward configuration, and our network never went down. However, caution should be used when changing the port costs in a real production network because you can cause havoc in a network if the configuration is not thought out carefully. The port costs are propagated in the BPDUs, so a small change on one switch can affect how spanning tree chooses the various ports on a switch a few cable segments away.

Setting the Port Priority

Another option you can use to help the switch determine the path selection that STP uses in your network is to set the port priorities. Remember, this only influences STP; it doesn't demand that STP do anything. However, between setting the port cost and priority, STP should always make your path selection.

The port priority and port cost configurations work similarly. The port with the lowest port priority will forward frames for all VLANs. The command to set a port priority is `set spantree portpri`:

```
Todd5000> (enable) set spantree portpri ?
Usage: set spantree portpri <mod_num/port_num> <priority>
       set spantree portpri <trcrf> <trcrf_priority>
       (priority = 0..63, trcrf_priority = 0..7)
Todd5000> (enable)
```

The possible port priority range is from 0 to 63, and the default is 32. If all ports have the same priority, then the port with the lowest port number will forward frames. For example, 2/1 is lower than 2/2. In the following example, the 5000 switch priority for port 1/1 is set to 20:

```
Todd5000> (enable) set spantree portpri 1/1 20
Bridge port 1/1 port priority set to 20.
Todd5000> (enable)
```

After you change your port priority, you can verify the configuration with the `show spantree 1/1` command:

```
Todd5000> (enable) show spantree 1/1
```

```
Port      Vlan  Port-State     Cost   Priority  Fast-Start
--------- ----  -------------  -----  --------  ----------
 1/1      1     forwarding        10        20   disabled
 1/1      2     forwarding        10        20   disabled
 1/1      3     forwarding        10        20   disabled
 1/1      4     forwarding        10        20   disabled
 1/1      1003  not-connected     10        20   disabled
 1/1      1005  not-connected     10         4   disabled
Todd5000> (enable)
```

Notice that, because port 1/1 is a trunked port, all VLAN priorities were changed on that port. Also notice in the following output that the priority is 20 for 1/1, but the default of 32 is set for 1/2:

```
Todd5000> (enable)show spantree
[output cut]
Port      Vlan  Port-State     Cost   Priority  Fast-Start
--------- ----  -------------  -----  --------  ----------
 1/1       1    forwarding      10       20     disabled
 1/2       1    forwarding      19       32     disabled
```

You can go one step further and set the port priority on a per-VLAN basis. The port with the lowest priority will forward frames for the VLAN for which you've set the priority. Again, if all the ports have the same priority, the lowest port number wins and begins forwarding frames.

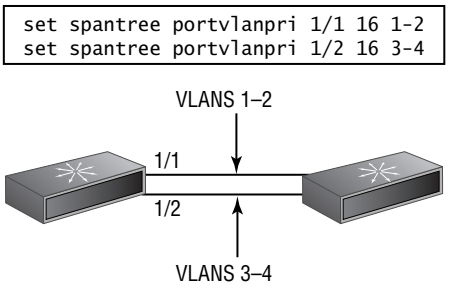
There is an advantage to setting the port priority per VLAN. If you have a network with parallel paths, STP will stop at least one link from forwarding frames so a network loop will not occur. All traffic would then have to travel over only the one link. However, by changing the port priority for a specific group of VLANs, you can distribute the VLANs across the two links. This isn't quite as good as load sharing, but at least you get to use both links as opposed to having one sit idle.

To change the priority of STP for a certain VLAN or group of VLANs, use the `set spantree portvlanpri` command:

```
Todd5000> (enable) set spantree portvlanpri ?
Usage: set spantree portvlanpri <mod_num/port_num>
   <priority> [vlans] (priority = 0..63)
Todd5000> (enable)
```

The priority can be set for each VLAN from 0 to 63. In the following example, we'll set port 1/1 to forward only VLANs 1 and 2, and port 1/2 to forward VLANs 3 and 4. Figure 5.1 shows the physical topology involved.

FIGURE 5.1 Prioritizing traffic by VLAN




```
Todd5000> (enable) set spantree portvlanpri 1/1 16 1-2
Port 1/1 vlans 1-2 using portpri 16.
Port 1/1 vlans 3-1004 using portpri 20.
Port 1/1 vlans 1005 using portpri 4.

Todd5000> (enable) set spantree portvlanpri 1/2 16 3-4
Port 1/2 vlans 1-2,5-1004 using portpri 32.
Port 1/2 vlans 3-4 using portpri 16.
Port 1/2 vlans 1005 using portpri 4.
Todd5000> (enable)
```

The preceding switch output displays the VLAN priority information. We set both VLAN port priorities to 16. Notice that for VLANs 1–4, the priority is 16. However, on port 1/1, all the other VLANs are listed as having a port priority of 20 because that is what we set the port priority to earlier in this chapter. On port 1/2, the switch thinks all the other ports have a port priority of 32, except for VLAN 1005, which becomes a default priority of 4.

You can view the changes by using the `show spantree` *`slot/port`* command, as shown here:

```
Todd5000> (enable) show spantree 1/1
Port      Vlan  Port-State     Cost   Priority  Fast-Start
--------- ----  -------------  -----  --------  ----------
 1/1      1     forwarding       10      16     disabled
 1/1      2     forwarding       10      16     disabled
 1/1      3     forwarding       10      20     disabled
 1/1      4     forwarding       10      20     disabled
 1/1      1003  not-connected    10      20     disabled
 1/1      1005  not-connected    10       4     disabled
```

```
Todd5000> (enable) show spantree 1/2
Port      Vlan  Port-State     Cost   Priority  Fast-Start
--------- ----  -------------  -----  --------  ----------
 1/2      1     forwarding       19      32     disabled
 1/2      2     forwarding       19      32     disabled
 1/2      3     forwarding       19      16     disabled
 1/2      4     forwarding       19      16     disabled
 1/2      1003  not-connected    19      32     disabled
 1/2      1005  not-connected    19       4     disabled
Todd5000> (enable)
```

We want to set the VLAN port priority on the 1900 switch now. Notice in the following switch output that f0/26 is in forwarding mode and f0/27 is blocking. Remember that we changed the port cost to 20 for f0/27, which makes port f0/26 more desirable to the switch:

```
Port FastEthernet 0/26 of VLAN1 is Forwarding
   Port path cost 10, Port priority 128
   Designated root has priority 8192, address   00E0.3488.FC00
   Designated bridge has priority 8192, address   00E0.3488.FC00
   Designated port is 2, path cost 0
   Timers: message age 10, forward delay 7, hold 1
Port FastEthernet 0/27 of VLAN1 is Blocking
   Port path cost 20, Port priority 128
   Designated root has priority 8192, address   00E0.3488.FC00
   Designated bridge has priority 8192, address   00E0.3488.FC00
   Designated port is 1, path cost 0
   Timers: message age 10, forward delay 7, hold 1
```

You can change the priority of the port, but not the VLAN priority as you can with the 5000 series switch. The command is `spantree priority`:

```
1900A#configure terminal
1900A(config-if)#interface f0/27
1900A(config-if)#spantree priority 16
1900A(config-if)#
```

After the priority is set, use the `show spantree` *`vlan`* command to see the port priority. Notice that, because both ports are equal 100Mbps ports, the switch will use the path cost to determine the forwarding or root port. The priority won't be used unless the path costs are the same.

If both ports have the same priority, the interface f0/26 will be used because it is a lower port number:

```
1900A# show spantree 1
[output cut]
Port FastEthernet 0/26 of VLAN1 is Forwarding
   Port path cost 10, Port priority 128
   Designated root has priority 8192, address   00E0.3488.FC00
   Designated bridge has priority 8192, address   00E0.3488.FC00
   Designated port is 2, path cost 0
   Timers: message age 10, forward delay 7, hold 1
Port FastEthernet 0/27 of VLAN1 is Blocking
   Port path cost 20, Port priority 16
   Designated root has priority 8192, address   00E0.3488.FC00
   Designated bridge has priority 8192, address   00E0.3488.FC00
   Designated port is 1, path cost 0
   Timers: message age 10, forward delay 7, hold 1
1900A#
```

By changing either the port priority or the port cost, you can persuade the switch to use your chosen paths. However, there are some miscellaneous other STP variables that you can change. We'll discuss those next.

Changing the STP Timers

The timers are important in an STP network to stop network loops from occurring. The different timers are used to give the network time to update the correct topology information to all the switches and also to determine the whereabouts of all the redundant links.

The problem with the STP timers is that, if a link goes down, it can take up to 50 seconds for the backup link to take over forwarding frames. This is a convergence problem that can be addressed when instability is occurring in the network. The following timers can be changed:

`fwddelay` This interval indicates how long it takes for a port to move from listening to learning state and then from learning to forwarding state. The default is 15 seconds, but it can be changed to anywhere from 4 to 30 seconds. If you set this too low, the switch won't be allowed ample time to make sure no loops will occur before setting a port in forwarding mode. The following switch output shows how to set the `fwddelay` to 10 seconds:

```
Todd5000> (enable) set spantree fwddelay ?
```

```
Usage: set spantree fwddelay <delay> [vlans]
       (delay = 4..30 seconds, vlan = 1..1005)
Todd5000> (enable) set spantree fwddelay 10
Spantree 1 forward delay set to 10 seconds.
```

hello This is the time interval for sending BPDUs from the root switch. It is set to 2 seconds by default; you would think it couldn't be set any lower, but it can be increased or decreased. You can set it to 1 second to actually double the amount of BPDUs sent out that must be lost before triggering an unwanted convergence in the network. However, it doubles the CPU load and processing load as well. The following switch output shows how to change the BPDU timers to 1 second:

```
Todd5000> (enable) set spantree hello ?
Usage: set spantree hello <interval> [vlans]
       (interval = 1..10, vlan = 1..1005)
Todd5000> (enable) set spantree hello 1
Spantree 1 hello time set to 1 seconds.
```

maxage The max age is the amount of time that a switch will hold BPDU information. If a new BPDU is not received before the max age expires, then the BPDU is discarded and is considered invalid. The default is 20 seconds; it can be set to as low as 6 seconds. However, network instability will happen if too many BPDUs are discarded because this timer is set too low. The following output shows how to change the max age of a BPDU to 30 seconds:

```
Todd5000> (enable) set spantree maxage ?
Usage: set spantree maxage <agingtime> [vlans]
       (agingtime = 6..40, vlan = 1..1005)
Todd5000> (enable) set spantree maxage 30
Spantree 1 max aging time set to 30 seconds.
Todd5000> (enable)
```

Rather than directly modifying the timers, it is usually better to modify the size of the network. Table 5.1 referred to a "diameter" value that can be set when selecting the spanning tree root. The diameter used is the width of the network from one side to the other. Three switches daisy-chained together would have a diameter of 3, whereas three configured in a triangle would have a diameter of 2.

The diameter will automatically set the timers to a value appropriate to the size of your network. Setting the timers yourself to low values in a large network risks topological loops because the delay might not be long enough to account for BPDU propagation delay. The best thing to do is to use the diameter option when setting the root and then modify the timers from there, if necessary.

We have been discussing redundant links and STP, but most of the discussion has been about how to make STP run efficiently, and that is by making the non-root port a blocking port. We discussed load balancing only when we showed you how to set the port priority on a per-VLAN basis. However, that really wasn't load balancing to the degree that is possible with a Cisco switched network. In the next section, we'll cover the most efficient ways of using redundant links in a large, switched internetwork.

Using Redundant Links with STP

Fast EtherChannel and *Gigabit EtherChannel* allow high-speed redundant links in a spanning tree environment by allowing dual parallel links to be treated as though they were one link. Cisco Fast EtherChannel technology uses the standards-based 802.3 Full-Duplex Fast Ethernet to provide a reliable high-speed solution for the campus network backbone. Fast EtherChannel can scale bandwidth within the campus, providing full-duplex bandwidth at wire speeds of 200Mbps to 800Mbps. It provides high bandwidth, load sharing, and redundancy of links in a switched internetwork.

Broadcast traffic, as well as unicast and multicast traffic, is distributed equally across the links in the channel. Fast EtherChannel also provides redundancy in the event of a link failure. If a link is lost in a Fast EtherChannel network, traffic is rerouted to one of the other links in just a few milliseconds, making the convergence transparent to the user.

Gigabit EtherChannel works in the same fashion that Fast EtherChannel does, except it's faster. Each device has a limit to the number of ports that can participate but it's in the range of 2 to 8, giving a potential channel size of 16 Gbps.

This section will introduce you to the several ways of configuring redundant links. In the part about EtherChannel, you'll learn about the communication protocol that switches use and how load balancing takes place. You will

then learn how the switch can violate the usual rules that spanning tree lives by, to create a network that responds faster when there is a problem.

Real World Scenario

Modifications to EtherChannel

EtherChannel has undergone some changes in the last four years on Cisco switches. It used to be that you had to group the ports together in order to use them in a channel. Ports 1–4 had to be used together, 5–8 had to be used together, and so on. If you were using only two, then they had to be the first two ports in the group of four. Of course, they all had to be on the same blade as well. The first thing an administrator would do when troubleshooting was to make sure the correct ports were being used.

The restrictions aren't quite as difficult now, though. A version 5.3 or higher system will enable you to use whatever ports you want to, as long as they are configured the same.

Different devices will also forward frames across the channel in different ways, and some can be set up to apply rules based on layer 3 or layer 4 headers. The secret to setting up an effective EtherChannel topology is to understand the limitations of your equipment and software.

Parallel Fast EtherChannel Links

Fast EtherChannel uses load distribution to share the links in a bundle. A bundle is a group of FastEthernet or Gigabit Ethernet links managed by the Fast EtherChannel process. Should one link in the bundle fail, the Ethernet Bundle Controller (EBC) informs the Enhanced Address Recognition Logic (EARL) ASIC of the failure, and the EARL in turn ages out all addresses learned on that link. The EBC and the EARL use hardware to recalculate the source and destination address pair on a different link.

The convergence time is sometimes referred to as the failover time, which is the time it takes for the new address to be relearned—about 10 microseconds. Windowing flow control techniques can make this process a touch longer, but that depends on the particular application in use. The key is not having the application time out, and the failover time is fast enough to stop the time-out from happening.

EtherChannel Guidelines

EtherChannel does not work under certain circumstances. This is to ensure that no network loops will occur if the bundle comes up. There are certain guidelines to follow when configuring EtherChannel technology:

- All ports must be in the same VLAN or they must all be trunk ports that belong to the same native VLAN.
- All ports must be configured as the same trunk mode if trunking is used.
- When trunking is used, all ports must be configured with the same VLAN range. If it is not the same, packets will be dropped and the ports will not form a channel when set to the auto or desirable mode.
- All ports must be configured with the same speed and duplex settings.
- If broadcast limits are configured on the ports, configure the limits for all the ports or packets might be dropped.
- The ports cannot be configured in a channel as dynamic VLAN ports.
- Port security must be disabled on channeled ports.
- All ports must be enabled in the channel before the channel can come up. If you disable a port, a link failure occurs.

Configuring EtherChannel

To create an EtherChannel bundle, use the `set port channel` command. You must first make sure that all the conditions for EtherChannel have been met.

Notice the switch output when we try to configure the ports on our 5000 switch as a bundle to the 1900 switch:

```
Todd5000> (enable) set port channel 1/1-2 on
Mismatch in trunk mode.
Mismatch in port duplex.
Mismatch in STP port priority.
Failed to set port(s) 1/1-2 channel mode to on.
Todd5000> (enable)
```

There is a mismatch in trunking, duplex, and STP port priority. All the ports must be configured the same for EtherChannel to work.

To view the configuration of a port, use the `show port capabilities` *`slot/port`* command:

```
Todd5000> (enable) show port capabilities 1/1
Model                     WS-X5509
Port                      1/1
Type                      100BaseTX
Speed                     100
Duplex                    half,full
Trunk encap type          ISL
Trunk mode                on,off,desirable,auto,nonegotiate
Channel                   1/1-2
Broadcast suppression     percentage(0-100)
Flow control              no
Security                  yes
Membership                static,dynamic
Fast start                yes
Rewrite                   no
Todd5000> (enable)
```

The preceding output shows the card model number and the configuration of the port. The easiest way for us to make sure all the ports we want to channel are configured the same is to just clear the configuration. We're not suggesting that you just clear your config whenever any problems come up, but the configuration we created in this chapter is pretty extensive, and it's easier to simply clear it out of the switch to perform the next function:

```
Todd5000> (enable) clear config all
This command will clear all configuration in NVRAM.
This command will cause ifIndex to be reassigned on the
   next system startup.
Do you want to continue (y/n) [n]? y
........
..................
System configuration cleared.
Console> (enable)
```

Remember that you need to reset the switch after erasing the configuration to clear the configuration. We need to reconfigure the switch with an IP address

and trunking on ports 1/1 and 1/2. Now, we're also going to delete the configuration on the 1900 so then we will have both switches back to our STP default:

```
1900A#delete nvram
This command resets the switch with factory defaults.  All system
parameters will revert to their default factory settings. All
static and dynamic addresses will be removed.
Reset system with factory defaults, [Y]es or [N]o?  Yes
```

Now that we have both the switches back to their default configurations, we'll just configure the IP addresses and turn on trunking on ports 1/1 and 1/2 of the 5000 and ports 0/26 and 0/27 of the 1900:

```
#configure terminal
(config)#hostname 1900A
1900A(config)#ip address 172.16.10.2 255.255.255.0
1900A(config)#ip default-gateway 172.16.10.1
1900A(config)#interface f0/26
1900A(config-if)#trunk on
1900A(config-if)#interface f0/27
1900A(config-if)#trunk on

Console> (enable) set prompt Todd5000>
Todd5000> (enable) set interface sc0 172.16.10.4
  255.255.255.0
Interface sc0 IP address and netmask set.
Todd5000> (enable) set trunk 1/1 on
Port(s) 1/1 trunk mode set to on.
Todd5000> (enable) set trunk 1/2 on
Port(s) 1/2 trunk mode set to on.
Todd5000> (enable)
```

To verify that the ports are trunking, use the `show trunk` command:

```
Todd5000> (enable) show trunk
Port      Mode         Encapsulation  Status      Native vlan
--------  -----------  -------------  ----------  -----------
  1/1     on           isl            trunking    1
  1/2     on           isl            trunking    1
```

Let's try to configure EtherChannel between the switches again:

```
Todd5000> (enable) set port channel 1/1-2 on
```

```
Port(s) 1/1-2 channel mode set to on.
Todd5000> (enable) 1997 Jul 25 23:08:20 %PAGP-5-
   PORTFROMSTP:Port 1/1 left bridge  port 1/1
1997 Jul 25 23:08:20 %PAGP-5-PORTFROMSTP:Port 1/2 left
   bridge port 1/2
1997 Jul 25 23:08:20 %PAGP-5-PORTTOSTP:Port 1/1 joined
   bridge port 1/1-2
1997 Jul 25 23:08:21 %PAGP-5-PORTTOSTP:Port 1/2 joined
   bridge port 1/1-2
```

To verify the EtherChannel bundle, use the `show port channel` command:

```
Todd5000> (enable) show port channel
Port  Status     Channel   Channel     Neighbor  Neighbor
                 mode      status      device    port
----- ---------- --------- ----------- --------- -------
 1/1  errdisable on        channel
 1/2  errdisable on        channel
----- ---------- --------- ----------- --------- -------
Todd5000> (enable)
```

You can see that the status is error disabled and that no neighbors are found. This is because we still need to configure Fast EtherChannel on the 1900 switch. If this were a remote switch, you would lose contact with the switch and have to go to the site and console into the switch to configure EtherChannel. You should configure the remote site first; then you will lose contact with it until you configure the local switch bundle.

To configure the EtherChannel bundle on a 1900 switch, use the `port-channel mode` command:

```
1900A(config)#port-channel mode ?
  auto       Set Fast EtherChannel mode to AUTO
  desirable  Set Fast EtherChannel mode to DESIRABLE
  off        Set Fast EtherChannel mode to OFF
  on         Set Fast EtherChannel mode to ON
1900A(config)#port-channel mode on
```

That is all you can configure on the 1900. The switch will look for the neighbor device ID and neighbor group capability that are the same and form the connections into a channel. In this case, ports 0/26 and 0/27 are connected to the same device ID (hostname). By using the command `show`

`spantree 1`, you can see that ports 0/26 and 0/27 are now one port:

```
1900A#show spantree 1
[output cut]
Port PortChannel of VLAN1 is Forwarding
   Port path cost 10, Port priority 128
   Designated root has priority 32768, address   0030.80CC.7B40
   Designated bridge has priority 32768, address   0030.80CC.7B40
   Designated port is 26, path cost 0
   Timers: message age 20, forward delay 15, hold 1
```

Ports 0/26 and 0/27 are now just listed as Port PortChannel. To verify the EtherChannel on the 5000 series switch, use the `show port channel` command:

```
Todd5000> (enable) show port channel
Port  Status     Channel    Channel     Neighbor            Neighbor
                 mode       status      device              port
----- ---------- ---------- ----------- ------------------ ----------
 1/1  connected  on         channel     cisco 1900  1900A     A
 1/2  connected  on         channel     cisco 1900  1900A     B
----- ---------- ---------- ----------- ------------------ ----------
Todd5000> (enable)
```

The preceding switch output shows the port numbers, status, mode, channel status, neighbor device, and neighbor port ID. Our EtherChannel is working!

Port Aggregation Protocol (PAgP)

The *Port Aggregation Protocol (PAgP)* is used to add more features to the EtherChannel technology. This protocol is used to learn the capabilities of the neighbors' EtherChannel ports. By doing this, it allows the switches to connect via Fast EtherChannel automatically. PAgP has four options when configuring the channel; `on`, `off`, `desirable`, and `auto`. The first two, `on` and `off`, are self-explanatory. A `desirable` link wants to become a channel, whereas a link set to `auto` doesn't want to but will if it has to. A channel will form if one of the following combinations are used: `on-on`, `on-desirable`, `on-auto`, `desirable-desirable`, `desirable-auto`.

The PAgP protocol groups the ports that have the same neighbor device ID and neighbor group capability into a channel. This channel is then added to the Spanning Tree Protocol as a single bridge port.

For PAgP to work, all the ports must be configured with static, not dynamic, VLANs, and all the ports must also be in the same VLAN or be configured as trunk ports. All ports must be the same speed and duplex as well. In other words, all the ports must be configured the same or PAgP will not work.

If an EtherChannel bundle is already working and you make a change on a port, all ports in that bundle are changed to match the port. If you change the speed or duplex of one port, all ports will then run that speed or duplex.

Load Balancing and Redundancy

Each switch will operate a channel in a different fashion, but there are two main issues that all the switches must face. The first is how they forward traffic across the bundle of physical links, and the second is what happens if a link fails. This section will cover the basics. Cisco provides a guide at `http://www.cisco.com/warp/public/473/4.html` detailing how each of the switches deal with these two topics.

Load Balancing

A channel is nothing more than a bundle of circuits that pretend to act like a single cable. Although this is convenient for increasing bandwidth without causing problems with spanning tree, it leaves us wondering which link gets used when a frame wants to cross the channel. The following list shows how the switches each approach this task.

The 5000 Will send frames across the channel in a fashion that depends on the source and destination MAC addresses. An X-OR process is run on the last bit in the MAC addresses. The output will be one of 0.0, 0.1, 1.0, or 1.1. All frames where the source and destination MAC addresses end in 1 will use the same circuit. All frames where the last bit in the source is 0 and the last bit in the destination is 1 will use a different circuit. There is no load balancing between the circuits.

The 2900/3500 and 1900/2820 Will send a frame out the same circuit that it learned about the destination device on, unless there is a circuit that is less busy. For instance, if a packet from PC-A going to PC-B arrived across a channel by using circuit 2, the switch will cache that information. When PC-B replies, the switch will forward the frame across the channel by using circuit 2. However, if circuit 2 is busy when compared to other

members of the channel, then a different circuit will probably be used. This allows for load balancing across the circuits.

Layer 3+ switches A switch that can recognize layer 3 or higher information can be configured to forward frames based on higher-layer header information. For example, the 6000 series can be configured with hardware that enables it to choose what circuit to use based on source, destination, or both. For addressing, it can use MAC addressing, IP addressing, or port values.

Redundancy

Because of the dynamic, load-balancing nature of the 2900, 3500, 1900, and 2820, redundancy is a breeze. The 2900 and 3500 will simply forward traffic out the link that has the least amount of utilization, just as it ordinarily would. The 1900 operates in the same fashion, but because it supports only a two-circuit channel, all remaining traffic is picked up by the remaining circuit.

The 5000 is a bit different in the way it handles redundancy. If a circuit drops, the 5000 will have addresses cached. The 5000 must find a new way to reach those addresses because the way it was using them is no longer valid. It will age out the addresses in the cache and forward them to the cache for the next numerical circuit. If circuit 1 has three addresses in its cache when it drops, those addresses will be relearned on circuit 2. There is a delay that typically doesn't exceed a couple of milliseconds to accomplish this task. If the original link comes up, the addresses will not revert back unless they naturally age out of the cache on the new port.

PortFast

By default, the Spanning Tree Protocol (STP) runs on all ports on a switch. Because most of the ports connect to workstations, printers, servers, routers, and so on, it's basically a waste of resources for these point-to-point ports to be running the Spanning Tree Protocol. When a device, let's say a workstation, powers up, it takes up to 50 seconds before the switch will forward data on the port because the STP is making sure no loops are going to occur when the port is in forwarding mode. Not only is this a waste of time (because a loop will not occur with point-to-point links), but some protocols or applications could time out.

PortFast is used to make a point-to-point port almost immediately enter into forwarding state by decreasing the time of the listening and learning

states. This is very helpful for switch ports that have workstations or servers attached, because these devices will connect immediately instead of waiting for the STP to converge. If you connect a hub to a port configured with PortFast and then accidentally connect another port into the switch from the hub, you will have a network loop, and STP will not stop it. It is important to make sure that PortFast is used only on point-to-point links connected only to workstations or servers.

Configuring PortFast

To configure PortFast on a switch, use the `set spantree portfast` command. The following switch output shows how to configure ports 2/1–12 with PortFast:

```
Todd5000> (enable) set spantree portfast ?
Usage: set spantree portfast <mod_num/port_num>
   <enable|disable>
        set spantree portfast <trcrf> <enable|disable>

Todd5000> (enable) set spantree portfast 2/1-12 enable

Warning: Spantree port fast start should only be enabled
   on ports connected to a single host. Connecting hubs,
   concentrators, switches, bridges, etc. to a fast start
   port can cause temporary spanning tree loops. Use with
   caution.
Spantree ports 2/1-12 fast start enabled.
Todd5000> (enable)
```

Notice the nice warning received on the switch console when PortFast was turned on. Also notice that we were able to turn on all 12 ports of our 10/100 card.

To configure PortFast on a 1900 switch, use the `spantree start-forwarding` command:

```
1900A#configure terminal
1900A(config)#interface e0/1
1900A(config-if)#spantree start-forwarding
1900A(config-if)#
```

This must be configured on each port you want to run PortFast.

Real World Scenario

PortFast and BPDUs

Some switches support an addition to PortFast called BPDUGuard. When you enable PortFast on a port, there is no guarantee that someone won't add a switch at their desk. Then, for redundancy, they also connect that switch to the LAN drop at their neighbor's desk. Congratulations, you now have a spanning tree loop!

BPDUGuard is a feature that can be set on many switches that enable PortFast. It monitors for BPDUs on that port. If a BPDU arrives, the switch shuts down the port, placing it in the `errdisable` state, and generates a status message.

UplinkFast

UplinkFast is used to minimize network downtime by ensuring that network loops do not occur when the network topology changes. STP convergence time is very time-consuming, so network loops can occur when the convergence is taking place. UplinkFast can reduce the convergence time during a link failure or a topology change.

Another problem with STP and the convergence time is that some hosts will not be available for communication during the convergence time because STP has disabled ports on a switch during convergence. The key is decreased convergence time, which UplinkFast was developed to provide.

UplinkFast enables a blocked port on a switch to begin forwarding frames immediately when a link failure is detected on the root port. For the switch to change a port from blocking to forwarding mode, UplinkFast must have direct knowledge of the link failure.

To utilize UplinkFast, several criteria must be met. First, UplinkFast must be enabled on the switch. The switch must have at least one blocked port, and the failure must be on the root port. If the failure is not on a root port, UplinkFast will ignore it and normal STP functions will occur.

When a link fault occurs on the primary root link, UplinkFast transitions the blocked port to a forwarding state. UplinkFast changes the port without passing through the listening and learning phases, which enables the switch

to skip the normal convergence time and start forwarding in about 3 to 4 seconds instead of the usual 50 seconds.

Cisco has designed UplinkFast to work with its access layer switches, not its core switches, because the switch running UplinkFast must not be the root bridge.

Configuring UplinkFast

When configuring UplinkFast, remember that all VLANs on the switch are affected and that you cannot configure UplinkFast on individual VLANs.

To configure UplinkFast on a set-based switch, use the `set spantree uplinkfast` command:

```
Todd5000> (enable) set spantree uplinkfast ?
Usage: set spantree uplinkfast <enable> [rate <station_
   update_rate>] [all-protocols <off|on>]
       set spantree uplinkfast <disable>
```

The options are really just `enable` or `disable`. The station update rate value is the number of multicast packets transmitted per 100 milliseconds (by default, it is set to 15 packets per millisecond). It is not recommended that you change this value.

The switch will provide an output describing what the command changed on the switch, as shown here:

```
Todd5000> (enable) set spantree uplinkfast enable
VLANs 1-1005 bridge priority set to 49152.
The port cost and portvlancost of all ports set to above 3000.
Station update rate set to 15 packets/100ms.
uplinkfast all-protocols field set to off.
uplinkfast enabled for bridge.
Todd5000> (enable)
```

The VLAN priorities are automatically changed to 49152, and the port costs are set to above 3000. These are changed to make it unlikely that the switch will become the root switch.

You can verify the UplinkFast configuration with the `show spantree uplinkfast` command:

```
Todd5000> (enable) show spantree uplinkfast
Station update rate set to 15 packets/100ms.
uplinkfast all-protocols field set to off.
```

```
VLAN          port list
-----------------------------------------------
1             1/1(fwd)
2             1/1(fwd)
3             1/1(fwd)
4             1/1(fwd)
Todd5000> (enable)
```

Notice that all four VLANs are changed and that we were not asked which VLANs to run UplinkFast on.

To configure UplinkFast on a 1900 switch, use the command `uplink-fast` in global configuration mode:

```
1900A#configure terminal
1900A(config)#uplink-fast
1900A(config)#exit
```

To verify that UplinkFast is configured and running, use the commands `show uplink-fast` and `show uplink-fast statistics`:

```
1900A#show uplink-fast
 Uplink fast                              Enabled
 Uplink fast frame generation rate        15

1900A#show uplink-fast statistics
 Uplink fast Transitions                   0
 Uplink fast Station Learning Frames       0
1900A#
```

The default frame generation rate is 15, which is displayed with the `show uplink-fast` command. The next command used to help STP maintain a consistent network is BackboneFast.

BackboneFast

Sometimes a switch might receive a BPDU from another switch that identifies the second switch as the root bridge when a root bridge already exists. This shouldn't happen, except when a new switch comes on line and the BPDU is considered inferior.

BPDUs are considered inferior when a switch has lost its link to the root bridge. The switch transmits the BPDUs with the information that it is now the root bridge as well as the designated bridge. The receiving switch will ignore the inferior BPDU for the max age time, to prevent spanning tree loops.

After receiving inferior BPDUs, the receiving switch will try to determine whether there is an alternate path to the root bridge. If the port that the inferior BPDUs are received on is already in blocking mode, then the root port and other blocked ports on the switch become alternate paths to the root bridge. However, if the inferior BPDUs are received on a root port, then all presently blocking ports become the alternate paths to the root bridge. Also, if the inferior BPDUs are received on a root port and there are no other blocking ports on the switch, the receiving switch assumes that the link to the root bridge is down and the max age time expires, which turns the switch into the root switch.

If the switch finds an alternate path to the root bridge, it will use this new alternate path. This new path, and any other alternate paths, will be used to send a Root Link Query BPDU. By turning on *BackboneFast*, the Root Link Query BPDUs are sent out as soon as an inferior BPDU is received. This can enable faster convergence in the event of a backbone link failure. To ensure proper operation, BackboneFast should be enabled on all switches, including the root, if it is enabled at all.

Configuring and Verifying BackboneFast

Configuring BackboneFast is pretty easy, but it sounds difficult, which is the cool part about this command. You turn it on with the `set spantree backbonefast` command. Here is an example of this command being enabled:

```
Todd5000> (enable) set spantree backbonefast
Usage: set spantree backbonefast <enable|disable>

Todd5000> (enable) set spantree backbonefast enable
Backbonefast enabled for all VLANs
```

Notice in the preceding switch output that BackboneFast is enabled for all VLANs, and it must be enabled on all switches in your network to function. To verify that it is running on a switch, use the `show spantree backbonefast` command:

```
Todd5000> (enable) show spantree backbonefast
Backbonefast is enabled.
Todd5000> (enable)
```

The preceding command shows that BackboneFast is enabled. That's all there is to it.

Summary

This chapter covered the detailed Spanning Tree Protocol information you need to be successful in the day-to-day maintenance of a layer 2 switched internetwork. Specifically, we covered the following:

- Cisco and the IEEE 802.1q committee
- Scaling the STP protocol
- Redundant links with STP
- Parallel FastEthernet links
- EtherChannel guidelines
- Port Aggregation Protocol
- PortFast
- UplinkFast
- BackboneFast

Exam Essentials

Know the types of spanning tree available. Understand that there are two types of spanning tree, ISL and 802.1q, and know what their limitations and benefits are. ISL is Cisco proprietary but it allows for one spanning tree instance per VLAN, whereas 802.1q doesn't but it is an industry standard. ISL supports Per-VLAN Spanning Tree (PVST), and 802.1q is limited to Common Spanning Tree (CST).

Know what can be configured to reduce the delay a port must go through with a topology change. Understand what PortFast, BackboneFast, and UplinkFast are capable of doing and under what circumstances.

Understand how an EtherChannel works. Know that an EtherChannel is formed from 2 to 8 ports connecting the same two switches together. A single command on each switch will logically bind the circuits together, but only if each circuit is configured in an identical fashion.

Key Terms

Before you take the exam, be sure you're familiar with the following terms:

- BackboneFast
- Common Spanning Tree (CST)
- Fast EtherChannel
- Gigabit EtherChannel
- Per-VLAN Spanning Tree (PVST)
- Per-VLAN Spanning Tree+ (PVST+)
- Port Aggregation Protocol (PAgP)
- PortFast
- UplinkFast

Written Lab

Write the answers to the following questions:

1. Write the command to set a switch to become the root bridge for VLANs 50–1000 with four switches in the internetwork on a 5000 series switch.
2. What command will show you the port cost and priority for VLAN 1 on a set-based switch?
3. Write the command to set the port cost on a 5000 switch port 2/1 from the default of 19 to 10.
4. Write the command to set the priority for port 1/1 to 20.
5. After you change your port priority, you can verify the configuration with which command?
6. Write the command to set port 1/1 priority on a set-based switch to 16 for VLANs 1 and 2 only.
7. Write the command to turn on PortFast on ports 2/1–12 on a set-based switch.

8. Write the command to set UplinkFast on a set-based switch to on.

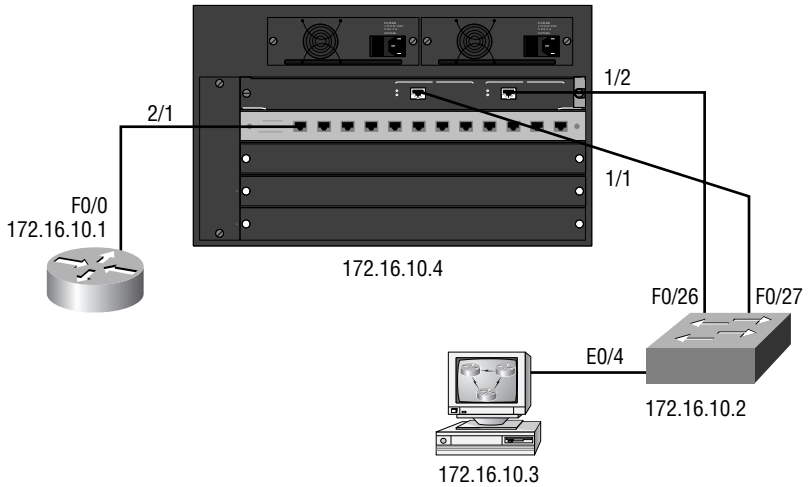
9. Write the command to create an EtherChannel bundle on a set-based switch using ports 1/1–2.

10. Write the command to change the `fwddelay` to 10 seconds on a set-based switch.

Hands-On Lab

In this lab, you'll test PortFast and UplinkFast on the network; then you'll configure the 5000 series switch as an STP root and add EtherChannel between the 5000 and 1900 switches. Figure 5.2 shows the network configuration used in this lab. Make sure the configurations of your switches are deleted and the default STP configuration is on both switches.

FIGURE 5.2 Network diagram for the hands-on lab



Configure both the 5000 series switch and the 1900 switch with the hands-on labs from Chapter 2, "Connecting the Switch Block," and Chapter 3, "VLANs." Each switch should have the hostname, interface descriptions, passwords, VTP domain information, and VLANs configured and trunk links on. Test by pinging from the workstation to the 1900 and 5000 switch.

1. Remember that PortFast is disabled on all ports of a switch by default. By turning on PortFast, you can start forwarding up to 50 seconds sooner when bringing up a device. To test this, connect your workstation into interface e0/4 of the 1900 switch and then from the DOS prompt of your workstation, ping the 5000 series switch.

   ```
   Ping -t 172.16.10.4
   ```

2. The `-t` will keep the ping running. Go to the 1900 switch and perform a **`shutdown`** and **`no shutdown`** on interface e0/4. Then notice how long it takes before the pings resume. This could be up to 50 seconds (although, if you have a small network, it might resume faster).

3. Leave the pings running. Go to int e0/4 and type **`spantree start-forwarding`**, which turns on PortFast for that port.

4. Go to the 1900 switch and perform a **`shutdown`**, then a **`no shutdown`** on e0/4. The pings will time out but should resume after only a few seconds.

5. Leave the Ping program running. Type **`show spantree 1`** and notice which port is forwarding and which port is blocking.

6. Leave the Ping program running. Perform a **`shutdown`** on the forwarding interface. Notice that the pings have timed out, but they should resume after a few seconds.

7. Type **`show spantree 1`** and notice which port is forwarding.

8. Perform a **`no shutdown`** on the port you originally shut down. Notice that the pings have timed out again, but the pings should resume after a few moments.

9. Turn on UplinkFast on your 1900 forwarding port by typing **`uplink-fast`** from global configuration mode.

10. Perform steps 5 through 8 again and notice that the ping's time-out and resume cycle was shorter. UplinkFast demonstrated an almost immediate transition to the second trunk link when the forwarding link was shut down.

11. Configure the 5000 series switch as the STP root switch by typing **`set spantree root 1-4 dia 2`** from the enable mode of the switch. The diameter of the network is determined by counting the switches connected to the root, including the root, which in this case is 2. The VLANs configured are 1–4.

12. Verify the configuration by typing **show spantree 1**. Notice the root designation.
13. Make sure your links are trunked by typing **show trunk** on the 5000 series switch.
14. Go to the 1900 and verify the forwarding port. Change the cost of the forwarding port to 20, which should make the blocked port the forwarding port. Type **spantree cost 20** from interface configuration of the forwarding port.
15. Verify the configuration with the **show spantree** command and notice that the blocked port is now forwarding and the forwarding port has been changed to blocked. Also notice the port costs.
16. Set the port priority on the forwarding port as well, to make sure that STP always uses this port to forward, by typing **spantree priority 64** from interface configuration, which is half of the 128 default interface priority.
17. Verify the configuration with the **show spantree** command.
18. Create an EtherChannel bundle between your two switches, but before you do, make sure your port configurations are exactly the same. Change the 1900 switch back to the default configuration. Type **spantree cost 10** and **spantree priority 128** from interface configuration mode. Also, set the duplex of the links to full-duplex on both the 1900 and 5000. Set the 5000 to be 100Mbps as well.
19. From the 1900 interface configuration mode, type **duplex full** on both ports.
20. From the 5000 series switch, type **set port speed 100** and **set port duplex full** for ports 1/1 and 1/2.
21. Set the EtherChannel bundle to on for the 1900 switch by typing **port-channel mode on** from global configuration mode.
22. From the 5000 series switch, turn on EtherChannel by typing **set port channel 1/1-2 on**.
23. Verify the EtherChannel bundle by typing **show port channel**.

Review Questions

1. The Spanning Tree Protocol was created to overcome the problems of what type of bridging?
   - **A.** Source route bridging
   - **B.** Shorter path bridging
   - **C.** Transparent bridging
   - **D.** UplinkFast bridging

2. Bridge Protocol Data Units (BPDUs) are responsible for providing information for which four services in a spanning tree?
   - **A.** Determining the locations of data loops
   - **B.** Electing a root bridge
   - **C.** Monitoring the spanning tree
   - **D.** Deciding the manufacturer's MAC address on a physical interface
   - **E.** Notifying other switches of network changes

3. On what VLAN are Bridge Protocol Data Units (BPDUs) sent by default?
   - **A.** VLAN 64
   - **B.** VLAN 1005
   - **C.** VLAN 1
   - **D.** VLAN 10

4. Which of the following provides a separate instance of Spanning Tree Protocol for every VLAN?
   - **A.** Common Spanning Tree (CST)
   - **B.** Spanning Tree Algorithm (STA)
   - **C.** Port Aggregation Protocol (PAgP)
   - **D.** Per-VLAN Spanning Tree (PVST)

5. To configure a backup root bridge on a set-based switch, what command would be used?

   A. `set spanning tree backup`

   B. `set spantree secondary`

   C. `set spantree root secondary`

   D. `spanning tree 2`

6. How many Spanning Tree Protocol instances are supported on the 1900 switch?

   A. 1005

   B. 10

   C. 512

   D. 64

7. Which of the following would change the VLAN port priority on a 1900 series IOS command-based switch to a value of 16?

   A. `spantree priority 16`

   B. `set spantree priority 16`

   C. `config spantree priority 16`

   D. `change spantree pri 16`

8. When setting the VLAN port priority, what are the available values you can use?

   A. 0–63

   B. 1–64

   C. 0–255

   D. 1–1005

9. When you're using EtherChannel on your switches and a link failure occurs, what controlling device notifies the EARL of the failure?

   A. SAMBA

   B. CPU

   C. EBC

   D. SAINT

10. From which of the following can PAgP form a bundle?

    A. Only statically assigned VLAN ports

    B. Dynamically assigned VLAN ports

    C. Dynamically and statically assigned VLAN ports

    D. Ports using different duplex types

11. What will the STP use to choose a forwarding port if the port costs are equal on a switch?

    A. Port ID

    B. MAC address

    C. Bridge name

    D. Hello timer

12. What is used to make a point-to-point port enter almost immediately into forwarding state by decreasing the time of the listening and learning states?

    A. PortUp

    B. PortFast

    C. Priority

    D. BackboneFast

13. What protocol sends Root Link Query BPDUs upon receiving an inferior BPDU?

    A. PortUp

    B. PortFast

    C. Priority

    D. BackboneFast

14. Which of the following commands is used to create a bundle on a 5000 series switch?

    A. `port set channel`

    B. `set port channel`

    C. `etherchannel on`

    D. `set bundle slot/port`

15. Which of the following commands is used to turn on BackboneFast?

    A. `set port channel backbonefast`

    B. `set spantree backbonefast on`

    C. `set spantree backbonefast enable`

    D. `set bundle enable slot/port`

16. Which of the following is true regarding PVST+? (Choose all that apply.)

    A. It is a Cisco proprietary protocol.

    B. It adds checking mechanisms to make sure there are no configuration problems on trunked ports and VLAN IDs across switches.

    C. It is set on a port-by-port basis.

    D. It enables Cisco switches to support the IEEE 802.1q standard.

17. What is the IEEE implementation of the STP?

    A. CST

    B. PVST

    C. PVST+

    D. 802.1u

18. How many spanning tree instances are defined with the PVST protocol running on a switch with six VLANs configured?

    A. 1005

    B. 1

    C. 6

    D. 64

19. How many spanning tree instances are defined with the CST protocol running on a switch with six VLANs configured?

    A. 1005

    B. 1

    C. 6

    D. 64

20. Which three of the following can STP use to determine the best path to the root bridge?

    A. STP protocol

    B. Port cost

    C. Path cost

    D. Bridge priority

    E. Port priority

Answers to Written Lab

1. `set spantree root 50-1000 dia 4`
2. `show spantree 1`
3. `set spantree portcost 2/1 10`
4. `set spantree portpri 1/1 20`
5. `show spantree 1/1`
6. `set spantree portvlanpri 1/1 16 1-2`
7. `set spantree portfast 2/1-12 enable`
8. `set spantree uplinkfast enable`
9. `set port channel 1/1-2 on`
10. `set spantree fwddelay 10`

Answers to Review Questions

1. C. The Spanning Tree Protocol was designed to help stop network loops that can happen with transparent bridge networks running redundant links.
2. A, B, C, E. The Bridge Protocol Data Units are sent out every 2 seconds by default and provide information to switches throughout the internetwork. This includes finding redundant links, electing the root bridge, monitoring the links in the spanning tree, and notifying other switches in the network about link failures.
3. C. VLAN 1 is a default VLAN and used for management by default.
4. D. The Cisco proprietary protocol Per-VLAN Spanning Tree (PVST) uses a separate instance of spanning tree for each and every VLAN.
5. C. The `set spantree root secondary` command enables you to configure a backup root bridge.
6. D. The 1900 switch can support up to 1005 VLANs but only up to 64 STP instances.
7. A. On a 1900 series IOS-based switch, use the `spantree priority 16` from interface configuration to change the port priority.
8. A. A priority from 0 to 63 can be set for each VLAN.
9. C. Should one link in the bundle fail, the Ethernet Bundle Controller (EBC) informs the Enhanced Address Recognition Logic (EARL) ASIC of the failure, and the EARL in turn ages out all addresses learned on that link.
10. A. PAgP bundled ports must all be configured the same, including the duplex and speed. Also, dynamic VLANs will not work, so VLANs must be assigned statically or they all must be trunked ports.
11. A. The switch will use the port ID to find the best forwarding port if the link costs are equal.
12. B. PortFast is used to put a blocked port into forwarding state immediately upon a bootup of a point-to-point device such as a workstation or server.

13. D. When BackboneFast is turned on, the Root Link Query BPDUs are sent out as soon as an inferior BPDU is received. This can enable faster convergence in the event of a backbone link failure.

14. B. The command `set port channel` *`slot/port`* `[on/off]` is used to create an EtherChannel bundle.

15. C. To enable BackboneFast on a switch, use the `set spantree backbonefast enable` command, which turns the protocol on for every VLAN.

16. A, B, D. PVST is proprietary to Cisco, and PVST+ is an extension of PVST. PVST+ enables non-PVST information to be accepted and received into PVST, adds configuration checking, and enables Cisco switches to support 802.1q.

17. A. The IEEE uses what is called Common Spanning Tree (CST), which is defined with IEEE 802.1q. The IEEE 802.1q defines one spanning tree instance for all VLANs.

18. C. The PVST protocol defines one instance of STP per VLAN.

19. B. The CST protocol defines one instance of STP per network regardless of the number of VLANs configured.

20. B, C, E. The port cost, path cost, and port priority are used to determine the best path to the root bridge.

Chapter

6

Inter-VLAN Routing

THE CCNP EXAM TOPICS COVERED IN THIS CHAPTER INCLUDE THE FOLLOWING:

- ✓ **Apply IOS command set to diagnose and troubleshoot a switched network problems**
- ✓ **Configure the VLAN Trunking Protocol**
- ✓ **Describe the VTP Trunking Protocol**
- ✓ **Configure a VLAN**
- ✓ **Facilitate InterVLAN Routing in a network containing both switches and routers**
- ✓ **Identify the network devices required to effect InterVLAN routing**

Routers break up broadcast domains. Layer 2 switches are used to break up collision domains. If you connect all your switches together, they will be in one broadcast domain. You can break up broadcast domains in layer 2 switched networks by creating virtual LANs (VLANs). However, the hosts within a VLAN can communicate only within the same VLAN by default.

For devices in one VLAN to communicate with devices in a different VLAN, they must be routed through a layer 3 device. This is called *inter-VLAN routing*. You can perform inter-VLAN routing with internal route processors in a layer 2 switch or with an external router called an *external route processor*.

In this chapter, we will cover both internal route processors and external route processors and how to configure them for inter-VLAN configuration.

Routing between VLANs

A VLAN's main job is to keep local traffic local, which it does very well. We have already mentioned in this book that you cannot communicate between VLANs without a router (layer 3 device), so understanding the configuration of VLANs and understanding routing go hand in hand.

Route processors provide the communication that hosts need between VLANs. However, if you are using local VLANs (see Chapter 3, "VLANs," for a thorough explanation), you want to design your networks so at least 80 percent of the users' traffic does not cross over into another VLAN. Therefore, you should design the network so that the users have access to local servers and other needed resources to prevent excessive packets from crossing the route processor.

Real World Scenario

ISL Network Cards

It is worth repeating that some network card vendors make NICs that can understand ISL and 802.1q encapsulated packets. When attempting to keep a large percentage of traffic from straying from the local VLAN, these cards might come in handy. It is possible to outfit a server with an ISL-aware NIC, and then the server can be a member of multiple VLANs and connect to a switch via a trunk link.

Example scenarios include installing one of these NICs in an e-mail server or a database server. Anything that a large number of people, across several VLANs, need to access is a candidate for this type of connection. It often makes more fiscal sense to upgrade a server NIC than to upgrade an entire router.

VLANs should be configured one for one with IP subnet designs. This means that you need to create a subnet mask for your network and then design your VLANs around the subnet design. For example, if you have engineering, marketing, sales, and support departments, you will typically—not always, but typically—create a subnet for each department, making sure you have room for growth. You would then create a VLAN for each department. In Chapter 3, we discussed the differences between local and end-to-end VLANs. Regardless of the type of VLAN you configure, each of these types would be associated with a subnet.

Each device within a VLAN would have a default gateway of the inter-VLAN device connected to its LAN. The inter-VLAN device would then route any packets with a destination not on the local network.

Before configuring routing between your VLANs, you need to understand the type of data sharing that is needed. By understanding the user and business needs, you can design the network with load balancing and/or redundant links if needed.

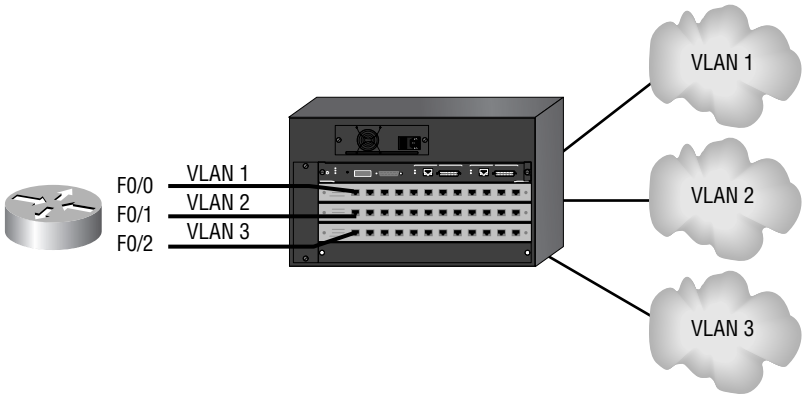
When configuring routing, you can choose from three options:

- Multiple links
- A single trunk link
- An internal or external route processor

Multiple Links

You can configure your VLANs to communicate by connecting a router interface into a switch port that is configured for each VLAN. Each workstation in the VLAN would have its default gateway configured for this router interface. Figure 6.1 shows how this might look in an internetwork.

FIGURE 6.1 Routers with multiple links



This is not a bad solution, but it does not scale well when you have more than four or so VLANs. It depends on the type of router you have. For every VLAN, you need to have a router interface (typically FastEthernet or Gigabit Ethernet), so a larger, more expensive router can have more interfaces without being saturated.

The more VLANs you have, the more router interfaces you have to purchase with the router. Also, you should have a fast router such as a high-end (at least a 4700 or 7200 series) router that can route quickly so the router does not become a bottleneck. Cost then becomes the issue with multiple links.

A Single Trunk Link

Another possible solution to routing between VLANs is creating a trunk link on a switch and then using a frame-tagging protocol such as ISL or 802.1q (which are used to identify frames as they traverse FastEthernet and Gigabit Ethernet links) on the router. Cisco calls this solution "router on a stick."

Real World Scenario

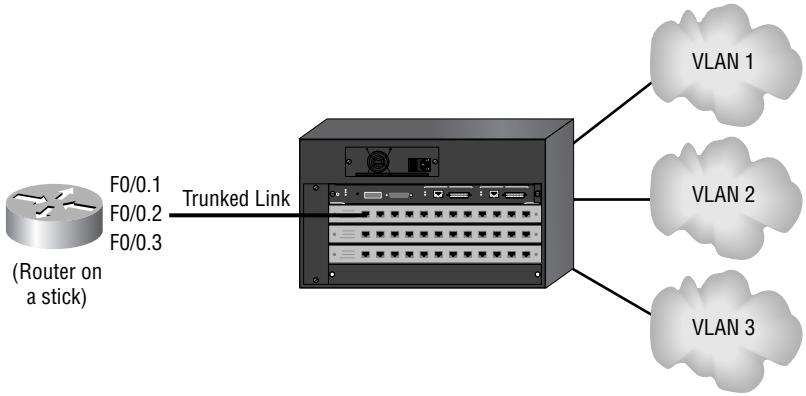
Sweet and Sour VLANs

Using multiple links is not a desirable thing to do in most cases, but there are times when it might be necessary. An example of such a case occurred in a rural area of China. Although large metropolitan areas usually have spare equipment available (if you can find it), finding a spare 3640 router to replace one that is down is pretty near impossible.

The company that this happened to did have some old 2500s that they managed to dig up from the closet that they were placed in when the 3640 went in. By attaching each VLAN to a separate Ethernet interface and connecting the routers together via the serial links, they had a solution that might be slow but worked.

Figure 6.2 shows how the internetwork might look with a single trunk link for all VLANs.

FIGURE 6.2 Single trunk link for all VLANs



This solution uses only one router interface on the router, but it also puts all the traffic on one interface. You really have to have a fast router to do this. Also, to even perform this function, you need, at minimum, a FastEthernet interface on a 2600 series router. ISL does not work on 10BaseT interfaces, nor would you want to run this on 10BaseT because it is processor- and bandwidth-intensive.

There are some really nice high-end routers that provide multi-layer switching by communicating to a NetFlow Feature Card (NFFC) in the Cisco Catalyst 5000 series of switches. The routers must have the IOS versions of 11.3.4 or later and run the Multi-Layer Switching Protocol (MLSP). The routers that support this are the 7500, 7200, 4500, and 4700 series of routers.

An Internal Route Processor

An *internal route processor* is a router on a card that fits inside the switch. This enables a switch to route packets without having the packets leave the box that the switch resides in. You need to add an internal route processor to a layer 2 device—for example, a 5000 Catalyst switch—to be able to provide forwarding of layer 3 packets without an external router.

An internal route processor makes layer 2 switches a multi-layer switch and can integrate layer 2 and layer 3 functionality in a single box. The 5000 series uses a *Route Switch Module (RSM)* or a *Route Switch Feature Card (RSFC)*, and the 6000 series uses the Multi-layer Switch Module (MSM) and the Multi-layer Switch Feature card (MSFC) to perform this function. The RSM, RSFC, MSM, and MSFC are configured in exactly the same way on their respective switches.

The RSM is a module plugged directly into the switch, which runs the Cisco IOS in order to perform inter-VLAN communication. The 5000 series switch sees the RSM as a single trunked port and a single MAC address. In other words, it appears as a router on a stick to the switch. The RSM interface to the switch is through VLAN 0 and VLAN 1. VLAN 0 is not accessible to the administrator. The RSM uses two channels, and VLAN 0 maps to channel 0, which supports communication between the RSM and the Catalyst 5000 series default VLAN (VLAN 1). VLAN 1 maps to channel 1. The MAC address assigned to the RSM is from the programmable read-only memory (PROM) on the line communication processor (LCP). This MAC address is used to identify the slot of the RSM and for diagnostics. The MAC addresses for VLAN 1 are assigned from a PROM that contains 512 MAC addresses. All routing interfaces except VLAN 0 use the base MAC address.

The RSFC is a daughter card for the Supervisor Engine II G and Supervisor III G cards. The RSFC is a fully functioning router running the Cisco IOS.

The MSM uses four internal full-duplex Gigabit Ethernet interfaces to connect to the switch and looks like an external router to the switch. These four

interfaces can be four separate links for four different VLANs, or they can be trunked and configured as one load-balanced link running EtherChannel and ISL or 802.1q. Subinterfaces are then used to configure each VLAN.

The MSFC is a daughter card for the Supervisor 1A and Supervisor 2 cards for a 6000 or 6500. It comes in two flavors, MSFC and MSFC2. In conjunction with a Policy Feature Card (PFC), the MSFC2 turns a 6500 series switch into a full-blown layer 3 switch, in addition to allowing all the functions of the MSM.

Using Inter-Switch Link Routing

The best solution to inter-VLAN routing is to provide a Gigabit Ethernet router interface for each VLAN. However, we have found that this can be cost prohibitive. What if you have 200 VLANs? Can you really afford a router with 200 Gigabit Ethernet ports? That would be an interesting configuration.

Cisco to the rescue! You can use either one FastEthernet or one Gigabit Ethernet interface for all your VLANs. Cisco has created the proprietary protocol Inter-Switch Link (ISL) to allow routing between VLANs with only one Ethernet interface. To run ISL, you need to have two VLAN-capable FastEthernet or Gigabit Ethernet devices, such as a Cisco 5000 switch and a 7000 series router.

Remember from Chapter 3 that ISL is a way of explicitly tagging VLAN information onto an Ethernet frame? This tagging information enables VLANs to be multiplexed over a trunk link through an external encapsulation method. By running ISL, you can interconnect multiple switches and still maintain VLAN information as traffic travels between switches on trunk links.

You can configure inter-VLAN routing with either an external router or an internal route processor that can be placed in a slot of a Catalyst switch. In this section, we'll take a look at both options.

Configuring ISL with an External Router

An external layer 3 device can be used to provide routing between VLANs. You can use almost any router to perform this function, but FastEthernet or Gigabit Ethernet is suggested. If trunking is used, the selected router must

support the VLAN tagging method used, whether it's ISL or 802.1q. If you have many small VLANs that perform at least 80 percent or more of their network function on the local VLAN, then you can probably get away with a 10Mbps Ethernet connection into each VLAN. Just remember that 10Mb interfaces do not support trunking, so the configuration would be one VLAN per interface. You should get FastEthernet if you can.

The external router can be configured to have one Ethernet interface for each VLAN, or you can use trunking protocols such as ISL or 802.1q to configure one FastEthernet or Gigabit Ethernet for all the VLANs that use subinterfaces. These subinterfaces give you an extremely flexible solution for providing routing between VLANs. To perform ISL routing on a single interface, the interface must be at least a FastEthernet interface that supports ISL routing. The Cisco 1750 is the least expensive router that can perform this function.

To configure ISL routing on a single interface, you must configure subinterfaces. These are configured by using the *type int.subinterface_number* command. Here is an example on a 2600 router with a FastEthernet interface:

```
Router#configure terminal
Enter configuration commands, one per line.  End with
   CNTL/Z.
Router(config)#interface f0/0.?
  <0-4294967295>  FastEthernet interface number

Router(config)#interface f0/0.1
Router(config-subif)#
```

Notice the number of subinterfaces available (4.2 billion). You can choose any number that feels good because the subinterfaces are only locally significant to the router. However, we usually like to choose the VLAN number for ease of administration. Notice that the prompt on the router is now telling you that you are configuring a subinterface (`config-subif`).

After you configure the subinterface number you want, you then need to define the type of encapsulation you are going to use. Here is an example of the different types of trunking protocols you can use:

```
Router(config-subif)#encapsulation ?
  dot1Q   IEEE 802.1Q Virtual LAN
  isl     Inter Switch Link - Virtual LAN encapsulation
```

```
sde     IEEE 802.10 Virtual LAN - Secure Data Exchange
tr-isl  Token Ring Inter Switch Link - Virtual LAN
  encapsulation
```

You're not done yet. You need to tell the subinterface which VLAN it is a member of, and you provide this information on the same line as the encapsulation command. Here is an example:

```
Router(config-subif)#encapsulation isl ?
  <1-1000>  Virtual LAN Identifier.
```

Notice that you can configure the subinterface to be a part of any VLAN up to 1000. The `dot1q` encapsulation is for the IEEE standard 802.1q trunking, and `isl` is for ISL encapsulation.

After you choose the interface and encapsulation type and VLAN number, configure the IP address that this subinterface is a member of. The complete configuration would look like this:

```
Router#configure terminal
Enter configuration commands, one per line.  End with
   CNTL/Z.
Router(config)#interface f0/0.1
Router(config-subif)#encapsulation isl 1
Router(config-subif)#ip address 172.16.10.1 255.255.255.0
```

The preceding configuration is for subinterface f0/0.1 to VLAN 1. You would create a subinterface for each VLAN. You can verify your configuration with the `show running-config` command:

```
!
interface FastEthernet0/0.1
 encapsulation isl 1
 ip address 172.16.10.1 255.255.255.0
!
```

Configuring ISL with an Internal Route Processor

If you do not have an external router or if you have many VLANs, you should use a RSM or RSFC to provide the layer 3 routing for your 5000 series switch.

The first thing you need to type in is the `show module` command so you can see the RSM. Notice in the following switch output that the 5000 switch

has an RSFC in slot 1, but it is in module 15. This information will enable you to connect and configure the internal route processor:

```
Todd5000> (enable) show module
Mod Slot Ports Module-Type                Model          Status
--- ---- ----- ------------------------  -------------- --------
1   1    2     1000BaseX Supervisor IIIG  WS-X5550       ok
15  1    1     Route Switch Feature Card  WS-F5541       ok
2   2    24    10/100BaseTX Ethernet      WS-X5225R      ok
3   3    2     UTP OC-3 Dual-Phy ATM      WS-X5156       ok
13  13         ASP/SRP

Mod Module-Name         Serial-Num
--- ------------------- --------------------
1                       00014364176
15                      14452699
2                       00017581709
3                       00014173130

Mod MAC-Address(es)                         Hw     Fw           Sw
--- --------------------------------------- ---    ---------- --------------
1   00-b0-c2-b2-d0-00 to 00-b0-c2-b2-d3-ff 1.1    5.1(1)     5.2(1)
15  00-30-f2-c8-11-00 to 00-30-f2-c8-11-3f 1.0    12.0(3c)W5 12.0(3c)W5(8a),
2   00-30-7b-36-2b-50 to 00-30-7b-36-2b-67 3.3    4.3(1)     5.2(1)
3   00-10-7b-42-e7-da                      2.4    1.3
                                                      11.3(8)WA4(11a)3.2(13)
```

Not only does the command `show module` provide the module and slot that each card is in, it provides the serial number and the modules' MAC addresses. After you find the module number, you can then connect to that module by using the `session` command. Here is an example:

```
Todd5000> (enable)
Todd5000> (enable) session 15
Trying Router-15...
Connected to Router-15.
Escape character is '^]'.
```

Module and slot will be the same number for most pieces of hardware, but there is a significant difference. The *slot* is the physical slot the device resides in. The *module* is the address used to administer the device. Usually, the only time the two are not the same number is when the device in question is a daughter card. It will reside in a slot and have a different number for the module address.

You are now connected to the internal route processor and can continue to configure the device as you would any other router. Notice in the following router output that we set the hostname and routing protocol as well:

```
Router>
Router>enable
Router#
Router#configure terminal
Enter configuration commands, one per line.  End with
   CNTL/Z.
Router(config)#hostname ToddRSM
ToddRSM(config)#router eigrp 10
ToddRSM(config-router)#network 172.16.0.0
```

As we mentioned, the route processor looks like any Cisco router, which is a really nice feature. It's just as important to configure the routing protocols on this device as it is to configure them on any other router. The route processor is able to handle most of the routing protocols that a traditional router can. Be careful of large routing tables, though.

Before we continue with configuring VLANs on the internal route processor, let's take a look at another 5000 series switch that has a Route Switch Module:

```
Todd5000> (enable) show module
Mod Module-Name  Ports Module-Type           Model      Serial-Num Status
--- ----------   ----- --------------------- ---------- ------------------
1                  2    100BaseTX Supervisor  WS-X5509    005147178 ok
2                 12    10/100BaseTX Ethernet WS-X5213A   005153813 ok
4                       Route Switch Ext Port
5                  1    Route Switch          WS-X5304    018465234 ok
```

```
Mod MAC-Address(es)                        Hw     Fw       Sw
--- -------------------------------------- ----   ------   --------------
1   00-e0-34-88-fc-00 to 00-e0-34-88-ff-ff  1.8    5.1(2)   4.5(5)
2   00-e0-1e-11-73-64 to 00-e0-1e-11-73-6f  1.1    1.4      4.5(5)
5   00-e0-1e-90-d2-bc to 00-e0-1e-90-d2-bd  7.6    20.14    11.3(8)WA4(11)

Mod Sub-Type Sub-Model Sub-Serial Sub-Hw
--- -------- --------- ---------- ------
1   EARL 1+  WS-F5511  0005059935 1.1
```

Notice that the RSM on the 5000 series is in slot/module 5. To configure the RSM, we would type **session 5**, as shown here:

```
Todd5000> (enable) session 5
Trying Router-5...
Connected to Router-5.
Escape character is '^]'.

Router>enable
Router#
```

After we have entered the CLI of the RSM, you can see that the `Router#` prompt appears just as it does on the RSFC. They are configured exactly the same.

Configuring VLANs on an RSM

Instead of creating subinterfaces as you would with an external router, you configure each VLAN with the `interface vlan #` command. Here is an example of how to configure the processor to route between three VLANs:

```
ToddRSM#configure terminal
ToddRSM(config)#interface vlan 1
ToddRSM(config-if)#ip address 172.16.1.1 255.255.255.0
ToddRSM(config-if)#interface vlan 2
ToddRSM(config-if)#ip address 172.16.2.1 255.255.255.0
ToddRSM(config-if)#interface vlan 3
ToddRSM(config-if)#ip address 172.16.3.1 255.255.255.0
ToddRSM(config-if)#no shutdown
```

The interesting part of the configuration is the necessary `no shutdown` command for each VLAN interface. Notice in the preceding configuration that we performed a `no shutdown` only on interface VLAN 3. Take a look

at the output of interface VLAN 2:

```
ToddRSM#show interface vlan 2
Vlan2 is administratively down, line protocol is down
  Hardware is Cat5k RP Virtual Ethernet, address is
    0030.f2c8.1138 (bia 0030.f2c8.1138)
```

It is important to think of each VLAN interface as a separate interface that needs an `IP address` and a `no shutdown` performed, just as with any other router interface.

You can then verify your configuration with the `show running-config` command:

```
ToddRSM#show running-config
Current configuration:
!
version 12.0
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname ToddRSM
!
interface Vlan1
 ip address 172.16.1.1 255.255.255.0
!
interface Vlan2
 ip address 172.16.2.1 255.255.255.0
!
interface Vlan3
 ip address 172.16.3.1 255.255.255.0
!
router eigrp 10
 network 172.16.0.0
```

To view the routing table on the internal processor, use the `show ip route` command:

```
ToddRSM#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP,
   M - [output cut]
Gateway of last resort is not set
```

```
     172.16.0.0/24 is subnetted, 3 subnets
C       172.16.3.0 is directly connected, Vlan3
C       172.16.2.0 is directly connected, Vlan2
C       172.16.1.0 is directly connected, Vlan1
C    127.0.0.0/8 is directly connected, Vlan0
ToddRSM#
```

OK, the most interesting part about the difference between the RSM and an external router is the presence of VLAN 0. Notice in the preceding `show ip route` output that VLAN 0 is connected via 127.0.0.0/8, which is a diagnostic IP address. Remember that VLAN 0 cannot be accessed by an administrator and is used to provide support for the communication between the RSM and the Catalyst 5000 switch.

VLAN 0 is used for administrative purposes but it is also used for telephones used in a voice-over IP network. On devices that support phone connectivity, the phone will dynamically configure the switch port to use VLAN 0. VLAN 0 can't be assigned to a port statically; it can be assigned only dynamically.

Assigning MAC Addresses to VLAN Interfaces

The RSM uses only one global MAC address for all VLAN interfaces on the device. If you want to assign a specific MAC address to a VLAN interface, use the `mac-address` command. You might want to configure this option to enhance the operation of the RSM interface. Here is an example:

```
ToddRSM#configure terminal
ToddRSM(config)#interface vlan 2
ToddRSM(config-if)#mac-address 4004.0144.0011
ToddRSM(config-if)#exit
ToddRSM(config)#exit
ToddRSM#show running-config
[oputput cut]
interface Vlan2
 mac-address 4004.0144.0011
 ip address 172.16.2.1 255.255.255.0
```

Defining a Default Gateway

One thing to keep in mind before configuring ISL on your switches is that the switches must be configured correctly with an IP address, subnet

mask, and default gateway. Understand that this has nothing to do with routing because the switches work only at layer 2. However, the switches need to communicate with IP through the network. Remember that this will not affect data that is passing through the switch. You can think of layer 2 switches as being just like any host on the network. To be able to send packets off the local network, you need to have a default gateway configured.

To configure a default gateway on a 5000 series switch, use the `set ip route` command:

```
Todd5000> (enable) set ip route 0.0.0.0 172.16.1.1
Route added.
```

You can also use the command `set ip route default 172.16.1.1`, which will configure the route the same as the `set ip route 0.0.0.0 172.16.1.1` will.

The IOS switch `default-gateway` command was covered in Chapter 2, "Connecting the Switch Block."

Summary

In this chapter, we described inter-VLAN routing issues and solutions. Because routers are needed to enable hosts on different networks to communicate, you also need to remember that a layer 3 device, either an external router or an internal route processor, is needed to allow inter-VLAN communication.

We discussed both internal route processors and external route processors and showed you how to use them for inter-VLAN configuration.

Exam Essentials

Know the difference between an internal and an external route processor. An external route processor is a standard router that is routing between VLANs, whereas an internal route processor is a

special card inside the switch that routes between VLANs. An external router can accept packets across a trunk terminating at a single Ethernet interface or it can have several connections, one per VLAN. The last method is required if there are only 10Mb Ethernet interfaces available.

Know how to configure VLANs on each of the routers. On an internal route processor, the router has VLAN interfaces as opposed to the Ethernet or serial interfaces found on an external router. The interfaces are accessed in the same fashion, but on an internal router, each VLAN interface gets an IP address and the `no shut` command must be issued to activate the interface.

On an external router, select the appropriate FastEthernet or Gigabit Ethernet interface and start making subinterfaces, preferably labeling them the same as the VLAN that will reside there. Configure each subinterface with the appropriate encapsulation and IP address and then issue the `no shut` command on the physical interface.

Know how to configure routing on the router and on the switch. Both internal and external route processors can be configured to route packets from one network to another based on routing protocol information. To configure a dynamic routing protocol, you must enter global configuration mode and use the `router` command followed by routing-protocol-specific information.

To configure routing on a switch, you must configure a default gateway on the switch. Use the command `set ip route` to accomplish this, pointing to an IP address that can forward packets to other networks, something like a router interface.

Key Terms

Before you take the exam, be sure you're familiar with the following terms:

- external route processor
- internal route processor
- inter-VLAN routing
- Route Switch Feature Card (RSFC)
- Route Switch Module (RSM)

Written Lab

Write the answers to the following questions:

1. Write the commands to configure ISL routing for VLAN 1 with an IP address of 172.16.10.1 with a 24 bit mask, on FastEthernet interface 0/0.
2. Write the command to view the different types of cards in a 5000 series switch.
3. Write the command to connect to an RSM module in slot 3.
4. Write the commands to configure two VLANs on an RSM. VLAN 1 has an IP address of 172.16.1.1, and VLAN 2 has an IP address of 172.16.2.1. Both addresses use a 24 bit mask.
5. Write the command to set a hardware address on the VLAN 2 interface of 4004.0144.0011.
6. What type of link is needed to run ISL routing on a FastEthernet interface?
7. What is the IEEE version of ISL?
8. True/False: You can assign a MAC address to a VLAN ISL interface.
9. How many VLANs can you create with subinterfaces on a FastEthernet interface?
10. What command would you use to see the configuration on a Catalyst 5000 switch?

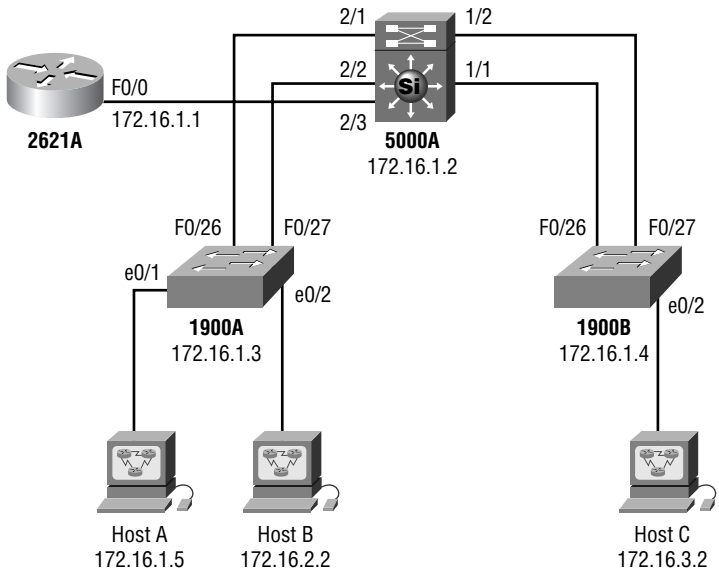
Hands-On Labs

In these hands-on labs, you will configure a 5000 series switch, two 1900 switches, and one 2621 router to provide ISL routing between VLANs. You will complete the following labs:

- External Inter-VLAN Routing
- Internal Inter-VLAN Routing

In both of the labs, refer to Figure 6.3 for configuring inter-VLAN communication.

FIGURE 6.3 Configuring inter-VLAN communication for hands-on labs



Lab 6.1: External Inter-VLAN Routing

In this lab, you'll configure the 2621 with ISL routing. You'll first configure the two 1900 switches, then the 5000 switch, and then the 2621 router.

Configuring the 1900A Switch

1. Plug into the 1900A console port and press K to enter the CLI.
2. Enter privileged mode by typing **enable**.
3. Enter configuration mode and set the hostname:

```
#config t
(config)#hostname 1900A
```

4. Set the user mode and privilege mode passwords:

```
1900A(config)#enable password level 1 cisco
1900A(config)#enable secret todd
```

5. Set the IP address of the switch by using the IP address assigned in Figure 6.3. Set the default gateway address by using interface f0/0 of the 2621 as the gateway:

```
1900A(config)#ip address 172.16.1.3 255.255.255.0
1900A(config)#ip default-gateway 172.16.1.1
```

6. Verify the IP configuration on the switch by typing **show ip**.

7. Set the VTP domain to **SwitchSim** and then make the switch a VTP client so that when you set the VLANs on the 5000 switch, the 1900A switch will automatically be updated with VLAN information:

```
1900A(config)#vtp domain SwitchSim
1900A(config)#vtp client
```

8. Set the FastEthernet interfaces to **trunk on** so that all VLAN information will be sent down both links from the 5000 series switch:

```
1900A(config)#int f0/26
1900A(config-if)#trunk on
1900A(config-if)#int f0/27
1900Aconfig-if)#trunk on
```

9. Configure the FastEthernet connection to the 5000 series switch to be full-duplex:

```
1900A(config)#int f0/26
1900A(config-if)#duplex full
1900A(config-if)#int f0/27
1900A(config-if)#duplex full
```

Configuring the 1900B Switch

1. Plug into the 1900B switch console port and press K to enter the CLI.

2. Enter privileged mode by typing **enable**.

3. Enter configuration mode and set the hostname:

```
#config t
(config)#hostname 1900B
```

4. Set the user mode and privilege mode passwords:

```
1900B(config)#enable password level 1 cisco
1900B(config)#enable secret todd
```

5. Set the IP address of the switch by using the IP address assigned in Figure 6.3. Set the default gateway address by using interface f0/0 of the 2621 as the gateway:

```
1900B(config)#ip address 172.16.1.4 255.255.255.0
1900B(config)#ip default-gateway 172.16.1.1
```

6. Verify the IP configuration on the switch by typing **show ip**.

7. Set the VTP domain to **SwitchSim** and then make the switch a VTP client so that when you set the VLANs on the 5000 switch, the 1900B switch will automatically be updated with VLAN information:

```
1900B(config)#vtp domain SwitchSim
1900B(config)#vtp client
```

8. Set the FastEthernet interfaces to **trunk on** so that all VLAN information will be sent down both links from the 5000 series switch:

```
1900B(config)#int f0/26
1900B(config-if)#trunk on
1900B(config-if)#int f0/27
1900B(config-if)#trunk on
```

9. Configure the FastEthernet connection to the 5000 series switch to be full-duplex:

```
1900B(config)#int f0/26
1900B(config-if)#duplex full
1900B(config-if)#int f0/27
1900B(config-if)#duplex full
```

10. Set the ports to configure an EtherChannel bundle when the 5000 series is configured. This can be run only on the supervisor card or a specific EtherChannel card. EtherChannel will be run only on the 1900B connection to the 5000 switch.

```
1900B(config-if)#port-channel mode on
```

Configuring the 5000 Series Switch

1. Connect your console cable to the 5000 series switch and press Enter. Press Enter at the password prompt; then again at the password prompt, type **enable** and press Enter.

2. Set the hostname of the switch:

```
#(enable)set system name Cat5000>
```

3. Set the user mode and privilege mode passwords:

```
Cat5000>(enable)set password [press enter]
Enter old password: [press enter]
Enter new password: [this doesn't show]
Retype new password: [this doesn't show]
Password changed.
Cat5000> (enable)set enablepass
Enter old password:[press enter]
Enter new password: [this doesn't show]
Retype new password: [this doesn't shoow]
Password changed.
Cat5000> (enable)
```

4. Set the IP address and default gateway of the switch:

```
Cat5000>(enable)set int sc0 172.16.1.2 255.255.255.0
Cat5000>(enable)set ip route default 172.16.1.1
```

5. Verify this configuration by typing **show int**.

6. Set the VTP domain name to **SwitchSim**:

```
Cat5000>(enable)set vtp domain SwitchSim
```

7. Set all ports connected to the 1900 switches as 100Mbps and full-duplex. The two ports on the supervisor engine are labeled 1/1 and 1/2 and run in only 100Mbps, so only the duplex can be set on those ports.

```
Cat5000> (enable) set port duplex 1/1 full
Port(s) 1/1 set to full-duplex.
Cat5000> (enable) set port duplex 1/2 full
Port(s) 1/2 set to full-duplex.
Cat5000> (enable) set port speed 2/1 100
Port(s) 2/1 speed set to 100Mbps.
Cat5000> (enable) set port speed 2/2 100
Port(s) 2/2 speed set to 100Mbps.
Cat5000> (enable) set port duplex 2/1 full
Port(s) 2/1 set to full-duplex.
```

```
Cat5000> (enable) set port duplex 2/2 full
Port(s) 2/2 set to full-duplex.
Cat5000> (enable)
```

8. It is possible that the ports on the 5000 have been disabled because of mismatched port configurations between the 1900 and 5000. Type the command **show port** ***slot/port*** to see the status. If it is disabled, use the **set port enable** ***slot/port*** command.

```
Cat5000> (enable) set port enable 1/1
Port 1/1 enabled.
```

9. Configure trunking on all ports connected to the 1900A and 1900B switches:

```
Cat5000> (enable) set trunk 2/1 on isl
Port(s) 2/1 trunk mode set to on.
Port(s) 2/1 trunk type set to isl.
Cat5000> (enable) set trunk 2/2 on isl
Port(s) 2/2 trunk mode set to on.
Port(s) 2/2 trunk type set to isl.
Cat5000> (enable) set trunk 1/1 on isl
Port(s) 1/1 trunk mode set to on.
Port(s) 1/1 trunk type set to isl.
Cat5000> (enable) set trunk 1/2 on isl
Port(s) 1/2 trunk mode set to on.
Port(s) 1/2 trunk type set to isl.
```

10. Verify that the trunk ports are working by typing **show trunk**:

```
Cat5000>(enable)show trunk
Port      Mode         Encapsulation  Status    Native vlan
--------  -----------  -------------  ---------  --------
 1/1      on           isl            trunking      1
 1/2      on           isl            trunking      1
 2/1      on           isl            trunking      1
 2/2      on           isl            trunking      1
 5/1      on           isl            trunking      1

[output cut]
```

11. Configure EtherChannel on both ports connected to the 1900B switch:

```
Cat5000> (enable) set port channel 1/1-2 on
Port(s) 1/1-2 channel mode set to on.
```

12. Verify that the EtherChannel is working by typing **show port channel**:

```
Cat5000> (enable) show port channel
Port  Status     Channel   Channel     Neighbor       Neighbor
                 mode      status      device           port
----- ---------- --------- ----------- --------------  -----
 1/1  connected  on        channel   cisco 1900  1900B  A
 1/2  connected  on        channel   cisco 1900  1900B  B
----- ---------- --------- ----------- --------------- -----
Cat5000> (enable)
```

13. At this point, the three switches should be up and working, and you should be able to ping all devices in the 172.16.1.0 network:

```
Cat5000> (enable) ping 172.16.1.3
172.16.1.3 is alive
Cat5000> (enable) ping 172.16.1.4
172.16.1.4 is alive
```

Configuring VLANs

Because the 5000 series switch is a VTP server and the two 1900 switches are VTP clients, you can configure VLANs on just the 5000 series switch, and the 5000 switch will automatically update the VTP NVRAM on the 1900 switches.

1. On the 5000 series switch console, create two new VLANs:

   VLAN 2: **Sales**

   VLAN 3: **Admin**

```
Cat5000> (enable) set vlan 2 name Sales
Vlan 2 configuration successful
Cat5000> (enable) set vlan 3 name Admin
Vlan 3 configuration successful
Cat5000>(enable)
```

2. Type the command **show vlan** to view the configured VLANs on the switch:

```
Cat5000>(enable)show vlan
VLAN Name                 Status    IfIndex Mod/Ports, Vlans
---- --------------    --------- ------- ------------------
1    default              active    5       2/3-12
2    Sales                active    10
3    Admin                active    11
1002 fddi-default         active    6
1003 token-ring-default   active    9
1004 fddinet-default      active    7
1005 trnet-default        active    8       1003
[output cut]
```

3. Verify that VTP is up and running correctly by telneting into 1900A and 1900B and typing **show vlan**. The same VLANs should appear if VTP is working properly. If not, verify that you spelled the VTP domain the same on all switches.

4. Configure Host A to be in VLAN 1, Host B to be in VLAN 2, and Host C to be in VLAN 3:

```
1900A#config t
Enter configuration commands, one per line.  End with
  CNTL/Z
1900A(config)#int e0/1
1900A(config-if)#vlan-membership static 1
1900A(config-if)#int e0/2
1900A(config-if)#vlan-membership static 2

1900B#config t
Enter configuration commands, one per line.  End with
  CNTL/Z
1900B(config)#int e0/2
1900B(config-if)#vlan-membership static 3
```

5. Type the **show vlan** command on the 1900B switch and verify that e0/2 is a member of VLAN 3. Type the same command on 1900A and verify that e0/1 is a member of VLAN 1 and that e0/2 is a member of VLAN 2.

```
1900B#show vlan
VLAN Name              Status     Ports
---------------------------------------------------
1    default           Enabled    1, 3-12, AUI, A, B
2    Sales             Enabled
3    Admin             Enabled    2
[output cut]
1900A#show vlan
VLAN Name              Status     Ports
---------------------------------------------------
1    default           Enabled    1, 3-12, AUI, A, B
2    Sales             Enabled    2
3    Admin             Enabled
[output cut]
```

6. Configure each host with the following IP addresses:

   Host A: 172.16.1.5/24 default gateway 172.16.1.1

   Host B: 172.16.2.2/24 default gateway 172.16.2.1

   Host C: 172.16.3.2/24 default gateway 172.16.3.1

7. Try pinging from host to host. This should fail. However, you should be able to ping from Host A to all switches in the network, and all switches should be able to ping to Host A because they are all in the same VLAN. To enable hosts in different VLANs to communicate, you need to configure inter-VLAN routing.

Configuring the 2621 Router

The 2621 router will provide the inter-VLAN routing and enable the hosts to communicate with each other.

1. Go to the privilege mode of the router and enter global configuration mode:

```
Router>enable
Router#configure terminal
Router(config)#
```

2. Set the hostname and passwords on the 2621 router:

```
Router(config)#hostname 2621A
2621A(config)#enable secret todd
```

```
2621A(config)#line console 0
2621A(config-line)password console
2621A(Config-line)login
2621A(config)#line vty 0 4
2621A(config-line)password telnet
2621A(Config-line)login
```

3. Configure the FastEthernet interface to run ISL routing for all three VLANs:

```
2621A(config-line)#exit
2621A(config)#interface f0/0.1
2621A(config-subif)#encapsulation isl 1
2621A(config-subif)#ip address 172.16.1.1 255.255.255.0
2621A(config-subif)#interface f0/0.2
2621A(config-subif)#encapsulation isl 2
2621A(config-subif)#ip address 172.16.2.1 255.255.255.0
2621A(config-subif)#interface f0/0.3
2621A(config-subif)#encapsulation isl 3
2621A(config-subif)#ip address 172.16.3.1 255.255.255.0
2621A(config-subif)#interface f0/0
2621A(config-if)#no shutdown
2621A(config-if)#
```

4. Before this will work, you need to set the port on the 5000 to trunk mode. Go to the 5000 switch and configure the port:

```
Cat5000> (enable) set trunk 2/3 on
Port(s) 2/3 trunk mode set to on.
Cat5000> (enable)
```

5. Test the configuration by pinging to all devices from the router:

```
2621A#ping 172.16.3.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.3.2, timeout
  is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/
   max = 1/1/4 ms
2621A#ping 172.16.1.3
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 172.16.1.3, timeout
  is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/
  max = 4/5/8 ms
2621A#ping 172.16.2.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.2.2, timeout
  is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/
  max = 4/5/8 ms
2621A#ping 172.16.1.5
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.2.2, timeout
  is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/
  max = 4/5/8 ms
2621A#ping 172.16.1.4
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.2.2, timeout
  is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/
  max = 4/5/8 ms
2621A#
```

The reason for the 80 percent success rate is that the IP hosts have not communicated before and the first ping timed out waiting for the ARP protocol to resolve the hardware addresses of each device.

6. Verify that all hosts can communicate by pinging from host to host.

Lab 6.2: Internal Inter-VLAN Routing

In this second lab, you'll configure the RSM in the 5000 switch for inter-VLAN routing using ISL. The 1900s will be configured first, then the 5000s. The 2621 router will not be needed in this lab.

1. Unplug the 2621 router from the 5000 series switch. The hosts should no longer be able to ping each other.

2. Configure the RSM on the 5000 series switch to provide inter-VLAN routing. Use the `show module` command to view the RSM card location:

```
Cat5000> (enable) show module
Mod Module-Name Ports Module-Type Model    Serial-Num Status
--- ----------- ------- -------------------- -------------------
1                2  100BaseTX Supervisor  WS-X5509    005147178 ok
2               12  10/100BaseTX Ethernet WS-X5213A   005153813 ok
4                   Route Switch Ext Port
5                1  Route Switch          WS-X5304    018465234 ok
```

3. Connect to the RSM through the 5000 console:

```
Cat5000> (enable) session 5
Trying Router-5...
Connected to Router-5.
Escape character is '^]'.

Router>
```

4. Configure three VLAN interfaces, one for each VLAN configured in the switched internetwork:

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with
  CNTL/Z.
Router(config)#hostname 5000RSM
5000RSM(config)#interface vlan 1
5000RSM(config-if)#ip address 172.16.1.1 255.255.255.0
5000RSM(config-if)#no shutdown
5000RSM(config-if)#interface vlan 2
5000RSM(config-if)#ip address 172.16.2.1 255.255.255.0
5000RSM(config-if)#no shutdown
5000RSM(config-if)#interface vlan 3
5000RSM(config-if)#ip address 172.16.3.1 255.255.255.0
5000RSM(config-if)#no shutdown
```

5. Verify that the RSM is working by pinging between hosts.

Review Questions

1. What command is used to connect to an RSM from a set-based switch CLI?

   A. `connect`

   B. `telnet`

   C. `session`

   D. `module`

2. What command will show you the hardware address of each card in a 5000 series switch?

   A. `sh cards`

   B. `show session`

   C. `show version`

   D. `show module`

3. What command is used to set a virtual hardware address on a VLAN interface?

   A. `mac-address` *`mac-address`*

   B. `config mac` *`slot/port mac-address`*

   C. `set vlan mac-address` *`mac-address`*

   D. `set mac` *`mac-address`*

4. What are the two types of frame-tagging encapsulation methods used with FastEthernet and Gigabit Ethernet trunk links? (Choose all that apply.)

   A. dot1q

   B. sde

   C. ISL

   D. tr-isl

5. What are the two options you can consider when you need to have inter-VLAN communication and you have only an external router? (Choose all that apply.)

   A. One router interface for every switch in the internetwork

   B. One router interface for every single VLAN

   C. Two router interfaces for every switch in the internetwork

   D. One router interface into one switch port running a trunking protocol

6. What is the correct configuration for a subinterface on a modular router?

   A. `int 10.f0/0`

   B. `int fa0/0.3980`

   C. `faste 0/0 subinterface 3`

   D. `set int f0/0.1`

7. Which of the following is true regarding layer 2 switches?

   A. They break up collision domains by default.

   B. They break up broadcast domains by default.

   C. They provide inter-VLAN routing by default.

   D. An external route processor can be attached to the backplane of the switch to provide inter-VLAN routing.

8. What are the types of internal route processors that can be used with Catalyst switches? (Choose all that apply.)

   A. FRM

   B. RSM

   C. MSM

   D. RSFC

9. Which of the following is true regarding the configuration between the different internal route processors?

   A. The 6000 series internal processors use the `set` commands.

   B. The 5000 series internal processors use the same Cisco IOS commands that a 1900 switch uses.

   C. The 8500 series of switches do not support internal route processors.

   D. There is no difference in the configuration between the different internal route processors.

10. Which two commands can be used to set a default route on a 5000 series switch to 172.16.1.1? (Choose all that apply.)

    A. `route add 0.0.0.0 0.0.0.0 172.16.1.1`

    B. `set ip route default 0.0.0.0 172.16.1.1`

    C. `set ip route default 172.16.1.1`

    D. `set ip route 0.0.0.0 172.16.1.1`

11. Which of the following is used to configure VLAN 1 on an internal route processor with an IP address of 208.211.78.200/28?

    A. `set vlan1 ip address 208.21.78.200 255.255.255.240`

    B. `config t, vlan1 ip address 208.21.78.200 255.255.255.240`

    C. `int vlan 1, ip address 208.211.78.200 255.255.255.240`

    D. `set int vlan1, ip address 208.211.78.200 255.255.255.224`

12. Which of the following is true?

    A. You are required to assign a password to an RSM interface CLI.

    B. You must perform a `no shutdown` command for every subinterface on an external route processor.

    C. You must perform a `no shutdown` command for every VLAN on an internal route processor.

    D. You can use a 2500 series router for ISL routing.

13. Which of the following internal route processors is a daughter card?

    A. RSM

    B. RSFM

    C. RSFC

    D. MSM

14. If you wanted to view the VLAN configuration of an RSM card, which command would you use?

    A. `sh vlan`

    B. `show config`

    C. `sho run`

    D. `sh port` *`slot/type`*

15. To view the routing table on the internal route processor, use the _____ command.

    A. `show routing protocol`

    B. `show vlan`

    C. `show config`

    D. `show ip route`

16. If you assigned a virtual hardware address to VLAN 2 on an internal route processor, how do you view this configuration? (Choose all that apply.)

    A. `show virtual address`

    B. `show vlan 2`

    C. `show interface vlan 2`

    D. `show run`

17. Which command will display the BIA address of a VLAN on an internal route processor?

    A. `show virtual address`

    B. `show vlan 2`

    C. `show interface vlan 2`

    D. `show run`

18. What type of link must be used on a switch port if you are running ISL on an external router interface?

    A. Access

    B. Trunk

    C. Virtual

    D. Ethernet

19. Which of the following will set VLAN 3 to run ISL on an external route processor with one FastEthernet interface?

    A. `(config)#encap isl vlan3`

    B. `(config)#encap vlan3 isl`

    C. `(config-if)#encap isl 3`

    D. `(config-if)encap 3 isl`

20. Which of the following is used to provide support for the communication between the RSM and the Catalyst 5000 switch?

    A. ISL

    B. VLAN 1

    C. VLAN 0

    D. 127.0.0.1/8

Answers to Written Lab

1. Router#**configure terminal**
   Enter configuration commands, one per line. End with CNTL/Z.
   Router(config)#**interface f0/0.1**
   Router(config-subif)#**encapsulation isl 1**
   Router(config-subif)#**ip address 172.16.10.1 255.255.255.0**
2. show module
3. session 3
4. ToddRSM#**configure terminal**
   ToddRSM(config)#**interface vlan 1**
   ToddRSM(config-if)#**ip address 172.16.1.1 255.255.255.0**
   ToddRSM(config-if)#**no shutdown**
   ToddRSM(config-if)#**interface vlan 2**
   ToddRSM(config-if)#**ip address 172.16.2.1 255.255.255.0**
   ToddRSM(config-if)#**no shutdown**
5. ToddRSM#**configure terminal**
   ToddRSM(config)#**interface vlan 2**
   ToddRSM(config-if)#**mac-address 4004.0144.0011**
6. Trunk
7. 802.1q
8. True
9. 1000
10. show config

Answers to Review Questions

1. C. The `session` command is used to create a session from the switch CLI to the RSM CLI.
2. D. The `show module` command displays the type of cards in each slot, the hardware address, and the serial number of each card.
3. A. The command `mac-address` *`mac_address`* is used under the `interface vlan #` command to set a virtual MAC address to a VLAN interface.
4. A, C. The frame-tagging encapsulation methods are `dot1q` and ISL. `dot1q` is the IEEE standard for frame tagging between disparate systems. ISL is a Cisco proprietary FastEthernet and Gigabit Ethernet frame-tagging method.
5. B, D. If you have an external router, you certainly can have a router interface for every single VLAN. However, you can also have one FastEthernet or Gigabit Ethernet interface connected into a switch running a trunking protocol that will provide inter-VLAN routing.
6. B. You can create subinterfaces on a FastEthernet or Gigabit Ethernet modular interface by using the *`type slot/port.subinterface_number`* command.
7. A. Layer 2 switches break up only collision domains by default. A layer 3 device is needed for inter-VLAN routing. An external route processor cannot attach to the backplane of a switch, only into a switch port.
8. B, C, D. The 5000 series uses the RSM or a Route Switch Feature Card (RSFC), and the 6000 series uses the Multi-layer Switch Module (MSM).
9. D. There is absolutely no difference in the configuration of the different types of internal route processors.
10. C, D. The command `set ip route default` and the command `set ip route 0.0.0.0` are the same command and can be used to set a default gateway on a 5000 series switch.
11. C. The command `interface vlan #` is used to create a VLAN interface. The IP address of the interface is then configured with the `ip address` command.

12. C. An external route processor configured with subinterfaces does not need a shutdown performed on each subinterface, only the main interface. However, an internal route processor must have a `no shutdown` command performed under every VLAN interface.

13. C. The Route Switch Feature Card (RSFC) is a daughter card for the Supervisor Engine II G and Supervisor III G cards. The RSFC is a fully functioning router running the Cisco IOS.

14. C. The RSM commands are the same as they are for any Cisco IOS router, and `show running-config` is used to view the current configuration.

15. D. To view the routing table on the internal processor, use the `show ip route` command, just as you would with any IOS-based router.

16. C, D. The commands `show interface vlan #` and `show running-config` will display the virtual hardware address of an interface if set.

17. C. The command `show interface vlan` *`vlan#`* will show both the virtual MAC address, if set, and the burned-in address (BIA) of the VLAN interface.

18. B. A switch port must be configured with a trunking protocol to run ISL inter-VLAN communication to a single router interface.

19. C. The subinterface command `encapsulation` *`type vlan`* is used to set the VLAN ID and encapsulation method on a subinterface.

20. C. VLAN 0, which cannot be accessed by an administrator, is used to provide support for the communication between the RSM and the Catalyst 5000 switch.

Chapter 7

Multi-Layer Switching (MLS)

THE CCNP EXAM TOPICS COVERED IN THIS CHAPTER INCLUDE THE FOLLOWING:

- ✓ Identify the components necessary to effect multiplayer switching
- ✓ Apply flow masks to influence the type of MLS cache
- ✓ Describe layer 2, 3, 4 and multiplayer switching
- ✓ Verify existing flow entries in the MLS cache
- ✓ Describe how MLS functions on a switch
- ✓ Configure a switch to participate in multilayer switching

In this chapter, we'll discuss *Multi-Layer Switching (MLS)*, which is part of the Bridging/Switching group of topics outlined by Cisco for the Switching exam (640-604).

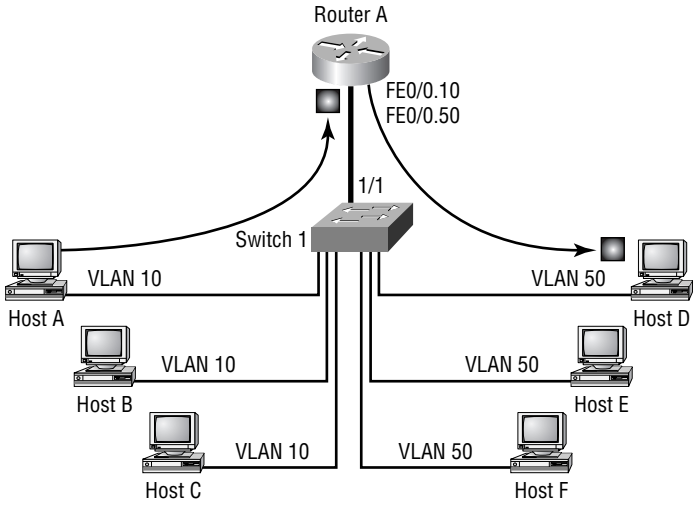
Why MLS? Why do you need layer 3 switching when you have layer 3 routing? The answer to both of these questions is simple: enhanced performance. Why do you implement any features on any piece of Cisco equipment? To increase performance and take advantage of the robust feature set provided by Cisco.

Understanding the Fundamentals of MLS

You have undoubtedly heard of the term "*router on a stick*." Figure 7.1 depicts the router on a stick architecture. As you can see from the diagram, there are multiple hosts using two separate VLAN assignments. One segment is running on VLAN 10, and the other segment is running on VLAN 50. Both VLANs are connected to the same switch. The switch is then connected to a router. Here we show an external router, but an RSM provides the same functionality, just internally.

By now you understand that for Host A on VLAN 10 to communicate to Host D on VLAN 50, packets must be routed through Router A. Because of the VLAN assignments, the switch must send the packet to the router on interface FE0/0.10. The router knows that the route to the network assigned to VLAN 50 is through interface FE0/0.50. The packet is then sent back to the switch and forwarded to Host D.

FIGURE 7.1 Router on a stick diagram



Now back to our original question. Why use MLS? You can see in Figure 7.1 that it is very inefficient to have to use a router to move a packet from Host A to Host D when they are connected to the same switch. MLS is used to bypass the router on subsequent packets of the same flow. A *flow* is a table entry for a specific conversation, created by using source and destination header information for layers 3 and 4. The switch caches the routing information for that particular flow to make changes to future packets. Several fields within a packet make it unique:

- Source and destination IP addresses
- Source and destination MAC addresses
- Type of Service (TOS)
- Protocol type (for example, HTTP, FTP, ICMP, and so on)

These are just some of the characteristics of a packet that can be used to establish a flow. A switch can be configured to support simple flows, such as IP address to IP address, or the switch can support complex flows dealing with port and protocol information.

To summarize, we use MLS to enable the switch to forward the first packet in the flow to the router and then learn what should be done with the rest of the packets in the flow so the router doesn't need to route them. In

Figure 7.1, the switch will make the necessary VLAN and destination MAC address changes in the subsequent packets.

Large Packet Streams

MLS tends to work better when the packet stream is fairly large. If a user is browsing the corporate intranet, they might be getting information from multiple servers located in various areas. If that same user is downloading a file via FTP, it is easy to see that the hundreds of fragments are all coming from the same place and going to the same place. Only the initial fragment needs to be routed; the rest of them are layer 3 switched.

For the best results, use MLS when large files are accessed or when the same type of information is accessed on a frequent basis. Users checking their e-mail every minute would be an example of an application that generates small but frequent packets.

MLS Requirements

Cisco Catalyst switches require additional hardware to make use of the packet header information. Catalyst 5000 switches use the *NetFlow Feature Card (NFFC)* to gather this information and cache it. Catalyst 6000 series switches use the *Multi-layer Switch Feature Card (MSFC)* and the *Policy Feature Card (PFC)* to gather and cache header information. A detailed process, which will be discussed later in this chapter, enables switches to establish flows.

MLS requires three components to function in any network (we have already briefly discussed two of them):

- *Multi-layer Switching Route Processor (MLS-RP)* is a directly attached router. This can be an MLS-capable external router or an RSM installed in the switch.
- *Multi-layer Switching Switch Engine (MLS-SE)* is an MLS-capable switch (a 5000 with an NFFC or a 6000 with an MSFC and PFC).
- *Multi-layer Switching Protocol (MLSP)* is a protocol that runs on the router and enables it to communicate to the MLS-SE regarding topology or security changes.

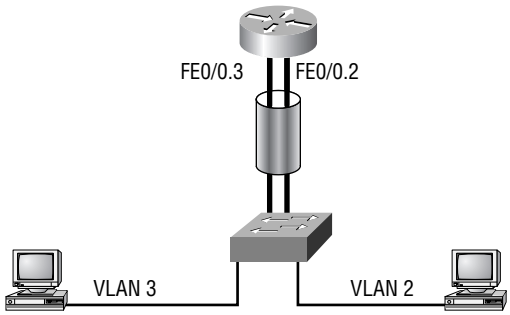
Now that you have a basic understanding of what MLS does and what is required for MLS to function in a network, let's get into the nitty-gritty of how it works. Throughout the rest of the chapter, you will see the preceding abbreviations many times.

MLS Procedures

We discussed the three required components of MLS. It is important to understand how they work together to enable layer 3 switching. Let's look at a sample network topology that will support MLS.

Figure 7.2 shows a simple architecture of a router and a switch with two connected hosts on the switch. Again, the hosts have different VLAN assignments, requiring the router's intervention to route packets. Notice that the figure depicts the main interface with two subinterfaces, FE0/0.2 and FE0/0.3. As it stands, the current topology requires that all packets sent from the client on VLAN 3 to the client on VLAN 2 be routed by the external router. If there are a large number of packets, this creates a lot of unnecessary work.

FIGURE 7.2 MLS example topology



MLS follows a four-step process to establish the layer 3 switching functionality. These four steps can then be broken down into more detailed processes, which will be discussed shortly. If these descriptions leave you a bit confused, the detailed explanation should clear things up. The four steps required to enable MLS are as follows:

MLSP discovery The MLS-RP uses MLSP to send hello packets out all interfaces to discover any MLS-SE devices and establish the MLS-RP/MLS-SE neighbor relationships.

Identification of candidate packets The NFFC or PFC watches incoming packets and as it forwards the packets to the router, creates partial cache entries for them, thus identifying the packets as potential candidates for a flow. A candidate packet is one that has yet to return from the router.

Identification of enable packets The NFFC or PFC watches packets coming from the MLS-RP and tries to match them with candidate packet entries. If matches are made, the packets are tagged as enable packets and a shortcut forwarding entry is made in the CAM table. This shortcut tells the switch how to duplicate the effect of routing. Everything that the router did to the packet, the switch will now be able to do.

Subsequent flow packets are layer 3 switched Incoming packets are compared against CAM table entries. If the packets match the flow criteria, the switch will take the shortcut information, make any necessary changes, and the packet will be directly forwarded to the appropriate exit port for the flow.

As we said, the preceding list is an overview of the steps that must take place before packets can be switched at layer 3. We'll discuss each step in detail next.

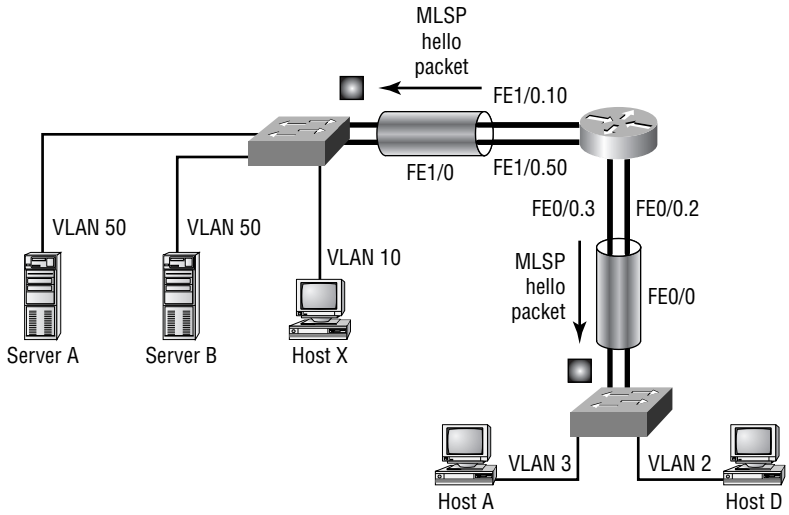
MLSP Discovery

Switches need routers to perform the initial route table lookup and the packet rewrite. This dependency requires that MLS adjacencies are established between the switch and the router. This is accomplished by using MLSP.

Initially, the router, or MLS-RP, sends hello packets containing all the MAC addresses and VLANs configured for use on the router. These messages are sent every 15 seconds to a layer 2 multicast address of 01-00-0C-DD-DD-DD. This is the address for the CGMP process on a Cisco switch. CGMP is covered in detail in Chapter 8, "Multicast," and Chapter 9, "Configuring Multicast." The intended recipients of these hello packets are the MLS-SE devices on the network.

When an MLS-SE receives the information, it makes an entry in the CAM table of all the MLS-RP devices in the layer 2 network. Layer 2 is mentioned because MLS-SE devices are not concerned with devices that are not directly connected to layer 2 devices, such as switches. Figure 7.3 depicts the MLSP discovery process.

FIGURE 7.3 MLSP discovery



Part of the information that is stored in the CAM table after an MLSP hello packet is received is an ID called an XTAG. The following is a description of the significance and purpose of the XTAG.

XTAGs

An *XTAG* is a unique identifier that MLS switches use to keep track of the MLS routers in the network. All the MAC addresses and VLANs in use on the MLS-RP are associated with the XTAG value in the CAM table.

The following output is from a Catalyst 6509 with an MSFC and PFC. The `show mls` command was issued to provide the output:

```
Switch1> (enable) show mls
Total packets switched = 4294967295
Total Active MLS entries = 85
IP Multilayer switching aging time = 256 seconds
IP Multilayer switching fast aging time = 0 seconds,
  packet
threshold = 0
IP Current flow mask is Destination flow
Active IP MLS entries = 85
Netflow Data Export version: 7
```

```
Netflow Data Export disabled
Netflow Data Export port/host is not configured.
Total packets exported = 0

IP MSFC ID      Module XTAG MAC               Vlans
--------------- ------ ---- ----------------- ----------
172.16.100.5    15     1    00-d0-bc-e3-70-b1 2,3

IPX Multilayer switching aging time = 256 seconds
IPX flow mask is Destination flow
IPX max hop is 0
Active IPX MLS entries = 0

IPX MSFC ID     Module XTAG MAC               Vlans
--------------- ------ ---- ----------------- ----------
172.16.100.5    15     1    -                 -

Switch1> (enable)
```

You can clearly see that the MSFC has been assigned the XTAG value of 1. The MSFC is a daughter card residing on the Supervisor card, which is why it uses module 15. The MSFC receives the assignment because the MSFC was configured as the MLS-RP. In this example, only one MAC address is associated with XTAG 1. However, two VLANs are associated with it.

MLS Cache

After MLS-SEs have established CAM entries for MLS-RPs, the switch is ready to start scanning packets and creating cache entries. This was described previously as identification of candidate and enable packets.

The cache entries are made in order to maintain flow data. Flow data enables the MLS-SE to rewrite the packets with the new source and destination MAC address and then forward the packets. All this is done without sending the packets to the router for a route lookup and to be rewritten.

Cache entries happen in two steps:

- Candidate packet entries
- Enable packet entries

After these entries have been made in the MLS-SE, subsequent packets are matched against existing flow entries and dealt with accordingly.

Identifying Candidate Packets

The process of identifying *candidate packets* is quite simple. As has already been established, the MLS-SE has MAC address entries for any and all interfaces that come from the MLS-RP. Using this information, the MLS-SE starts watching for incoming frames destined for any MLS-RP-related MAC addresses.

An incoming frame will match one of the following three criteria:

- Not destined for an MLS-RP MAC address
- Destined for an MLS-RP MAC address, and a cache entry already exists for this flow
- Destined for an MLS-RP MAC address, but no cache entry exists for this flow

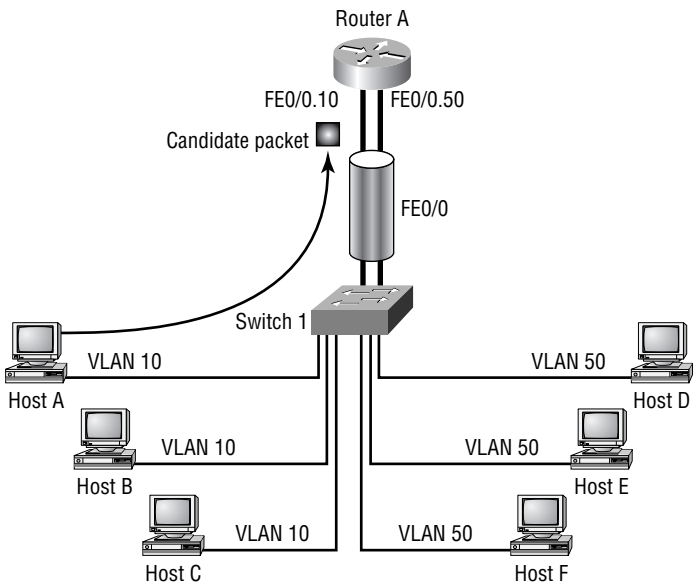
Different actions will be taken by the MLS-SE, depending on which criteria match.

Destination Other Than the MLS-RP

If the incoming frame is not destined for a MAC address associated with the MLS-RP, no cache entry is made. No cache entry is made because MLS is used to avoid additional route lookups. If the frame is destined to another MAC address in the CAM table, the frame is layer 2 switched.

Figure 7.4 depicts the occurrence of a candidate packet.

FIGURE 7.4 Candidate packet



Cache Entry Exists

When frames destined for an MLS-RP MAC address enter the switch, the switch checks whether a cache entry has been made that matches the attributes of the current packet.

As was mentioned briefly previously, each frame has distinguishing characteristics or attributes that enable the MLS-SE to categorize a packet into a flow. A switch can place all packets from a particular IP address and destined for a different IP address, into a flow. A flow entry can use IP addresses as well as, optionally, layer 4 information. The MLS-SE uses these cache attributes to match header information in future incoming packets. If an incoming packet has the same attributes as an established flow cache entry, the packet is layer 3– or shortcut-switched.

No Cache Entry

When an incoming frame, destined for the MLS-RP, is compared against the cache and no existing flow entry is found, a new cache entry is made. At this point, the packet is tagged as a candidate packet.

After the cache entry is made, the packet is forwarded to the router (MLS-RP) for normal processing. Here the router performs the route lookup, rewrites the layer 2 header, and sends the packet out the next-hop interface, whichever it might be.

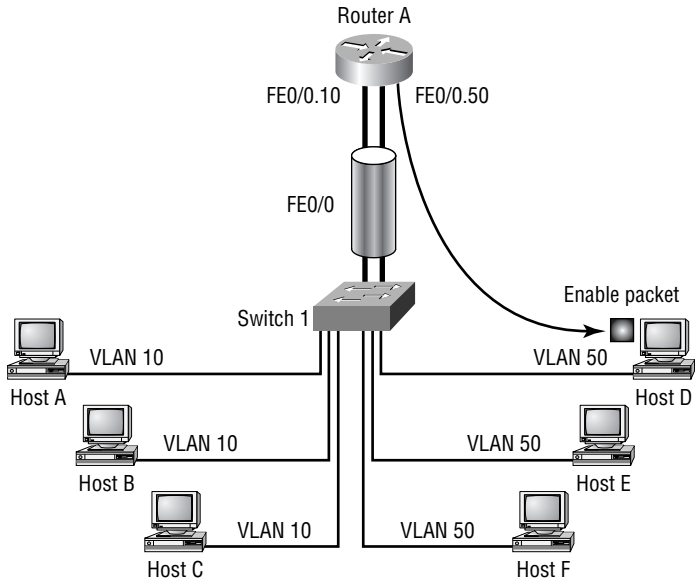
The state of the MLS cache is only partial at this stage. A complete flow cache has not been established because the MLS-SE has seen a packet only come in and be forwarded to the router. It still needs to see the packet come back from the router before the flow is complete.

Identifying Enable Packets

Enable packets are the missing piece of the flow cache puzzle. Just as the MLS switch watched all incoming frames destined for the MLS router's MAC addresses, it also watches all the packets coming from the MLS router.

It watches these packets, hoping for a match with the candidate packet cache entry. If it can make the match, the packet is tagged as an enable packet and the remaining elements of the flow cache are completed in the CAM table. Figure 7.5 depicts the occurrence of an enable packet.

FIGURE 7.5 Enable packet



The match is made by using the following criteria:

- The source MAC address is from an MLS-RP.
- The destination IP matches the destination IP of a candidate packet.
- The source MAC address is associated with the same XTAG value as the candidate packet's destination MAC address.

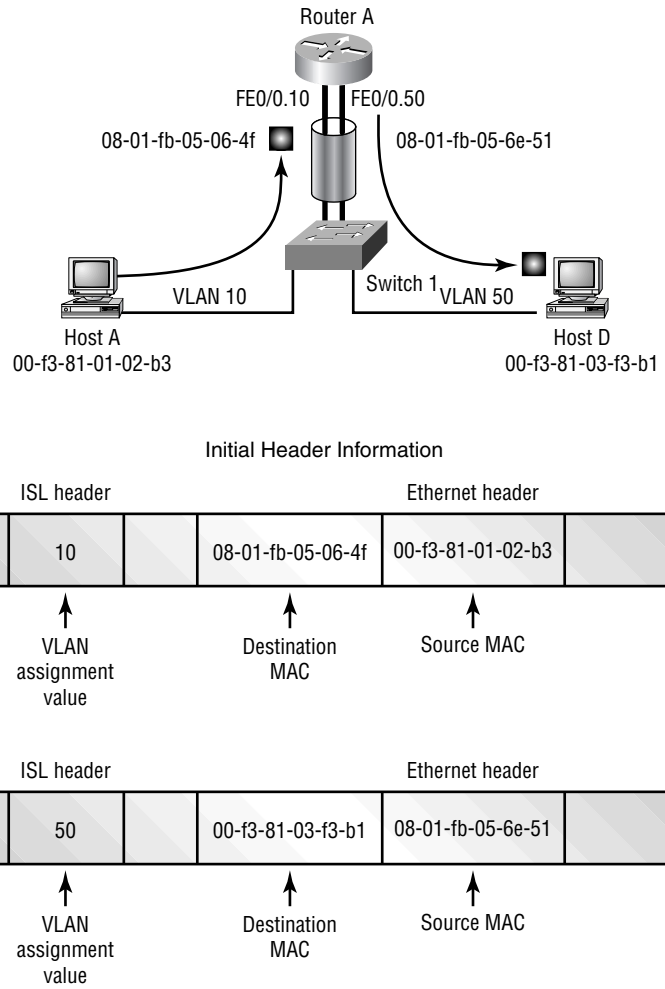
If all three of these criteria are met, the MLS-SE completes the shortcut cache entry.

Frame Modification

It is important to understand that this shortcut switching occurs at layer 3. The layer 2 frames that are a part of the conversation but come after the first frame are rewritten by the switch. Normally, a router (layer 3 device) would rewrite the frame with the necessary information. A rewrite consists of changing the VLAN assignment, the source and destination MAC addresses, and the checksums. The MLS-SE can also modify the TTL, TOS, and encapsulation.

Because these packets are no longer sent to the router, the MLS-SE must perform the rewrite function. When the switch changes the source and destination MAC address, the MLS-SE uses the MAC address of the MLS-RP for the source, and it changes the destination MAC to the MAC of the directly connected host. Through this procedure, the frame appears to the destination host as if it had come through the router. Figure 7.6 depicts the differences between the incoming frame and the exiting frame.

FIGURE 7.6 Frame modification



Subsequent Packets

After the candidate and enable packets have been identified and a shortcut, or flow cache, has been established, subsequent packets are forwarded by the switch to the destination without the use of the router. Because the MLS-SE has the capability to rewrite the frames, it can make the necessary modifications and forward the frame directly to the destination host.

The MLS-SE caches the necessary information, such as the source and destination IP addresses, the source and destination MAC addresses, and the MLS-RP-related MAC addresses. Using this information, the MLS-SE is then capable of identifying packets belonging to a specific flow, rewriting the frame, and forwarding the packets to the proper destination.

Disabling MLS

There is a right way and a wrong way to disable MLS on a router or switch. Both methods will be discussed here.

The Right Way

The correct way to disable MLS depends on the equipment you are using. Disabling MLS on a router can be paralleled with disabling MLS on an MSFC for a 6500 series switch. The command is even the same: `no mls rp ip` issued from the interface on either the router or the MSFC. To disable it completely, you can issue the same command from global configuration mode. The consequences of this action vary depending on the system on which it is issued. When the command is issued on the router, the router alone disables MLS. When it's issued on an MSFC, MLS is disabled on the MSFC and the switch itself.

MLS is enabled by default for IP traffic and disabled for IPX. To disable MLS on a 5000 series switch, use the `set mls disable` command. On a 6000 series, MLS should be disabled by issuing the `no ip mls` command on the MSFC.

The Wrong Way

There are several ways to inadvertently disable MLS on switches. Some are temporary, and others are permanent. Here is a list of MSFC/router commands that can disable MLS:

- `no ip routing`
- `ip security`

- `ip tcp compression-connections`
- `ip tcp header-compression`
- `clear ip route`

By disabling IP routing on the MSFC or router, you automatically disable MLS. The `ip security` command disables MLS on the interface to which the command is applied. The same results occur with the `ip tcp` compression commands. Finally, the `clear ip route` command simply clears the MLS cache entries, and the flow caches must be reestablished.

Configuring MLS-RP

To fully enable MLS, you must properly configure all participating devices. This section will cover the different configurations and settings that must be executed on the MLS-RP. Remember, the MLS-RP can be an external router, an RSM on a 5000 series switch, or an MSFC on a 6000 series switch.

We will discuss optional configuration settings. These options depend on the existing layer 2 network and configuration. All the remaining subsections, except "Verifying the MLS Configuration," apply only to external routers. We will start with the most basic and essential commands and then move on to management commands that can be used for verification and troubleshooting if necessary.

Enabling MLS

Although MLS is enabled on an MSFC, other routers might or might not need MLS enabled before it can be used. To enable MLS on a route processor, type the command `mls rp ip` while in global configuration mode. Much like the `ip routing` command, enabling MLS on a router just begins the process; you still need to configure more. Here is an example:

```
RouterA#configure terminal
Enter configuration commands, one per line.  End with
  CNTL/Z.
RouterA(config)#mls rp ip
```

```
RouterA(config)#^Z
RouterA#

!
ip subnet-zero
mls rp ip
!
```

Enabling MLS on the router is just the tip of the iceberg as far as required configuration tasks. We'll continue with the domain information that is needed.

VTP Domain Assignments

If a router interface is connected to a switch that is a VTP server or client, assigning the VLAN Trunk Protocol (VTP) domain is also a necessary step for MLS to work properly. It is very important to note that this step should be executed before any further MLS interface-specific commands are entered.

Failing to assign the VTP domain before configuring interfaces will place interfaces into a "null domain" rather than the proper one. Fixing this requires disabling MLS on the interfaces, and then fixing the domain and adding the interfaces back in.

Verifying the VTP Domain

First you should verify which VTP domain the interface belongs to. This is done with the `show vtp domain` command from the switch. You can also obtain this information by looking at the switch configuration. Here are the two examples:

```
switch1> show vtp domain
Domain Name  Domain Index VTP Version Local Mode  Password
-----------  ------------ ----------- ----------  --------
test         1            2           server      -
```

```
Vlan-count Max-vlan-storage Config Revision Notifications
---------- ---------------- -------------- -------------
7          1023             2              disabled

Last Updater   V2 Mode  Pruning  PruneEligible on Vlans
-------------- -------- -------- --------------------------
172.16.10.1    disabled disabled 2-1000
switch1>

switch1> (enable) write terminal
.....
.........
.........
.........
.........
..
-- ommitted text --
!
#vtp
set vtp domain test
set vtp mode server
```

VTP Interface Configuration

After you have the VTP domain name, you are ready to assign the router interface to that VTP domain. This is done with the execution of the command `mls rp vtp-domain` *`domain_name`* on the specified interface.

Here is an example:

```
RouterA#configure terminal
Enter configuration commands, one per line.  End with
  CNTL/Z.
RouterA(config)#interface fastethernet 4/0
RouterA(config-if)#mls rp vtp-domain test
RouterA(config-if)#^Z
RouterA#
```

```
!
interface FastEthernet4/0
 ip address 172.16.10.1 255.255.255.0
 no ip directed-broadcast
 no ip route-cache
 no ip mroute-cache
 mls rp vtp-domain test
!
```

VLAN Assignments

The command to establish a VLAN is used only if an external router's interface is not using ISL or 802.1q encapsulation. (RSMs and MSFCs use logical VLAN interfaces.) An example is a router that has two physical interfaces connected to the same switch, each to a different VLAN. This scenario doesn't require that the router be aware of VLAN assignments and would typically be found on routers that have only 10Mb interfaces.

If you wish to enable MLS on interfaces that don't use VLANs, you can issue the `mls rp vlan-id` *`vlan_id_number`* command to assign a VLAN to the interface. Here is an example:

```
RouterA#configure terminal
Enter configuration commands, one per line.  End with
  CNTL/Z.
RouterA(config)#interface fastethernet 4/0
RouterA(config-if)#mls rp vlan-id 10
RouterA(config-if)#^Z
RouterA#

!
interface FastEthernet4/0
 ip address 172.16.10.1 255.255.255.0
 no ip directed-broadcast
 no ip route-cache
 no ip mroute-cache
 mls rp vtp-domain test
 mls rp vlan-id 10
!
```

Interface Configurations

After VTP and VLAN assignments have been made, you can finally enable MLS on the interface. This is done with the same command that was used to globally enable MLS, `mls rp ip`. Here is an example:

```
RouterA#configure terminal
Enter configuration commands, one per line.  End with
  CNTL/Z.
RouterA(config)#interface fastethernet 4/0
RouterA(config-if)#mls rp ip
RouterA(config-if)#^Z
RouterA#

!
interface FastEthernet4/0
 ip address 172.16.10.1 255.255.255.0
 no ip directed-broadcast
 no ip route-cache
 no ip mroute-cache
 mls rp vtp-domain test
 mls rp vlan-id 10
 mls rp ip
!
```

MSA Management Interface

As you might remember, MLS has three components. The third component is MLSP, the communication protocol itself. Well, in order for MLS to function between a switch and a router, MLSP must be able to communicate between both devices.

This requirement makes this next configuration step essential for MLS functionality. At least one interface on the router that is connected to the same switch must be enabled as the management interface. This indicates which interface is going to participate in MLSP exchanges.

Another requirement is that there be at least one management interface per VLAN on the switch. To specify a router interface as a management

interface, issue the `mls rp management-interface` command on the specified interface. Here is an example of the syntax for the command:

```
RouterA#configure terminal
Enter configuration commands, one per line.  End with
  CNTL/Z.
RouterA(config)#interface fastethernet 4/0
RouterA(config-if)#mls rp management-interface
RouterA(config-if)#^Z
RouterA#
```

Verifying the MLS Configuration

After all the pieces have been configured, you can issue the `show mls rp` command to view the MLS status and information on the router. There are two options in correlation with the main command. All three commands are shown here:

`show mls rp` Provides global MLS information

`show mls rp interface` ***`interface`*** Provides interface-specific MLS information

`show mls rp vtp-domain` ***`domain_name`*** Provides MLS information for the VTP domain

Here is an example of the global command:

```
RouterA#show mls rp
multilayer switching is globally enabled
mls id is 0010.a6a9.3400
mls ip address 172.16.21.4
mls flow mask is destination-ip
number of domains configured for mls 1

vlan domain name: test
   current flow mask: destination-ip
   current sequence number: 3041454903
   current/maximum retry count: 0/10
   current domain state: no-change
```

```
current/next global purge: false/false
current/next purge count: 0/0
domain uptime: 00:34:35
keepalive timer expires in 4 seconds
retry timer not running
change timer not running
fcp subblock count = 1

1 management interface(s) currently defined:
   vlan 10 on FastEthernet4/0

1 mac-vlan(s) configured for multi-layer switching:

   mac 0010.a6a9.3470
      vlan id(s)
      10

router currently aware of following 1 switch(es):
   switch id 00-e0-4e-2d-43-ef

RouterA#
```

Here is an example of the interface option:

```
RouterA#show mls rp interface fastethernet 4/0
mls active on FastEthernet4/0, domain test
interface FastEthernet4/0 is a management interface
RouterA#
```

These are the `show` commands, and as with any IOS, there are debugging opportunities. Table 7.1 provides a summary of the debug commands available for MLS troubleshooting.

TABLE 7.1 MLS Debug Command Summary

Command	Description
`all`	Performs all MLS debugging
`error`	Displays information about MLS errors

TABLE 7.1 MLS Debug Command Summary *(continued)*

Command	Description
`events`	Displays information from MLS events
`ip`	Displays IP MLS events
`locator`	Displays MLS locator information
`packets`	Displays information for all MLS packets
`verbose packets`	Displays information on all MLS verbose packets

Access Lists

It's not unusual to want to use an access list to filter traffic from one VLAN to another, especially if one VLAN needs higher security than the others do. The problem is that you usually want all the packets to be examined by the access list, and the switch is forwarding only the first one.

Until IOS release 12.0(2), inbound access lists were not supported. If a router interface had an inbound access list applied, MLS was disabled. With versions after 12.0(2), inbound access lists are supported, but the support is not enabled by default. Use the command `mls rp ip input-acl` from global configuration mode to enable the router to use MLS with inbound access lists.

Outbound access lists (ACLs) are a little more problematic. Although they have always been supported, applying the access list to an interface will clear the MLS cache information for connections passing through that interface. Another packet will need to be forwarded to the router to start the MLS process again. Also, outbound lists utilizing the following functions will disable MLS on the interface to which they are applied:

- TOS
- Established
- Log
- Precedence
- Reflexive

This is because these features require the router to examine every packet. Because these features tend to be more security related than a simple access list often is, using these features disables MLS on the interface in question.

Configuring the MLS Switch Engine

Switch configuration of MLS is very simple. MLS is on by default for the 6000 and 2926G, and for the 5000s with RSMs and NFFC cards in them. The only time that it is necessary to perform configuration tasks on the MLS-SE is when you want to change specific MLS attributes or when the device requires configuration. Here are some examples:

- Using an external router
- Establishing flows
- Changing the MLS cache aging timers
- Enabling NetFlow Data Export (NDE)

Each of these topics will be addressed in this section.

Enabling MLS on the MLS-SE

As mentioned, the only time you need to actually enable MLS on the switch is when it has been disabled or on a system on which MLS is off by default.

To enable MLS on the MLS-SE, issue the command `set mls enable`. Here is an example:

```
Switch2> (enable) set mls enable
Multilayer switching is enabled
Switch2> (enable)
```

If the MLS route processor being used is an external router, the switch needs to be told to send MLSP packets to the appropriate IP address. Use the command `set mls include` *`rp_ip_address`* to tell the switch which IP address that will be. The command `show mls include` will display the list of IP addresses of external route processors.

Configuring Flow Masks

A flow is the cache entry on the switch that is used for layer 3 switching. The switch learns the appropriate information from the MLS router and the switch caches the information for subsequent packets in the stream. Typically, flow information is received from a router based on what type of access list is configured on the outbound interface.

There are three ways of configuring flow masks:

Destination-IP This is the default mask and is the least specific. A flow is created for each destination IP address, and all packets—no matter the source—get layer 3 switched if they match the destination. This mask is used if no outbound access list is used.

Source-Destination-IP The switch engine will have a flow entry for each source/destination pair of addresses. No matter what applications are used between the two addresses, all traffic that matches the source and destination IP addresses will be switched according to this flow. This mask is used if there is a standard access list used on the outbound interface.

IP-Flow This mask builds flows that have a specific source and destination port in addition to specific source and destination IP addresses. Two different processes, for example, HTTP and Telnet, from one client to a single server will create two different masks because the port numbers are different. This mask is used if the outbound access list is extended.

If no outbound access list is configured on the router but either IP-Flow or Source-Destination-IP is desired, it is possible to configure the switch to build flows in a more specific fashion. The command `set mls flow [destination|destination-source|full]` can be used to tell the MLS switch what information to cache with candidate packets.

Using Cache Entries

MLS entry or shortcut cache exists on the NFFC for the 5000 series switches and on the PFC for 6000 series switches. The purpose of the cache is consistent across all platforms: The cache is a layer 3 switching table. It maintains the flow information that facilitates MLS.

Here is a sample of a layer 3 cache table:

```
Switch1> (enable) show mls entry
Dest-IP  Source-IP Prot DstPrt SrcPrt Dest-Mac Vlan EDst
  ESrc DPort SPort  Stat-Pkts  Stat-Bytes  Uptime   Age
--------------- --------------- ----- ------ ------ -----------------
---- ---- ---- ------ ------ ---------- ---------- -------- --------
MSFC 10.10.100.5 (Module 15):
172.16.10.1 -               -      -       -      00-30-96-2d-24-20
  188  ARPA ARPA 2/7    2/6    870         157785
  00:05:29 00:00:27
172.16.55.115    -              -      -       -      00-30-96-2d-24-20
  188  ARPA ARPA 2/7    2/6    2407       642886       00:00:39
  00:00:00
172.16.96.101   -               -      -       -      00-d0-bc-f3-69-44
  4    ARPA ARPA 2/2    2/7    2710       2200670      00:12:23
  00:00:00
172.16.8.35    -                -      -       -      00-d0-bc-f3-66-9c
  180  ARPA ARPA 3/7    3/3    76634      24951932     00:24:31
  00:00:00
172.16.8.17    -                -      -       -      00-30-96-2d-24-20
  188  ARPA ARPA 2/7    2/6    81752      26599352     00:18:32
  00:00:00
172.16.8.102   -                -      -       -      00-30-96-2d-24-20
  188  ARPA ARPA 2/7    2/6    313        148298       00:00:24
  00:00:22
```

This command has many options, but the most basic ones involve viewing cache information based on the source and destination IP addresses. The syntax of the command is `show mls entry [rp|destination|source] ip_address`. Also, be aware that the display has room for many pieces of information, but you won't see them unless the flow is being based on that information. For example, when using the preceding Destination-IP flow, the source IP address isn't displayed. You will always be able to see the destination IP address as well as the destination MAC address.

Cache entries are kept while the flow is active. After the flow no longer receives traffic, the cache entry gets aged out and removed from the layer 3 cache on the NFFC or PFC. This attribute can be modified and adjusted. You'll learn how to do that next.

A candidate entry will be cached for five seconds to allow for an enable packet to arrive from the router. If the enable packet doesn't arrive in that

time, the switch assumes that the best path is not through itself and removes the entry.

Modifying the Cache Aging Time

A layer 3 cache entry will remain in cache for 256 seconds after the last packet for the flow has passed through the switch. This is the default value. The value can be changed to different values depending on your needs as a network administrator.

The syntax is `set mls agingtime` *`agingtime`*, where *`agingtime`* is a value of seconds. The value is a multiple of 8. The valid range is from 8 to 2032. If the value specified is not a multiple of 8, the nearest multiple will be used. Here is an example:

```
Switch2> (enable) set mls agingtime 125
Multilayer switching aging time set to 128
Switch2> (enable)
```

Modifying Fast Aging Time

When the layer 3 cache grows greater than 32KB in size, the possibility increases that the PFC or NFFC will not be able to perform all layer 3 switching, causing some packets to be forwarded to the router. To aid in maintaining a layer 3 cache smaller than 32KB, you can enable and adjust fast aging times.

Because some flows can be very short—a DNS query, for example—you can enable packet thresholds that can be used in correlation with the fast aging time to quickly age out these entries. Both of these attributes are thresholds. When you set the fast aging time, you specify the amount of time for which *n* number of packets (defined by the packet threshold) must have used the cache entry.

When a flow is initialized, the switch must see a number of packets equal to or greater than the packet threshold set within the time specified by the fast aging time. If this criterion isn't met, the cache entry is aged out immediately.

Valid values for the fast aging time are 32, 64, 96, and 128. Valid values for the packet threshold are 0, 1, 3, 7, 15, 31, and 63. Let's try an example so you can understand how this works.

Say you configured a fast aging time of 64 seconds and set the packet threshold to 31 packets by using the `set mls agingtime fast 64 31` command

on the switch. This is telling the MLS-SE that a layer 3 cache entry has 64 seconds in which 31 packets or more must utilize the entry. If this doesn't happen, the cache entry is removed.

The actual syntax for the command is `set mls agingtime fast` *`fastagingtime pkt_threshold`*. An example configuration follows:

```
Switch2> (enable) set mls agingtime fast 64 31
Multilayer switching fast aging time set to 64 seconds for
  entries with no more than 31 packets switched.
Switch2> (enable)
```

Verifying the Configuration

MLS-SE configuration settings can be seen by using the `show mls ip` command. The command provides information regarding the aging time, fast aging time, and packet threshold values. In addition, it gives summary statistics for the type of flow mask and MLS entries. Finally, it provides details about the MLS-RP, including XTAG, MAC, and VLAN values. Here is an example:

```
Switch1> show mls ip
IP Multilayer switching aging time = 256 seconds
IP Multilayer switching fast aging time = 0 seconds,
  packet threshold = 0
IP Current flow mask is Destination flow
Active IP MLS entries = 87
Netflow Data Export version: 7
Netflow Data Export disabled
Netflow Data Export port/host is not configured.
Total packets exported = 0

IP MSFC ID      Module XTAG MAC               Vlans
--------------- ------ ---- ----------------- ------------
172.16.10.1     15     1    00-d0-bc-f4-81-c0 10,100
Switch1>
```

Displaying the MLS Cache Entries

There are several methods of viewing MLS cache entries. The base command is `show mls entry`. However, many options are available to customize the output of this basic command.

If you are on a switch and issue the Help command for `show mls entry`, this is what you get:

```
Switch1> (enable) show mls entry ?
Usage: show mls entry [mod] [long|short]
       show mls entry ip [mod] [destination <ip_addr_spec>]
              [source <ip_addr_spec>] [protocol <protocol>]
              [src-port <src_port>] [dst-port <dst_port>]
                [short|long]
       show mls entry ipx [mod] [destination <ipx_addr_spec>]
         [short|long]
    (mod = 15 or 16
     ip_addr_spec = ip_addr|ip_addr/netmask|ip_addr/maskbit
       (maskbit: 0..32)
     protocol = 1..255|ip|ipinip|icmp|igmp|tcp|udp
     src_port, dst_port = 1..65535|dns|ftp|smtp|telnet|x|www
     ipx_addr_spec = dest_net.dest_node|dest_net/mask)
Switch1> (enable)
```

As you can see, there are quite a few options. This command, with the options shown, enables the administrator to view very general information or very specific information. To get an idea of what can be generated from this command, let's review the options.

You can show MLS entries based on the module. The `long` and `short` options modify the output in different ways. `Long` displays the information all on one line, and `short` displays the information by using carriage returns. It is impossible to give an example due to the formatting limitations in this book.

More specific information can be obtained by specifying an IP address or port information. By specifying options, you can refine your output. Instead of getting pages and pages of cache entries, you get entries that match your criteria.

Removing MLS Cache Entries

If you do not want to wait for aging times to expire, or if you want to clear the cache immediately, you can issue the `clear mls entry` command. This command also has options that enable the network administrator to clear specific cache entries instead of the entire table.

The syntax of the command is as follows:

```
clear mls entry destination ip_addr_spec source ip_addr_
  spec flow protocol src_port dst_port [all]
```

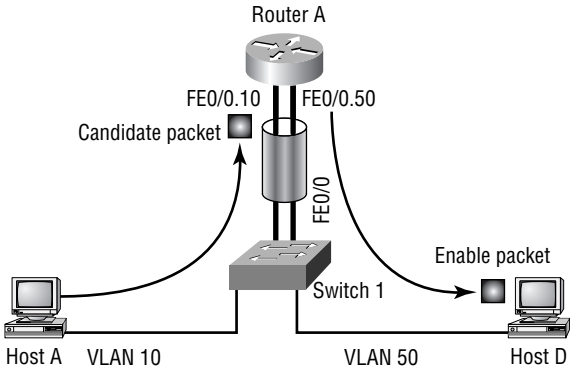
The use of the `all` optional keyword causes all MLS cache entries to be removed. If you use specific IP addresses, ports, or protocols, specific cache entries can be removed.

Using Acceptable MLS Topologies

Few topologies support MLS. Due to the nature of MLS, only certain system topologies will allow candidate and enable packets to transit the router and switch properly. If both candidate and enable packets cannot be identified, no complete flow cache entry can be made. Acceptable topologies include the following:

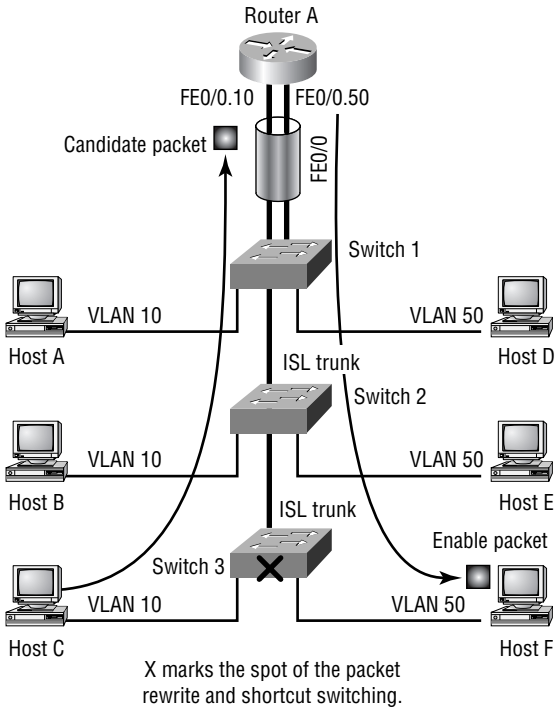
Router on a stick This includes one router (internal RSM/MSFC or external) and one switch. The router has a single connection to the network, which is the stick. See Figure 7.7.

FIGURE 7.7 Router on a stick



Multiple switches, one router This is acceptable if only one switch connects to the router and the switches are connected via an ISL trunk. See Figure 7.8.

FIGURE 7.8 Multiple switches, one router



Summary

You have learned a great deal in this chapter. It is important that you understand the fundamentals of MLS as well as the different platforms that support it.

The support of MLS on multiple platforms shouldn't be of much concern. However, implementation and configuration syntax depend greatly on the equipment and topology being deployed.

To summarize, in this chapter you learned the following:

- The fundamentals of MLS: layer 3 switching
- Components of MLS

- System and topology requirements
- Candidate and enable packet identification processes
- Layer 3 cache entry properties
- MLS configuration on multiple platforms

Exam Essentials

Know the components of MLS. Multi-Layer Switching is made of three components. The first is the MLS-SE, the switch. The second is the MLS-RP, the router that makes the changes to the initial packet. The third component is MLSP, the communication protocol used between the router and any switches.

Understand what a flow is and how a switch uses them. A flow is nothing more than a conversation, a stream of packets between two devices. A switch will cache information about the conversation and information about how the packets are supposed to be manipulated. When a packet arrives that matches a packet stream the switch has already seen, the switch makes the necessary changes.

Know what information a switch can use to identify flows. A switch can use various pieces of information to identify flows, but only three broad configurations are allowed. The first tells the switch to identify flows based only on the destination IP address. The second way says to use both source and destination IP address. The third way uses the protocol as well as the source and destination IP addresses and ports.

Understand how access lists on the router affect MLS. Outbound access lists have always been supported and are the primary way of telling the switch what information to use to identify the flow. Inbound access lists are supported with additional configuration. Reflexive lists and IP security on the interface will disable the MLS process for that interface.

Key Terms

Before you take the exam, be sure you're familiar with the following terms:

candidate packets	Multi-layer Switching Route Processor (MLS-RP)
enable packets	Multi-layer Switching Switch Engine (MLS-SE)
flow	NetFlow Feature Card (NFFC)
Multi-layer Switch Feature Card (MSFC)	Policy Feature Card (PFC)
Multi-Layer Switching (MLS)	router on a stick
Multi-layer Switching Protocol (MLSP)	XTAG

Written Lab

Write the answers to the following questions:

1. Write the command that enables MLS globally on an external router.
2. Write the command that will assign the VTP domain to the external router's interface. Use *cisco* as the VTP domain name.
3. Write the command that will assign VLAN 5 to the interface.
4. Write the command that will configure an external router interface to allow MLSP packets across it.
5. Write the command that will show you MLS information on a switch.
6. Write the command that will show you the XTAG information on a switch.

7. Write the command that will display all the layer 3 cache entries.

8. Write the command that will display a layer 3 cache entry based on the destination IP address of 172.16.10.100.

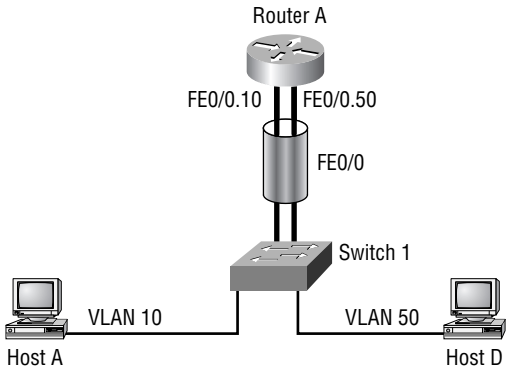
9. Write the command to clear all MLS cache entries.

10. Write the command that sets the fast aging time to 64 and the packet threshold to 63.

Hands-On Lab

Refer to Figure 7.9 for the topology of this lab. This lab will use the simplest architecture: router on a stick using a Catalyst 5000 and an external router (7200 series).

FIGURE 7.9 Lab topology



1. Assume that Router A does not have MLS enabled. You can assume that the subinterfaces are running ISL and have VLAN assignments. Switch 1 is a VTP server for the sybex domain. Configure MLS to work on Router A:

```
RouterA#configure terminal
Enter configuration commands, one per line.  End with
  CNTL/Z.
```

```
RouterA(config)#mls rp ip
RouterA(config)#interface fastethernet 4/0
RouterA(config-subif)#mls rp vtp-domain sybex
RouterA(config-subif)#interface fastethernet4/0.50
RouterA(config-subif)#mls rp management-interface
RouterA(config-subif)#mls rp ip
RouterA(config-subif)#interface fastethernet4/0.10
RouterA(config-subif)#mls rp ip
RouterA(config-subif)#^Z
RouterA#
```

2. The aging timers need to be adjusted to be shorter than the default of 256 seconds. Make the new value 128. In addition to changing the aging timers, add a command that will help keep the layer 3 cache size under 32KB. To do this, use values of aging timer = 64 and packet threshold = 31:

```
Switch1> (enable) set mls agingtime 128
Multilayer switching aging time set to 128
Switch1> (enable) set mls agingtime fast 64 31
Multilayer switching fast aging time set to 64 seconds
  for entries with no more than 31 packets switched.
Switch1> (enable)
```

3. Verify MLS status on the switch and router. Provide samples of the MLS entries and XTAG values.

   Results will vary on this answer; here are the commands that should be issued:

   - `show mls` (executed on the switch)
   - `show mls rp` (executed on the router)
   - `show mls entry` (executed on the router)

Review Questions

1. Which of the following is one of the three components of MLS?
   - **A.** MFSC
   - **B.** PCF
   - **C.** MLS-P
   - **D.** MLSP

2. Which of the following is one of the three components of MLS?
   - **A.** MLS
   - **B.** MLS-SW
   - **C.** MLS-ES
   - **D.** MLS-SE

3. Which of the following is one of the three components of MLS?
   - **A.** RP
   - **B.** RSP
   - **C.** MLS-RP
   - **D.** MLS-MSFC

4. Which of the following describes the router on a stick topology? (Choose all that apply.)
   - **A.** A router connected to a switch with coax
   - **B.** A single external router connected to a single switch
   - **C.** A single internal router (RSM/MSFC) installed in a switch
   - **D.** A switch with an RSM/MSFC connected to an external router

5. Which of the following elements are *not* used to create a flow or shortcut cache entry? (Choose all that apply.)

   A. TOS

   B. Protocol

   C. CRC

   D. Payload

   E. Source MAC

   F. Destination MAC

   G. Destination IP

6. Which answer best describes the MLSP discovery process?

   A. The MLS-SE sends hello packets to the multicast address 01-00-0C-DD-DD-DD. MLS-RPs then respond to these hello packets.

   B. The MLS-RP sends hello packets to the multicast address 01-00-0C-DD-DD-DD. MLS-SEs then respond to these hello packets.

   C. The MLS-RP sends hello packets to the multicast address 01-00-0C-DD-DD-DD. MLS-SEs then record the hello packet information.

   D. The MLS-SE sends hello packets to the multicast address 01-00-0C-DD-DD-DD. MLS-RPs then record the hello packet information.

7. What is the XTAG used for, and what is its significance?

   A. XTAG is a numerical value assigned by the MLS-SE to identify an MLS-RP. It must be unique throughout the VTP domain.

   B. XTAG is a numerical value assigned by the MLS-SE to identify an MLS-RP. It is locally significant.

   C. The XTAG is the MLS-RP router ID and is used to uniquely identify the MLS-RP to the MLS-SE. It is a unique value throughout the layer 2 network.

   D. The XTAG is the MLS-SE ID and is used to identify each MLS-SE in the layer 2 network. Therefore, it must be unique across all switches.

8. Which of the following commands will display XTAG information on a switch?

   A. `show mls entry`

   B. `show mls statistics`

   C. `show mls`

   D. `show mls rp ip`

9. What are the two prerequisites before a complete shortcut entry can be entered into cache?

   A. Identification of the MLS-SE

   B. Identification of the candidate packet

   C. Identification of the MLS topology

   D. Identification of the enable packet

10. Which of the following criteria qualify a packet as a candidate packet?

    A. Any incoming packet that is destined to a MAC address associated with the MLS-RP

    B. Incoming packets sourcing from 224.0.0.1 and destined for the MAC address of the MLS-SE

    C. Incoming packets sourcing a MAC address associated with the MLS-RP

    D. Outbound packets destined for a remote host

11. Which of the following criteria qualify a packet as an enable packet? (Choose all that apply.)

    A. The packet is sourced from an MLS-RP MAC address.

    B. The XTAG value matches the candidate packet XTAG value.

    C. The destination MAC address is the same as the corresponding candidate packet's source MAC address.

    D. The destination IP address matches the destination IP of the corresponding candidate packet.

12. Which component or device performs the frame rewrite? (Choose all that apply.)

    A. PFC

    B. MSFC

    C. RSM

    D. NFFC

13. Which of the following fields can be rewritten by the MLS-SE? (Choose all that apply.)

    A. ISL header

    B. DEST MAC

    C. Source MAC

    D. Destination IP address

14. Which of the following fields can be rewritten by the MLS-SE? (Choose all that apply.)

    A. Source IP address

    B. TOS

    C. CRC

    D. Payload

15. At what MLS cache size does the probability of involving the router increase dramatically?

    A. 8KB

    B. 64KB

    C. 32KB

    D. 128KB

    E. 256KB

16. What command can inadvertently disable MLS on a router or interface? (Choose all that apply.)

A. `no ip routing`

B. `ip security`

C. `ip access-group access-list-number [in|out]`

D. `no tcp-small-servers`

17. What command can inadvertently disable MLS on a router or an MLS-configured interface?

A. `clear ip route`

B. `ip tcp header-compression`

C. `route-map`

D. `ip router rip`

18. Which of the following commands will enable MLS on an MSFC?

A. `set mls ip enable`

B. `set mls enable`

C. `mls rp ip`

D. `mls ip`

19. Which of the following commands will enable MLS on an external router?

A. `set mls ip enable`

B. `set mls enable`

C. `mls rp ip`

D. `mls ip`

20. When must you configure the VTP domain on an interface of an external router?

A. Always

B. When it uses ISL encapsulation

C. When it doesn't use ISL or 802.1q encapsulation

D. When it is connected to a VTP server or client

Answers to Written Lab

1. `mls rp ip`
2. `mls rp vtp-domain cisco`
3. `mls rp vlan-id 5`
4. `mls rp management-interface`
5. `show mls`
6. `show mls`
7. `show mls entry`
8. `show mls entry ip destination 172.16.10.100`
9. `clear mls entry destination all`
10. `set mls agingtime fast 64 63`

Answers to Review Questions

1. D. MLSP is the proper acronym for Multi-layer Switching Protocol. MFSC should be MSFC; PCF should be PFC.
2. D. Multi-layer Switching Switch Engine is the name of the component. The proper acronym is provided in the last answer.
3. C. MLS-RP represents the broad spectrum of route processors. RP, RSP, and MSFC are all types of route processors.
4. B, C. The topology name comes from the original look of an external router connected to a switch. With the implementation of RSM/MSFC, the same functional topology is achieved in the same chassis. The media connection type does not define the topology.
5. C, D. CRC can vary from packet to packet and is used for error checking. The payload is also unique for each packet. Flows are established by using packet similarities.
6. C. The key to this question is twofold. The MLS-RP is the only device that sends hello packets. Because the packets are sent to a multicast address, the MLS-RP doesn't require a response from the switch. The MLS-RP doesn't need to establish an actual connection with the switch.
7. B. XTAGs are used by the MLS-SE to identify each MLS-RP connected to the layer 2 network. Each switch can utilize the same XTAG values; they are used only locally.
8. C. The `show mls rp ip` command is used on routers and doesn't provide XTAG information. Neither does any of the other switch commands.
9. B, D. Both packets must be identified to complete the shortcut entry.
10. A. Incoming packets must be destined to a MAC address that is associated to the MLS-RP via the XTAG value. If the packet is not destined for this address, the packet is not tagged as a candidate packet.
11. A, B, D. Enable packets have more criteria to match than do candidate packets. Because the destination MAC address is different for every hop, there is no way that a packet could match using the destination MAC address and still use MLS.

12. A, D. MSFC and RSMs are layer 3 devices that are used in Catalyst switches. Pattern matching and frame rewrites are done by the NFFC and PFC.

13. A, B, C. Although the rewrite engine can modify some fields in the IP header, it does not change the IP addresses.

14. B, C. The MLS-SE has to rewrite the CRC because it changes the values for the source MAC and destination MAC addresses. It calculates a new CRC for the new frame.

15. C. After the MLS cache size exceeds 32KB, chances are that the MLS-SE will not be able to shortcut-switch all flows, and packets will be sent to the router.

16. A, B. Other commands also can inadvertently disable MLS, but access lists no longer do. They can cause the cache to be cleared, but now, since IOS 12.0(2), inbound as well as outbound access lists are supported and do not disable MLS.

17. B. Using header compression disables MLS on the configured interface. `Clear ip route` is not a correct answer because it temporarily clears the cache, but it doesn't disable MLS.

18. D. The `mls rp ip` command is used on an external router, the first command is invalid, and `set mls enable` is used to enable MLS on a 5000 series switch.

19. C. The command `set mls enable` is used to enable MLS on a 5000 series switch, and the command `mls rp ip` is used to enable MLS on an external router.

20. D. Internal routers such as RSMs or MSFCs don't require a VTP domain configuration because they are physically connected to a single switch. However, external routers that have connections to VTP servers or clients must configure the interface for the VTP domain.

Chapter

8

Multicast

THE CCNP EXAM TOPICS COVERED IN THIS CHAPTER INCLUDE THE FOLLOWING:

- ✓ **Describe the functionality of CGMP**
- ✓ **Describe how switches facilitate Multicast Traffic**
- ✓ **Translate Multicast Addresses into MAC addresses**

Just as blue, yellow, and red are the primary colors, unicast, multicast, and broadcast are the primary forms of communication on networks.

Today's Web and enterprise applications are directed to larger audiences on the network than ever before, causing increased bandwidth requirements. This increased demand on bandwidth can be accommodated with as little cost increase as possible by using multicast. For example, voice and video are being sourced for larger and larger audiences. One-on-one communications can overwhelm both servers and network resources. Unlike unicast and broadcast, however, multicast services can eliminate this problem.

This chapter will help you understand the differences in unicast, broadcast, and multicast communication methods and when each should be used. Unicast is an excellent method of point-to-point communication, whereas broadcast traffic is imperative for many systems and protocols to work on a network. Multicast comes in as a bridge between these two communication extremes by efficiently allowing point-to-multipoint data forwarding. It is imperative that you understand how multicast addressing spans both layer 3 and layer 2 of the OSI model. You will also learn about the protocols and tools used to implement and control multicast traffic on your network. As with any service that runs on your network, you must understand the resources needed and the implications of enabling multicast.

Multicast Overview

Just as blue, yellow, and red are different and each has its own place within the spectrum of visible light, unicast, broadcast, and multicast are different in that each is used to achieve a specific purpose or fulfill

requirements of a specific part of the communication spectrum. It is important to know where each falls within the spectrum as well as the potential applications.

RFC 1112 discusses multicast and goes into great detail about host extensions and multicast groups. In addition to address assignment for multicast applications and hosts, protocol methods and procedures are discussed. For example, it covers the methods by which hosts join and leave multicast groups, and it also covers group advertisements and multicast forwarding.

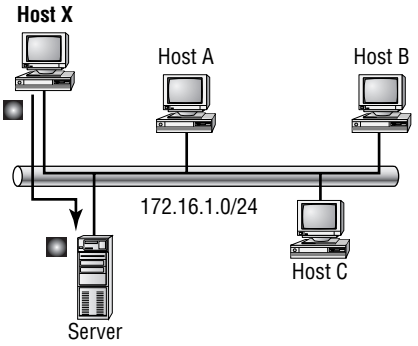
Unicast

Unicast is used for direct host-to-host communication. When the layer 3 Protocol Data Unit (PDU, or packet) is formed, two layer 3 IP addresses are added to the IP header. These are the source and destination IP addresses. They specify a particular originating and receiving host. After the layer 3 PDU is formed, it is passed to layer 2 to create the layer 2 PDU, or frame. The frame consists of all the previous layers' headers in addition to the layer 2 header. With an Ethernet frame, for example, the two 48-bit source and destination MAC addresses are specified in the layer 2 header. Other protocols such as IEEE 802.5 (Token Ring) and FDDI also have headers that contain specific host source and destination addresses.

Unicast communication is used when two hosts need to exchange data with only one another and are not concerned with sharing the data with everyone. A MAC address must *uniquely* identify a host. No two MAC addresses, on a single network, can be the same. Therefore, unicast capitalizes on the unique MAC address of each host. With the specific address, any source host should be able to contact the destination host without confusion.

One of the caveats to unicast communication is that the source host must know or be able to learn what every destination MAC is for every station it wishes to communicate with. In order to figure out which MAC address the source should send frames to, it uses an ARP request, explained in the following "Broadcast" part of this section. The normal operation is that the host has a default gateway assigned for use when the logical destination address does not reside on the same subnet as the source host. Figure 8.1 depicts how unicast traffic works on the same subnet.

FIGURE 8.1 Unicast communication

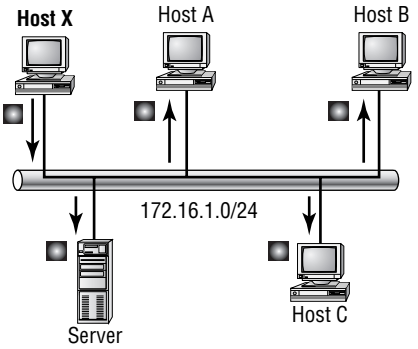


The unicast process, then, is a two-device communication. These two hosts are interested in communicating with only one another. So what happens when one host wants to talk to multiple hosts or all the hosts on the same network segment? That is where broadcast communication comes in.

Broadcast

Now that you have a good understanding of unicast, we can discuss the principle of broadcast communication on networks. Whereas unicast messages target a single host on a network (unicast communication can be compared to sending an e-mail to a friend; the mail is addressed to the friend, and it is sent from you), *broadcast* messages are meant to reach all hosts on a broadcast domain. Figure 8.2 depicts a broadcast message sent from Host X to all machines within the same broadcast domain.

FIGURE 8.2 Broadcast message on a network



A good example of a broadcast message is an Address Resolution Protocol (ARP) request. When a host has a packet, it knows the logical address of the destination. To get the packet to the destination, the host needs to forward the packet to a default gateway if the destination resides on a different IP network. If the destination is on the local network, the source will forward the packet directly to the destination. Because the source doesn't have the MAC address it needs to forward the frame to, it sends out a broadcast, something that every device in the local broadcast domain will listen to. This broadcast says, in essence, "If you are the owner of IP address 192.168.2.3, please forward your MAC address to …" with the source giving the appropriate information. Each device will answer a request for its own IP address, but a correctly configured router can serve as a proxy as well, with the process of Proxy ARP.

This brings up another good point: broadcasts can cause problems on networks. Because the broadcast frame is addressed to include every host, every host must process the frame. CPU interruption occurs so that the frame can be processed. This interruption affects other applications that are running on the host. When unicast frames are seen by a router, a quick check is made to identify whether the frame is intended for the host. If it isn't, the frame is discarded.

Multicast

Multicast is a different beast entirely. At first glance, it appears to be a hybrid of unicast and broadcast communication, but that isn't quite accurate. Multicast does allow point-to-multipoint communication, which is similar to broadcasts, but it happens in a different manner. The crux of *multicast* is that it enables multiple recipients to receive messages without flooding the messages to all hosts on a broadcast domain.

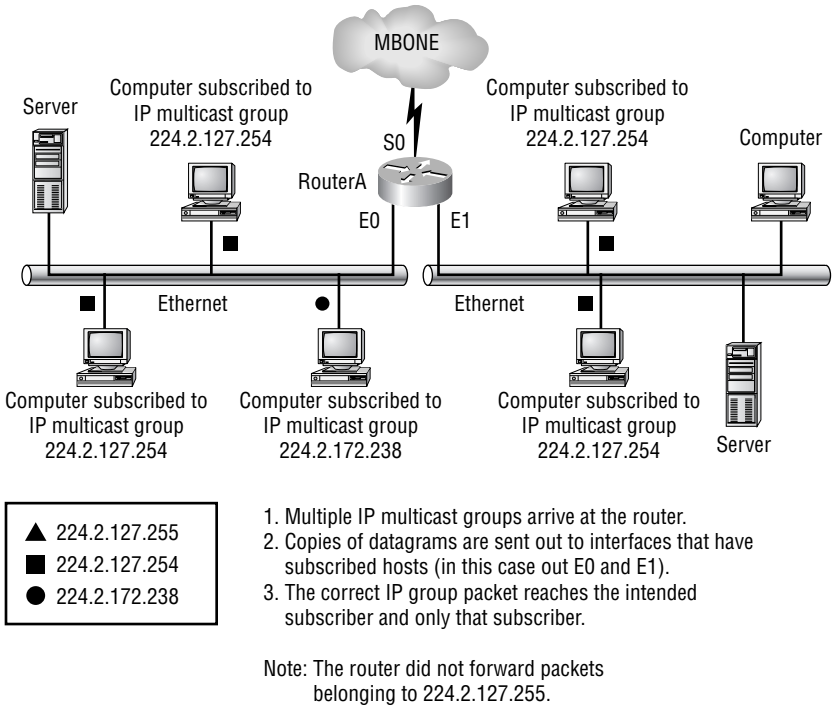
Multicast works by sending messages or data to IP *multicast group* addresses. Routers then forward copies of the packet out every interface that has hosts *subscribed* to that group address. This is where multicast differs from broadcast messages. With multicast communication, copies of packets are sent only to subscribed hosts.

The difference between multicast and unicast is comparable to the difference between mailing lists and spam. You subscribe to a mailing list when you want to receive mail from a specific group regarding specific information—for example, a Cisco User Group mailing list. You expect to get messages only from other members of the group regarding topics related to

the user group. In contrast, spam is unsolicited mail that arrives in your inbox. You aren't expecting it from the sender, nor are you likely to be interested in the content.

Multicast works in much the same way as a mailing list. You (as a user) or an application will *subscribe* to a specific IP multicast group to become a member. After you become a member of the group, IP multicast packets containing the group address in the destination field of the header will arrive at your host and be processed. If the host isn't subscribed to the group, it will not process packets addressed to that group. Refer to Figure 8.3 for a reference on how multicast works.

FIGURE 8.3 Multicast communication



The key to multicast is the addressing structure. This is key because all communication is based on addressing. In unicast communication, there is a unique address for every host on a network. In broadcast communication, a global address that all hosts will respond to is used. Multicast uses

addressing that only some hosts will respond to. The next section will cover multicast addressing in detail.

Using Multicast Addressing

Just as with mailing lists, there are several different groups that users or applications can subscribe to. The range of multicast addresses starts with 224.0.0.0 and goes through 239.255.255.255. As you can see, this range of addresses falls within IP Class D address space based on classful IP assignment. This is denoted by the first four bits in the first octet being 1110. Just as with regular IP addresses, there are some addresses that can be assigned and there are ranges of reserved addresses.

It is important to recognize that the reserved addresses are categorized. Table 8.1 depicts some of the reserved addresses and their corresponding categories. For a full listing of these assignments, you can go to `http://www.iana.org/assignments/multicast-addresses`.

TABLE 8.1 IP Multicast Reserved Addresses

Address	Purpose	Reserved Category
224.0.0.0–224.0.0.18	Use by network protocols	Local-link
224.0.0.1	All hosts	Local-link
224.0.0.2	All routers	Local-link
224.0.0.19–224.0.0.255	Unassigned	Local-link
224.0.1.0–224.0.1.255	Multicast applications	Misc. Applications
224.0.1.1	NTP	Misc Applications
224.0.1.8	NIS+	Misc Applications
224.0.1.39	Cisco-RP-Announce	Misc Applications

TABLE 8.1 IP Multicast Reserved Addresses *(continued)*

Address	Purpose	Reserved Category
224.0.1.40	Cisco-RP-Discovery	Misc Applications
224.0.1.80–224.0.1.255	Unassigned	Misc Applications
224.0.0.10	EIGRP	Local-link
239.0.0.0–239.255.255.255	Private multicast domain	Administratively Scoped

Each address range is managed by the Internet Address Number Authority (IANA). Due to the limited number of multicast addresses, there are very strict requirements for new assignments within this address space. The 239.0.0.0–239.255.255.255 range is equivalent in purpose to the private networks defined by RFC 1918.

The difference between the IP multicast ranges of 224.0.0.0–224.0.0.255 and 224.0.1.0–224.0.1.255 is that addresses in the first range will not be forwarded by an IP router. Both ranges of addresses are used by applications and network protocols. The first group, classified as local-link, is meant to remain local to the subnet or broadcast domain on which the system resides. The second group is a global address that can be routed and forwarded across multiple IP routers.

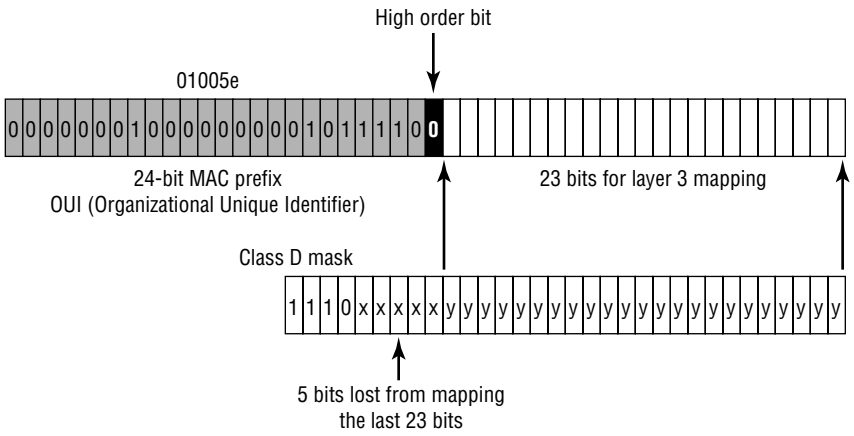
Mapping IP Multicast to Ethernet

Multicast addressing began on MAC addresses. Growth needs required that there be a way to use multicast across routers instead of limiting it to the physical segment where hosts were located. In regular unicast, MAC addresses are layer 2 addresses, and in order for the local host to reach remote hosts, layer 3 logical IP addresses are used to route data to the destination. After the packet reaches the remote subnet, the ARP is used to find the MAC address of the host. By using an existing ARP table, or via an ARP request, the MAC address that is associated to the layer 3 IP address is found and the packet is forwarded to the destination host.

IP multicast generates a MAC address based on the layer 3 IP multicast address. The MAC frame has a standard prefix of 24 bits. This prefix, 01-00-5e, is used for all Ethernet multicast addresses. This leaves another 24 bits for

use in creating the multicast MAC address. When the MAC address is generated, the 25th bit (or high order bit) is set to 0 and then the last 23 bits of the IP address are mapped in to the remaining 23 bits of the MAC address. Figure 8.4 depicts how this looks.

FIGURE 8.4 IP multicast mapped to MAC multicast

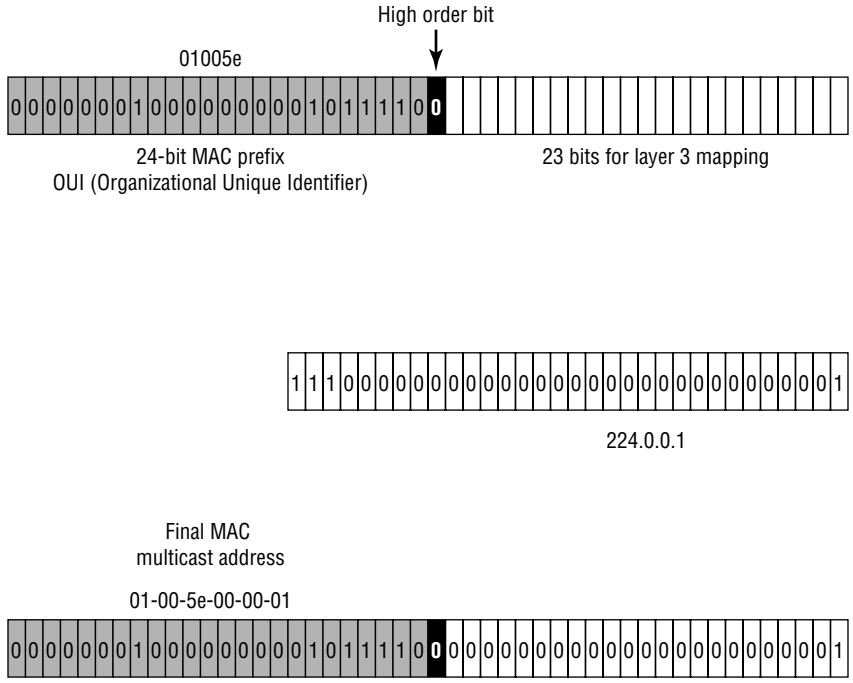


MAC addresses are made up of two sets of addresses, each with 24 bits. The first set is an address reserved for a particular manufacturer. The second set identifies a particular device by that manufacturer. This is why Cisco devices always seem to have one of a small number of "first halves." Multicast MAC addresses use 01-00-5E for the vendor code, with the device code based on the IP address.

Let's look at some examples of mapping layer 3 multicast addresses to layer 2 multicast addresses. A local IP multicast address is 224.0.0.1. Refer to Figure 8.5 to see how this is mapped. The conversion from binary to hexadecimal reveals the MAC multicast address. The prefix was 01-00-5e. The last 23 bits, including the high order bit, give you 00-00-01. Put them together and you get 01-00-5e-00-00-01 as the MAC address.

Now let's try one a little bit harder. Suppose, for example, you have the IP multicast address of 225.1.25.2 (follow along with Figure 8.6). Part of the 225 octet falls within the Class D mask. However, there is 1 bit that is not masked. By looking carefully at the location of the bit, you will see that it is part of 5 lost bits and is not mapped to the layer 2 MAC multicast address.

FIGURE 8.5 Example 1 for mapping IP multicast to MAC multicast addresses

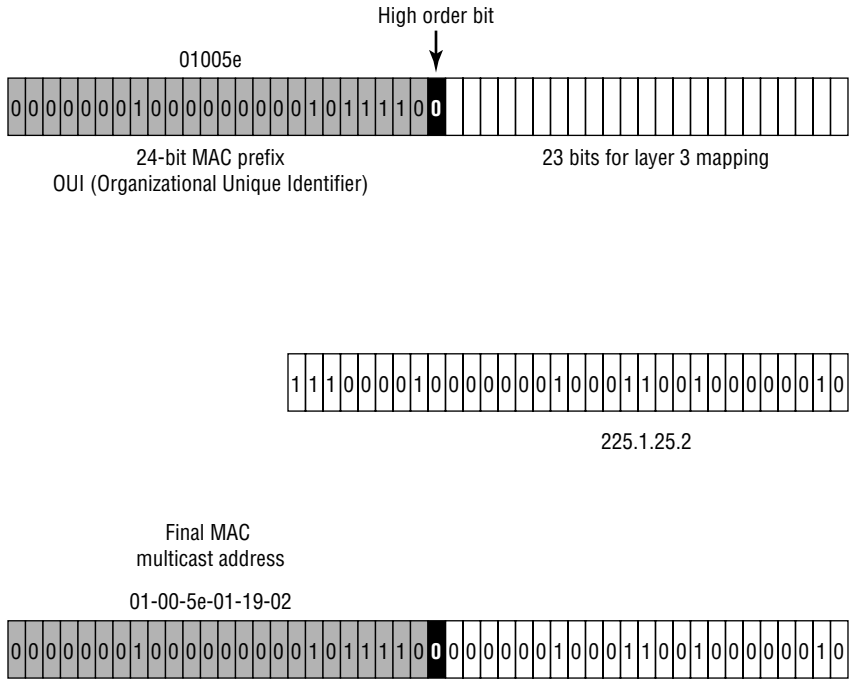


Convert the octets from decimal into binary so you can get a clear picture of what the last 23 bits are. Here you would see the following address (the last 23 bits are indicated in bold font): 11100001.0**0000001.00011001.00000010**. Also, as you can see, Figure 8.6 depicts the last 23 bits that are mapped into the free spaces of the multicast MAC address. After the mapping has occurred in binary, convert the binary value to hex and you will have the new MAC multicast address.

After you do the math and map the last 23 bits, the MAC address becomes 01-00-5e-01-19-02. The easiest way to map layer 3 to layer 2 manually is to do the math and make the binary conversion so you can see what the last 23 bits of the layer 3 IP address are. After you have that number, all you have to do is insert it into the MAC address and then calculate the remaining 3 hex octet values. The first three octets will always be the same, 01-00-5e.

It is important that you spend time studying this procedure and the steps needed to convert a layer 3 IP multicast address to a layer 2 MAC multicast address.

FIGURE 8.6 Example 2 for mapping IP multicast to MAC multicast addresses



There is one last method of determining the last 23 bits, but this method will work only on some addresses. Keep in mind that the highest value you can get in the second octet is 127 and still have it be included in the 23 bits that will map to the MAC address. You know that the last two octets (3 and 4) will map no matter what. So you will have 7 bits from the second octet, and 16 bits from the last two octets, for a total of 23 bits. After your value goes above 127 in the second octet, you will have to break down the octet into binary so you can see the values of the first seven fields.

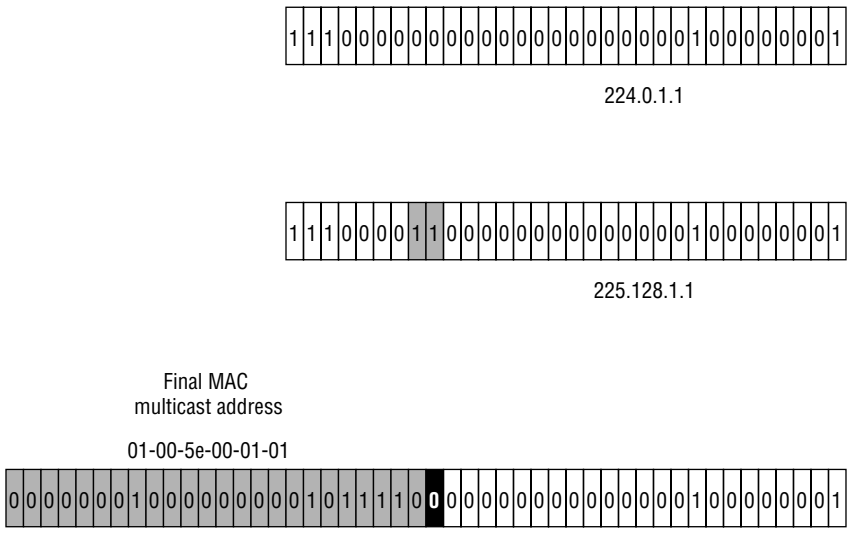
Layer 3 to Layer 2 Overlap

After you have done a few of these conversions, you'll notice, or maybe you already have, that there is a problem with this conversion scheme. By not using all available bits for a Class D address, you cannot get an accurate map of layer 3 to layer 2 addresses. If you look at properties of a Class D address, you will see that the high order bit lies in the first octet and is in the 16's value position. This leaves 28 bits for host specification. However, by using only

23 bits of the layer 3 IP address, you leave 5 bits out of the mapping. This causes an overlap of 2^5, or 32 layer-3 addresses for every 1 layer-2 address. With a ratio of 32:1, you can expect to see a significant amount of address ambiguity. It is safe to say that any IP addresses that have the same values in the last 23 bits will map to the same MAC multicast address.

For example, 224.0.1.1 and 225.128.1.1 map to the same MAC address. Figure 8.7 shows why this is true. You can see that the bits that differ between 224.0.1.1 and 225.128.1.1 are all within the lost 5 bits. The last 23 bits are equivalent.

FIGURE 8.7 Multicast addressing overlap



The impact of this overlap can be significant. The overlap creates a window for multiple multicast groups' data to be forwarded to and processed by machines that didn't intentionally subscribe to the multiple groups. To give another example, a machine that subscribes to a multicast group 224.2.127.254 would be given a MAC address of 01-00-5e-02-7f-fe. This host will also process packets that come from multicast group 225.2.127.254 because the layer 2 MAC address is identical.

The problem this creates is that the end host must now process packets from both multicast groups even though it is interested only in data from 224.2.127.254. This causes unwanted overhead and processor interrupts on the host machine.

Managing Multicast in an Internetwork

As a user on the network, you can understand that spam is not something that is managed by a systems administrator, whereas valid mailing lists require maintenance to keep a current list of valid subscribers. The same can be said of multicast. As we said earlier, one of the major differences between broadcast and multicast communication is that broadcast traffic goes to all hosts on a subnet, whereas multicast traffic goes only to the hosts that request it. The distinguishing factor that puts multicast traffic so far ahead of broadcast traffic in utility is the ability to specify which multiple hosts will receive the transmission.

This isn't done magically; routers and switches don't know who and where the recipients are just because it's multicast traffic. As with any application, protocols are needed to make things happen. Multicast works on the basis of host subscription to groups.

Several methods and protocols have been developed and implemented to facilitate multicast functionality within the internetwork:

- Subscribing groups
- Maintenance groups
- Joining groups
- Leaving groups

Each of these protocols and methods is used for specific tasks or to achieve specific results within the multicast environment. More importantly, each device in the network must know its role regarding multicasting; otherwise, you are left with nothing except a broadcast.

We will now look at these protocols and learn just where they fit in and what they are needed for. We will begin with the most important, subscription and group maintenance, and then move on to enhancements for multicast deployment and distribution.

Subscribing and Maintaining Groups

For multicast traffic to reach a host, that host must be running an application that sends a request to a multicast-enabled router informing the router that it wishes to receive data belonging to the specified multicast group. If this

request were to never take place, the router wouldn't be aware that the host was waiting for data from the specified group.

As an overview, a multicast-enabled router receives all group advertisements and routes. It listens on all interfaces, waiting for a request from a host to forward multicast group traffic. After a host on an interface makes a request to become a member of a group, the interface activates the requested group on itself and only on itself. While the host is a member, multicast data will be forwarded to that interface, and any host subscribed to the group will receive the data.

That was a simple overview; now let's look at how this is accomplished in more detail. We will start by discussing four major host subscription protocols:

- IGMPv1
- IGMPv2
- CGMP
- IGMP Snooping

The differences among them will become apparent as we get further into the discussion.

Internet Group Management Protocol Version 1 (IGMPv1)

As the name indicates, *Internet Group Management Protocol version 1 (IGMPv1)* was the first version of the protocol. It was a result of RFC 1112. The purpose of this protocol is to enable hosts to subscribe to or join specified multicast groups. By subscribing to groups, the hosts are thereby enabled to receive multicast data forwarded from the router.

IGMP has several processes that it executes to manage multicast group subscription and maintenance. We will discuss them in greater detail so you can get an understanding of what happens.

IGMPv1 Processes

Three processes are employed by version 1 of IGMP:

- Query
- Join
- Leave

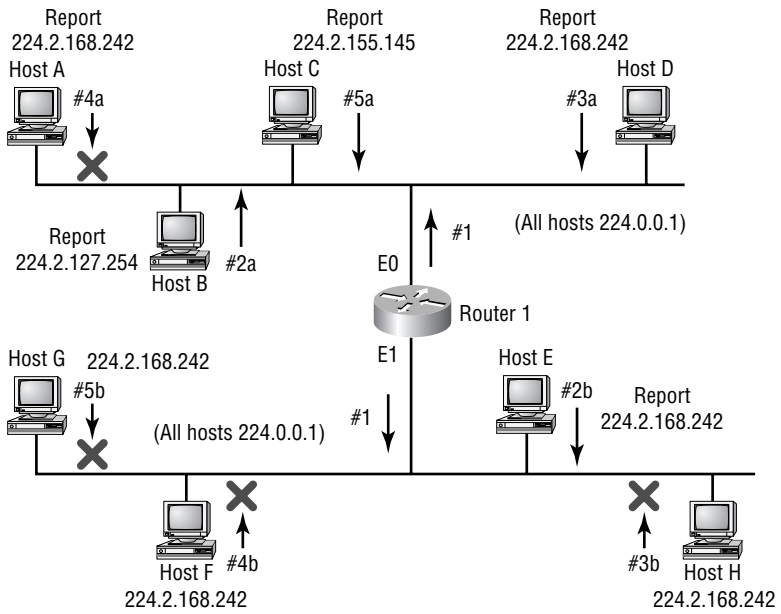
These processes are the means by which multicast group membership is maintained. The first two processes are functional processes, whereas the Leaving process is more of a time-out than a formal request. Each process is defined in detail next.

Membership Query Process

One important process is the *IGMP Query process*, which is kindred to a keep-alive procedure. Because the router needs to keep tabs on which multicast groups need to remain active, or be made active or inactive, it sends a Membership Query out each interface. The query is directed to the reserved address of 224.0.0.1, to which all multicast hosts will answer.

After the request is received, the hosts report back with their group subscription information. After a specific group has been reported to the router, subsequent reports for the same group coming from different hosts will be suppressed. This is done because only one host on a subnet/VLAN needs to request membership for the router to activate that group on the interface. Once active on the router interface, any host on that segment wanting to receive data for that specific group will receive it. Figure 8.8 depicts how this process works.

FIGURE 8.8 IGMPv1 Query routine



You can follow the numbers indicated in the figure. First, the query to 224.0.0.1 is sent, and subsequently, the hosts begin to report back. The first host to respond (#2a) is Host B, requesting data for the multicast group 224.2.127.254. Host D responds next (#3a) with a request for the group 224.2.168.242. The next host to reply is Host A (#4a). However, because the report from Host D was already multicast to the 224.2.168.242 group, Host A heard the report and suppressed its own report to the group.

The protocol is "smart" enough to understand that after one host has reported, more hosts don't need to report as well. This helps prevent unwanted and unnecessary bandwidth and processor utilization. To accomplish this, when a query is sent, each participating device will set a random countdown timer. The first device whose timer runs out will respond; the others will reset their timers.

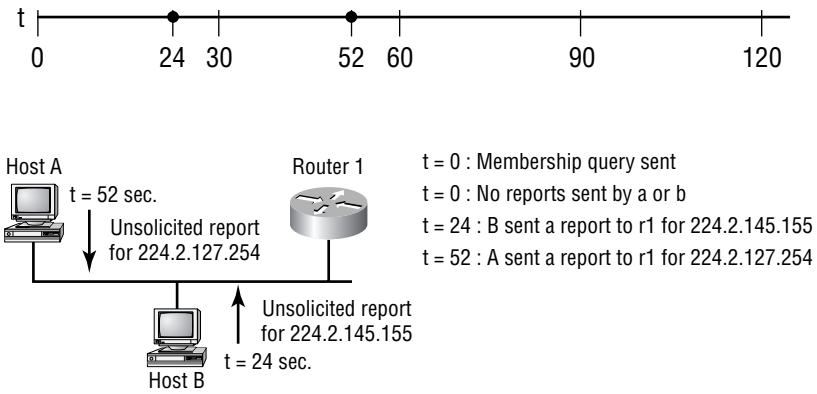
Host C (#5a) responds with a different group number, 224.2.155.145. After all the hosts have responded to the query, Router 1 can maintain activity for these groups on interface E0.

Notice that this description applies to interface E0 on Router 1. Simultaneously, a multicast flood to 224.0.0.1 was sent out interface E1 as well. The first host to respond on this segment is Host E (#2b), and it is reporting membership to 224.2.168.242. Notice that this report was not suppressed, even though Host D had already multicast a report to this group, because it occurred on a different interface. The router queries the local All Hosts address 224.0.0.1, which is not forwarded by the router. That is why the same query is sent out all interfaces on the router. Now that Host E has multicast to the group for that segment, none of the other hosts on the E1 segment will report because they are all members of the 224.2.168.242 group.

Join Process

The other processes are joining and leaving multicast groups. Both of these processes are quite simple and straightforward. You understand how interfaces are maintained in an active state through Membership Queries. The query process runs only every 60 seconds. If a host wants to join a multicast group outside the Membership Query interval, it can simply send an unsolicited report to the multicast router stating that it wants to receive data for the specified multicast group. Figure 8.9 depicts how this occurs. This is known as the *IGMP Join process*.

FIGURE 8.9 Unsolicited join requests



Leave Process

Withdrawal from a group is not initiated by the host as one would imagine. The router hosts a timer that is reset every time a response is received from a host on the subnet. The timer runs for three minutes, which is equivalent to three Membership Query cycles (every 60 seconds). If the timer expires and no response is received from the hosts on the interface, the router disables multicast forwarding on that interface. If the router was forwarding for a specific group and doesn't get responses for that group but continues to get responses for other groups, it will stop forwarding only for the group that no longer has hosts listening.

Internet Group Management Protocol Version 2 (IGMPv2)

As with any software revision, features are made better. Defined by RFC 2236, *Internet Group Management Protocol version 2 (IGMPv2)* provides the same functionality as version 1 did, but with a few enhancements:

- The Leave process in version 2 was included to avoid long time-outs that are experienced in version 1.
- There are two Query forms, General and Group-Specific.
- Network traffic is less bursty due to new timing mechanisms.

In this section, these enhancements will be discussed.

IGMPv2 Processes

It is important to be aware of issues when both versions of IGMP are present on the network. Version 2 provides backward compatibility with version 1, but the functionality of version 2 is lost when it's operating with version 1 devices. A version 2 host has to use version 1 frame formats when talking with a version 1 router. The same applies when a version 2 router tries to communicate with a version 1 host; it must use the version 1 format.

General and Group-Specific Query Processes

One enhancement that was made to IGMPv2 processes was the creation of a new query type. The Membership Query, as it was called in IGMPv1, was renamed General Queries, and the new type is Group-Specific Query. The new query type is used to query a specific multicast group (kind of obvious from the name). The overall procedure is the same as it is in IGMPv1.

When multiple IGMPv1 routers existed on the same segment, a multicast routing protocol made the decision as to which of all the multicast routers would perform the Membership Queries. Now, the decision is made by using a feature added to IGMPv2. This feature is known as the Querier Election Process.

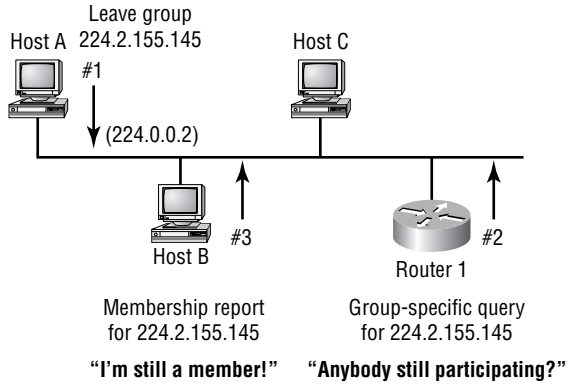
The frame for the query was changed to enable a maximum response time that allows the hosts on the segment more time to respond to the query. This reduces the bursty traffic on the network.

IGMPv2 Leave Process

IGMPv2 implemented the capability for hosts to remove themselves from the multicast group immediately (in a matter of seconds) instead of the router having to wait up to three minutes. The process is known as the *IGMP Leave process*. The two new additions of the Leave and Group-Specific messages work together to enable a host to remove itself from the multicast group immediately without interrupting the state of the interface on the multicast router.

Figure 8.10 depicts how the IGMPv2 Leave process works. First, Host A sends a Leave message to the All multicast routers address (224.0.0.2) expressing the intent to withdraw from the multicast group. Because Router 1 doesn't know how many hosts on the segment belong to group 224.2.155.145, it must send a Group-Specific Query to see whether any hosts remain members of the group. If no responses are received, the router disables multicast forwarding out of the interface for the 224.2.155.145 group. If any hosts respond to the query, the router leaves the interface status quo. In the figure, you can see that Host B responds because it is still participating in the group 224.2.155.145. Hence, the interface is left active for that group.

FIGURE 8.10 IGMPv2 Leave process



Real World Scenario

Multicast Design

If the router interface is connected to a hub or a switch that doesn't understand multicasting, when the router forwards the multicast, the stream acts like a broadcast. In other words, every device gets a copy. In IGMPv1, the router would keep forwarding the multicast stream out to the hub, which forwards it to every connected client. Multicast routers work well because they can forward a broadcast from one router to the next, something that doesn't happen with true broadcasts. The problem is that clients on a multicast segment get the stream whether they want it or not.

This type of scenario is fine when the CEO wants to give a speech to every desktop, but what about video that is only for a specific division, department, or business unit? If the packets need to go to five different locations, and after you get past the routers, all you have are switches, everyone will receive the multicast stream. This doesn't reduce bandwidth utilization!

So far, corporate multicasting with IGMP, either version, works well at the router level. Too bad most clients aren't connected directly to router ports. Because IGMP is essentially nothing more than intelligent broadcast propagation, Cisco created something that would enable switches to participate as well, CGMP.

Cisco Group Management Protocol (CGMP)

We have discussed IGMPv1 and IGMPv2, which are open standard protocols for host membership of multicast groups. When running multicast at layer 2, things get a little complicated for the switch. It doesn't know which packets are membership report messages or which are actual multicast group data packets because all of them have the same MAC address. *Cisco Group Management Protocol (CGMP)* was implemented to fill this void. It runs on both routers and switches.

The key feature of CGMP is that it uses two MAC addresses:

Group Destination Address (GDA) The GDA is the multicast group address mapped to the MAC multicast address.

Unicast Source Address (USA) The USA is the unicast MAC address of the host. USA enables the host to send multicast membership reports to the multicast router—the multicast router can also be a Route Switch Module (RSM) or Multi-layer Switch Feature Card (MSFC)—and still tell the switch which port needs to receive the multicast data.

In addition to being able to make port assignments on the switch, CGMP also handles the interface assignment on the router. If a switch doesn't have any ports that need to receive multicast data, CGMP will inform the router that it doesn't need to forward multicast group data out the router interface.

CGMP Processes

CGMP uses many of the same processes IGMP uses. The main difference is that CGMP is used between the router and switch. When switches are involved, the IGMP requests must be translated to CGMP and passed on to the switch. These processes include the following:

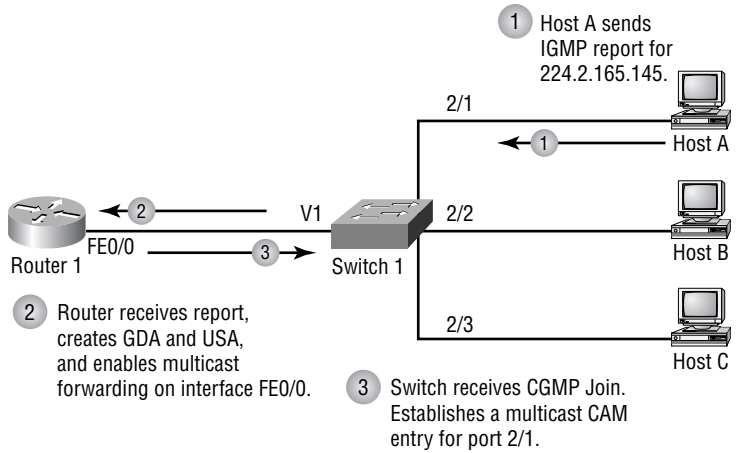
- CGMP Join process
- Switch host management
- CGMP Leave process

CGMP Join

Hosts do not use CGMP; only the switches and routers that the host connects to use it. When a host sends an IGMP report (membership report) advertising membership of a multicast group, the message is forwarded to the router (that is, an actual multicast router, RSM, or an MSFC) for

processing. The router sees the request and processes it accordingly. The multicast group is set up, and the two MAC addresses are generated. The router then gives the switch the CGMP message. With the CGMP message, the switch can assign the multicast group to the port of the requesting host. You can see the entire process in Figure 8.11.

FIGURE 8.11 CGMP Join process



Host Management

Host management is performed by the router. The router continues to receive IGMP messages from the host. Then the router converts the message into a CGMP message and forwards it to the switch. The switch then performs the port maintenance as directed by the router. This process is followed for the multiple types of messages that the host can generate. The router forwards three critical pieces of information to the switch in the CGMP message:

- Request type
- MAC address of the requesting host
- Multicast group the request is for

The CGMP Leave process is done in the same manner. The router receives the request and then informs the switch that the multicast group address needs to be removed from the Content Addressable Memory (CAM) table for the host's port.

IGMP Snooping

While CGMP is a Cisco proprietary protocol to enable switches and routers to communicate regarding multicast traffic patterns, IGMP Snooping is referenced in IGMPv3 and does that same thing. Several vendors have created implementations of IGMP Snooping that don't quite play well with each other.

IGMP Snooping doesn't require any sort of translation into a different protocol at the switch. IGMP is used from the client to the router. The switch monitors, or sniffs, the IGMP packets as they pass through and records the MAC addresses and the port that requested to be a part of the process.

Because the switch becomes an integral part of the process of IGMP, the router will forward status messages to the switch and the switch will forward them out the appropriate ports. This is the process of Fast-Leave and is done on both CGMP and IGMP Snooping:

- Client A is listening to a multicast stream and decides to stop listening. The client sends an IGMP Leave message to the switch.
- The switch responds with an IGMP Query to find out whether other clients exist that still want that multicast stream.
- If a client exists out that port, the switch makes no changes.
- If there is no reply out that port but other ports are receiving the stream, the switch does nothing.
- If there is no reply to the Query and there are no other ports participating, the switch will forward the Leave to the router.

Real World Scenario

Multicast and Spanning Tree

It might seem that CGMP and IGMP Snooping are the way to go. That is true—if you have a very stable network. Remember that spanning tree is used to allow for redundancy but that it disables the redundant links until they are needed. If you have a switched network with redundant connections and a link drops, spanning tree takes over and figures out the next best topology. Unfortunately, the spanning tree process doesn't tell the multicasting process that this is happening. The switch will still forward the multicast message out the port that it was using. This can cause delays and dropped connections. Eventually it settles down, unless the topology changes are always going on.

Routing Multicast Traffic

Up to this point, we have been discussing the host side of multicast. You have learned how hosts interact with switches and routers to join multicast groups and receive the traffic. It is now time to move on to discuss how multicast traffic travels across the Internet (or intranet) from a source on a remote network to a local router and host.

Unicast data uses routing protocols to accomplish the task of getting data to and from remote destinations. Multicast does the same, but it goes about it in a somewhat different manner. Unicast relies on routing tables. Multicast uses a sort of spanning tree system to distribute its data. This section will describe the tree structures that can be implemented to enable multicast routing. In addition to trees, several different protocol methods can be used to achieve the desired implementation of multicast.

Distribution Trees

Two types of trees exist in multicast:

Source trees *Source trees* use the architecture of the source of the multicast traffic as the root of the tree.

Shared trees *Shared trees* use an architecture in which multiple sources share a common rendezvous point.

Each of these methods is effective and enables sourced multicast data to reach an arbitrary number of recipients of the multicast group. Let's discuss each of them in detail.

Source Tree

Source trees use special notation. This notation is used in what becomes a multicast route table. Unicast route tables use the destination address and next-hop information to establish a topology for forwarding information. Here is a sample from a unicast routing table:

```
B    210.70.150.0/24 [20/0] via 208.124.237.10, 3d08h
B    192.5.192.0/24 [20/0] via 208.124.237.10, 2w1d
B    193.219.28.0/24 [20/0] via 208.124.237.10, 1d03h
B    136.142.0.0/16 [20/0] via 208.124.237.10, 3d07h
```

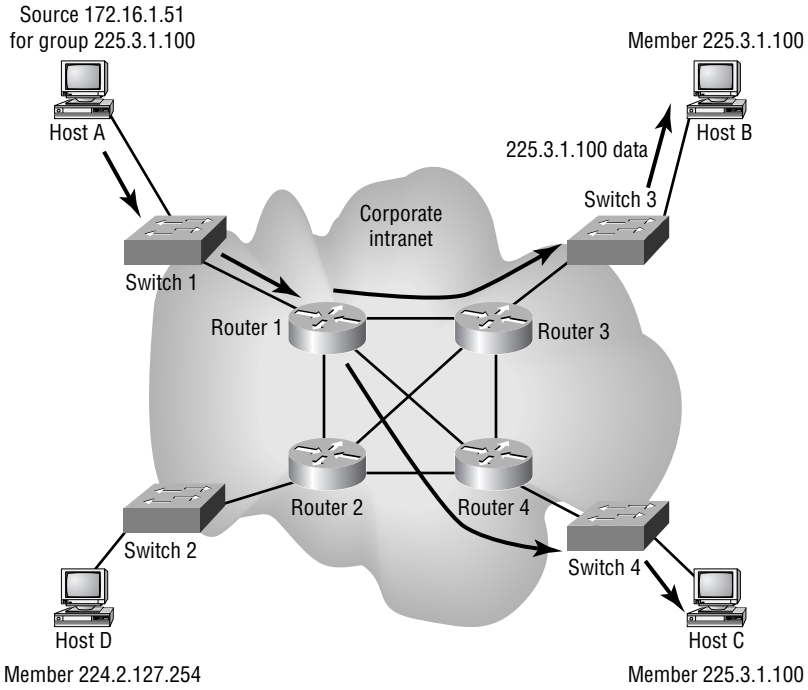
```
B    202.213.23.0/24 [20/0] via 208.124.237.10, 1w2d
     202.246.53.0/24 is variably subnetted, 2 subnets, 2 masks
B       202.246.53.0/24 [20/0] via 208.124.237.10, 1w2d
B       202.246.53.60/32 [20/0] via 208.124.237.10, 1w2d
```

Multicast route tables are somewhat different. A sample of a multicast table follows. Notice that the notation is different. Instead of having the destination address listed and then the next hop to get to the destination, source tree uses the notation (S, G). This notation specifies the source host's IP address and the multicast group address for which it is sourcing information. Let's take the first one, for example. This is seen as (198.32.163.74, 224.2.243.55), which means that the source host is 198.32.163.74 and it is sourcing traffic for the multicast group 224.2.243.55:

```
(198.32.163.74, 224.2.243.55), 00:01:04/00:01:55, flags: PT
  Incoming interface: POS1/0/0, RPF nbr 208.124.237.10, Mbgp
  Outgoing interface list: Null
(198.32.163.74, 224.2.213.101), 00:02:06/00:00:53, flags: PT
  Incoming interface: POS1/0/0, RPF nbr 208.124.237.10, Mbgp
  Outgoing interface list: Null
(195.134.100.102, 224.2.127.254), 00:00:28/00:02:31, flags: CLM
  Incoming interface: POS1/0/0, RPF nbr 208.124.237.10, Mbgp
  Outgoing interface list:
    FastEthernet4/0/0, Forward/Sparse, 00:00:28/00:02:54
    FastEthernet4/1/0, Forward/Sparse, 00:00:28/00:02:31
(207.98.103.221, 224.2.127.254), 00:00:40/00:02:19, flags: CLM
  Incoming interface: POS1/0/0, RPF nbr 208.124.237.10, Mbgp
  Outgoing interface list:
    FastEthernet4/0/0, Forward/Sparse, 00:00:41/00:02:53
    FastEthernet4/1/0, Forward/Sparse, 00:00:41/00:02:19
(128.39.2.23, 224.2.127.254), 00:04:43/00:02:06, flags: CLMT
  Incoming interface: POS1/0/0, RPF nbr 208.124.237.10, Mbgp
  Outgoing interface list:
    FastEthernet4/0/0, Forward/Sparse, 00:04:43/00:02:43
    FastEthernet4/1/0, Forward/Sparse, 00:04:43/00:03:07
(129.237.25.152, 224.2.177.155), 00:17:58/00:03:29, flags: MT
  Incoming interface: POS1/0/0, RPF nbr 208.124.237.10, Mbgp
  Outgoing interface list:
    FastEthernet4/0/0, Forward/Sparse, 00:17:58/00:02:44
```

Figure 8.12 gives you a good picture of how source trees work.

FIGURE 8.12 Source tree forwarding



Also notice in the drawing that the shortest path to the receivers was chosen. This is known as choosing the shortest path tree (SPT). You can see from the preceding output that there are three sources for the same group of 224.2.127.254. This indicates that there are three SPT groups shown here: (195.134.100.102, 224.2.127.254), (207.98.103.221, 224.2.127.254), and (128.39.2.23, 224.2.127.254). Each of these sources has its own shortest path tree to the receivers.

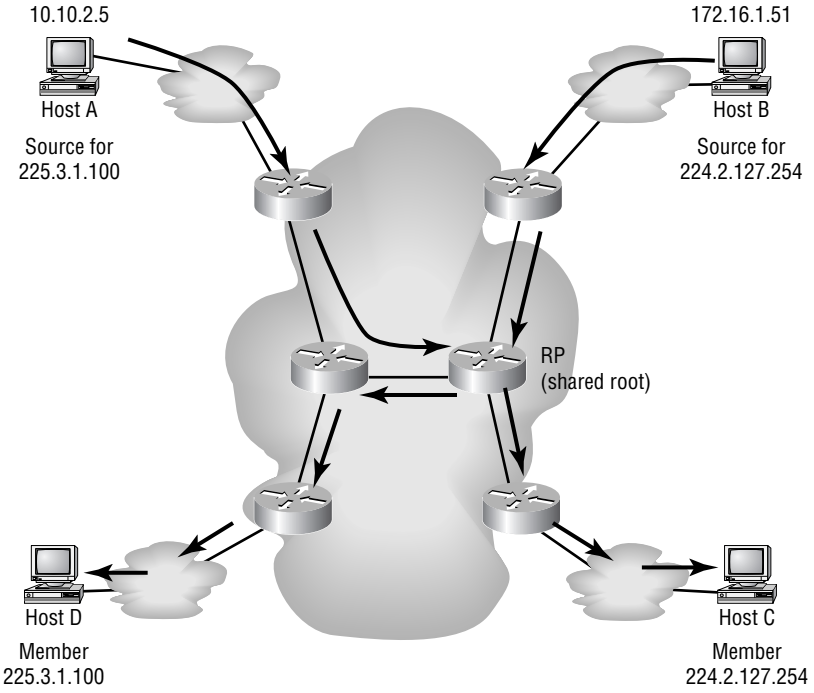
Shared Tree

There are two types of shared tree distribution:

- Unidirectional
- Bidirectional

They both work a little differently than source tree distribution. Shared tree architecture lies in the possibility that there might be multiple sources for one multicast group. Instead of each individual source creating its own SPT and distributing the data apart from the other sources, a shared root is designated. Multiple sources for a multicast group forward their data to a shared root or rendezvous point (RP). The rendezvous point then follows SPT to forward the data to the members of the group. Figure 8.13 depicts how the shared tree distribution works.

FIGURE 8.13 Shared tree forwarding



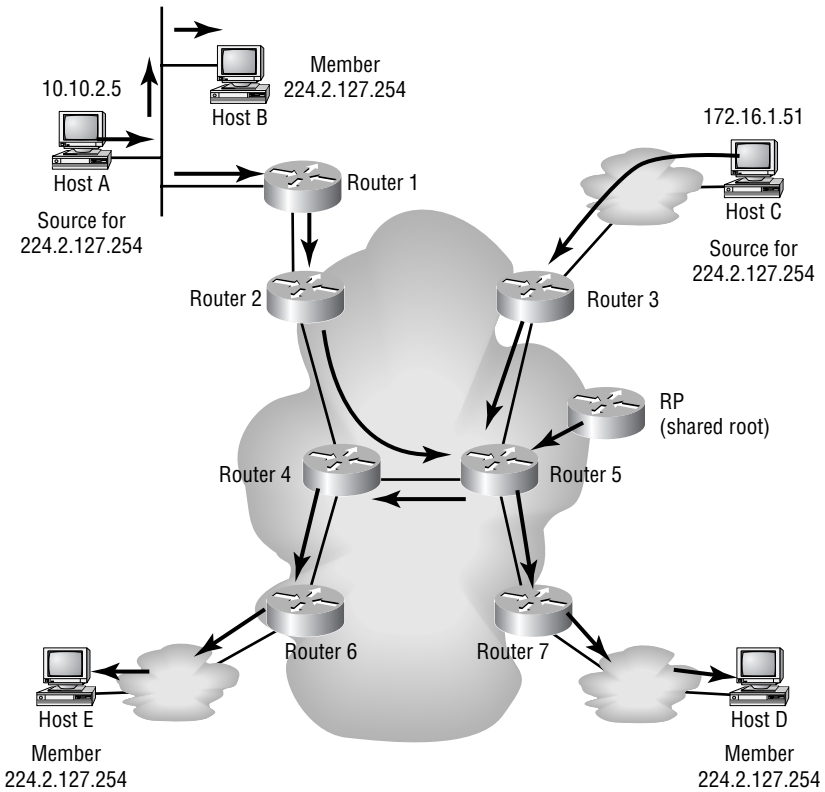
Unidirectional Shared Tree Distribution

Unidirectional shared tree distribution operates as shown in Figure 8.13. All recipients of a multicast group receive the data from a rendezvous point (RP) no matter where they are located in the network. This is very inefficient if subscribers are close to the source because they will need to get the multicast stream from the RP.

Bidirectional Shared Tree Distribution

Bidirectional shared tree distribution operates somewhat differently. If a receiver lives upstream from the RP, it can receive data directly from the upstream source. Figure 8.14 depicts how this works. As you can see, Host A is a source for group 224.2.127.254, and Host B is a receiver of that same group. In a bidirectional shared tree, data goes directly from Host A to Host B without having to come from the RP.

FIGURE 8.14 Bidirectional shared tree



Managing Multicast Delivery

The tree distributions explain how source information is managed; now we must discuss how the actual data delivery is managed. There are several

methods of making sure that delivery is as efficient as possible. The following will be discussed here:

- Reverse Path Forwarding (RPF)
- Time to Live (TTL) attributes
- Routing protocols

Reverse Path Forwarding

RPF works in tandem with the routing protocols, but it will be described briefly here. As you have seen in Figures 8.13 and 8.14, the traffic goes only to the multicast group receivers. We also indicated that bidirectional distribution eliminates the need to forward data upstream. You might ask, "How do you define *upstream*?" It is easy to clarify. By means of the routing protocols, routers are aware of which interface leads to the source(s) of the multicast group. That interface is considered *upstream*.

The Reverse Path Forwarding process is based on the upstream information. After receiving an incoming multicast packet, the router verifies that the packet came in on an interface that leads back to the source. The router forwards the packet if the verification is positive; otherwise, the packet is discarded. This check stops potential loops. To avoid increased overhead on the router's processor, a multicast forwarding cache is implemented for the RPF lookups.

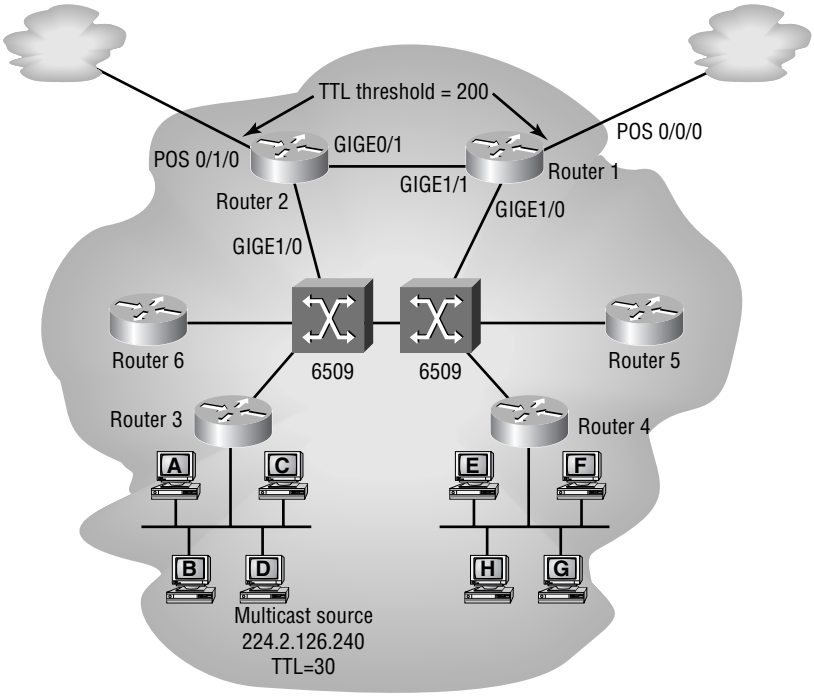
Time to Live (TTL)

You can also control the delivery of IP multicast packets through the TTL counter and TTL thresholds. The Time to Live counter is decremented by one every time the packet hops a router. After the TTL counter is set to zero, the packet is discarded.

Thresholds are used to achieve higher granularity and greater control within one's own network. Thresholds are applied to specified interfaces of multicast-enabled routers. The router compares the threshold value of the multicast packet to the value specified in the interface configuration. If the TTL value of the packet is greater than or equal to the TTL threshold configured for the interface, the packet will be forwarded through that interface.

TTL thresholds enable network administrators to bound their network and limit the distribution of multicast packets beyond the boundaries. This is accomplished by setting high values for outbound external interfaces. The maximum value for the TTL threshold is 255. Refer to Figure 8.15 to see how network boundaries can be set to limit distribution of multicast traffic.

FIGURE 8.15 TTL threshold utilization



The multicast source initially sets the TTL value for the multicast packet and then forwards it on throughout the network. In this scenario, the TTL threshold values have been set to 200 on both of the exiting Packet over Sonet (POS) interfaces. The initial TTL value has been set to 30 by the application. There are three to four router hops to get out of the campus network. Router 3 will decrement by one, leaving a TTL value of 29; the Catalyst 6509's MSFC will decrement by one as well, leaving the value set to 28. After the packet reaches Router 2 or Router 1, the value will be 27 or 26 respectively. Both of these values are less than the TTL threshold of 200, which means Router 1 and Router 2 will drop any outbound multicast packets.

Routing Protocols

Unicast has several routing protocols that build route tables enabling layer 3 devices such as routers and some switches to forward unicast data to the next hop toward its final destination. We have also discussed some of the methods that multicast, in general, uses to distribute multicast data. Similar to

unicast, multicast has a variety of routing protocols, including distance vector and link state protocols.

Protocols are used to enhance the efficiency by which multicast application data is distributed and to optimize the use of existing network resources. This section will cover Distance Vector Multicast Routing Protocol (DVMRP), Multicast Open Shortest Path First (MOSPF), and Protocol Independent Multicast dense mode (PIM DM).

Distance Vector Multicast Routing Protocol (DVMRP)

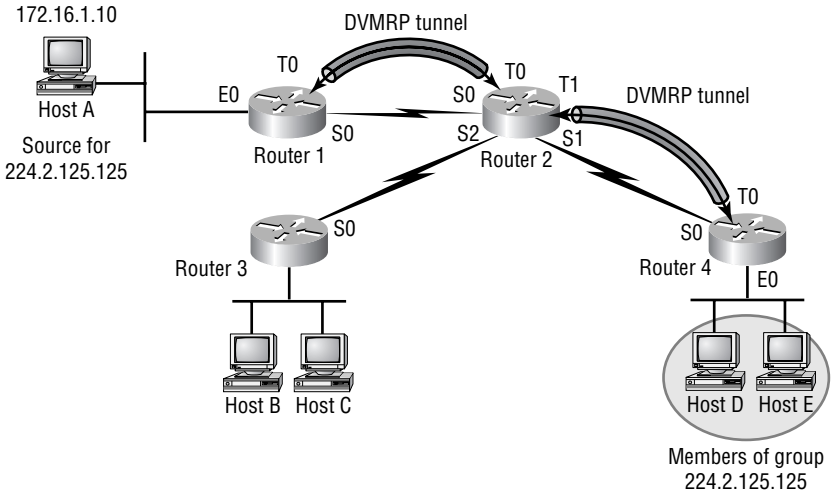
Distance Vector Multicast Routing Protocol (DVMRP) has achieved widespread use in the multicast world. A few years ago, you might have often heard the term "DVMRP tunnel" used when discussing the implementation of multicast feeds from an ISP or a feed from the Multicast Backbone (MBONE). As the name indicates, this protocol uses a distance vector algorithm. It uses several of the features that other distance vector protocols (such as RIP) implement. Some of these features are a 32 max hop-count, poison reverse, and 60-second route updates. It also allows for IP classless masking of addresses.

Just as with other routing protocols, DVMRP-enabled routers must establish adjacencies in order to share route information. After the adjacency is established, the DVMRP route table is created. Route information is exchanged via route reports. It is important to remember that the DVMRP route table is stored separately from the unicast routing table. The DVMRP route table is more like a unicast route table than the multicast route table that was shown earlier in this chapter. A DVMRP table contains the layer 3 IP network of the multicast source and the next hop toward the source.

Because the DVMRP table has this form, it works perfectly with source tree distribution, as discussed earlier. Using the information in the DVMRP table, the tree for the source can be established. In addition, the router uses this information to perform the Reverse Path Forwarding check to verify that the multicast data coming into the interface is coming in an interface that leads back to the source of the data. DVMRP uses SPT for its multicast forwarding.

Figure 8.16 shows how DVMRP works. You can see that not every router in the network is a DVMRP router. You should also notice that the adjacencies are established over tunnel interfaces. DVMRP information is tunneled through an IP network. On either end of the tunnel, information is learned and exchanged to build a multicast forwarding database or route table.

FIGURE 8.16 DVMRP tunnels



Multicast Open Shortest Path First (MOSPF)

Multicast Open Shortest Path First (MOSPF) is a link state protocol. OSPFv2 includes some changes that allow multicast to be enabled on OSPF-enabled routers. This eliminates the need for tunnels such as those used for DVMRP.

To completely understand the full functionality of MOSPF, you must have a thorough understanding of OSPF itself. However, here we will cover only the basic functionality of MOSPF, so you should be fine with just a basic understanding of OSPF.

For more on OSPF, see *CCNP: Routing Study Guide,* Second Edition by Todd Lammle and Raymond Doucette (Sybex, 2002).

MOSPF's basic functionality lies within a single OSPF area. Design gets more complicated as you route multicast traffic to other areas (inter-area routing) or to other autonomous systems (inter-AS routing). This additional complication requires more knowledge of OSPF routing. We will briefly discuss how this is accomplished in MOSPF, but most detail will be given regarding MOSPF intra-area routing.

Intra-area MOSPF

OSPF route information is shared via different Link State Advertisement (LSA) types. LSAs are flooded throughout an area to give all OSPF-enabled routers a logical image of the network topology. When changes are made to the topology, new LSAs are flooded to propagate the change.

In addition to the unicast-routing LSA types, in OSPFv2 there is a special multicast LSA for flooding multicast group information throughout the area. This additional LSA type required some modification to the OSPF frame format.

Here is where you need to understand a little about OSPF. Multicast LSA flooding is done by the Designated Router (DR) when multiple routers are connected to a multi-access media, such as Ethernet. On point-to-point connections, there are no DR and Backup Designated Router (BDR). Look at the following code from a Cisco router running OSPF over point-to-point circuits:

```
Neighbor ID    Pri    State          Dead Time    Address         Interface
172.16.1.2       1    FULL/  -       00:00:31     172.16.1.2      Serial3/0
192.168.1.2      1    FULL/  -       00:00:39     192.168.1.2     Serial3/1
```

On a multi-access network, the DR must be multicast enabled, that is, running MOSPF. If any non-MOSPF routers are on the same network, their OSPF priority must be lowered so none of them become the DR. If a non-MOSPF router were to become the DR, it would not be able to forward the multicast LSA to the other routers on the segment.

Inside the OSPF area, updates are sent describing which links have active multicast members on them so that the multicast data can be forwarded to those interfaces. MOSPF also uses (S, G) notation and calculates the SPT by using the Dijkstra algorithm. You must also understand that an SPT is created for each source in the network.

Inter-area and Inter-AS MOSPF

When discussing the difference between intra-area and inter-area MOSPF, you must remember that all areas connect through Area 0, the backbone. In large networks, having full multicast tables in addition to all the unicast tables flow across Area 0 would cause a great deal of overhead and possibly latency.

Unicast OSPF uses a Summary LSA to inform the routers in Area 0 about the networks and topology in an adjacent area. This task is performed by

the area's Area Border Router (ABR). The ABR summarizes all the information about the area and then passes it on to the backbone (Area 0) routers in a summary LSA. The same is done for the multicast topology. The ABR summarizes which multicast groups are active and which groups have sources within the area. This information is then sent to the backbone routers.

In addition to summarizing multicast group information, the ABR is responsible for the actual forwarding of multicast group traffic into and out of the area. Each area has an ABR that performs these two functions within an OSPF network.

OSPF implements Autonomous System Border Routers to be the bridges between different autonomous systems. These routers perform much the same as an ABR but must be able to communicate with non-OSPF speaking devices. Multicast group information and data is forwarded and received by the Multicast Autonomous Border Router (MASBR). Because MOSPF runs natively within OSPF, there must be a method or protocol by which the multicast information can be taken from MOSPF and communicated to the external AS. Historically, DVRMP has provided this bridge.

PIM DM

There are three types of *Protocol Independent Multicast (PIM)*; sparse mode, dense mode, and a combination of the two. Although *PIM dense mode (PIM DM)* maintains several functions, the ones that will be discussed here are flooding, pruning, and grafting. We'll talk about sparse mode later in this chapter.

PIM is considered "protocol independent" because it actually uses the unicast route table for RPF and multicast forwarding. PIM DM understands classless subnet masking and uses it when the router is running an IP classless unicast protocol.

PIM DM routers establish neighbor relationships with other routers running PIM DM. It uses these neighbors to establish an SPT and forward multicast data throughout the network. The SPT created by PIM DM is based on source tree distribution.

PIM, either sparse mode or dense mode, is the method that Cisco recommends for multicast routing on their routers.

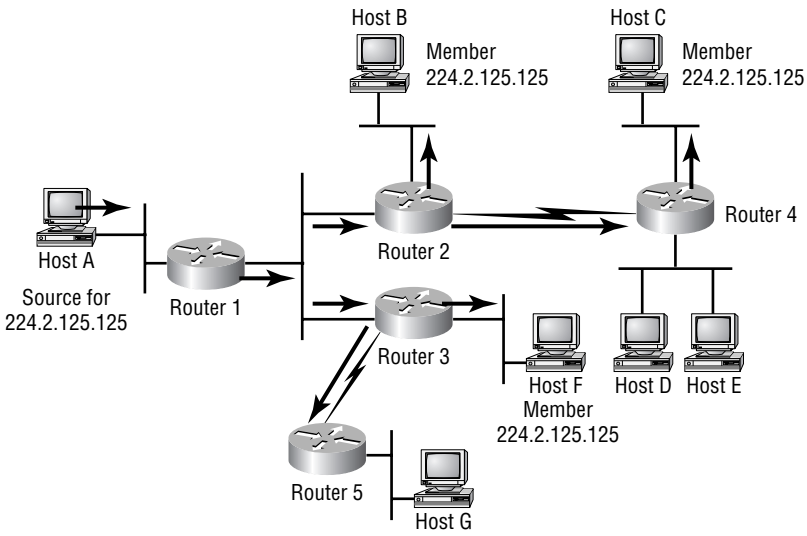
FLOODING

When a multicast source begins to transmit data, PIM runs the RPF, using the unicast route table to verify that the interface leads toward the source. It then forwards the data to all PIM neighbors. Those PIM neighbors then forward the data to their PIM neighbors. This happens throughout the network, whether there are group members on the router or not. Every multicast-enabled router participates; that is why it is considered *flooding* and is where the term "dense mode" comes from.

When multiple, equal-cost links exist, the router with the highest IP address is elected to be the incoming interface (used for RPF). Every router runs the RPF when it receives the multicast data.

Figure 8.17 depicts the initial multicast flooding in a PIM DM network. You can see that the data is forwarded to every PIM neighbor throughout the network. After a PIM neighbor does the RPF calculation, the router will then forward the data to interfaces that have active members of the group.

FIGURE 8.17 PIM DM flooding



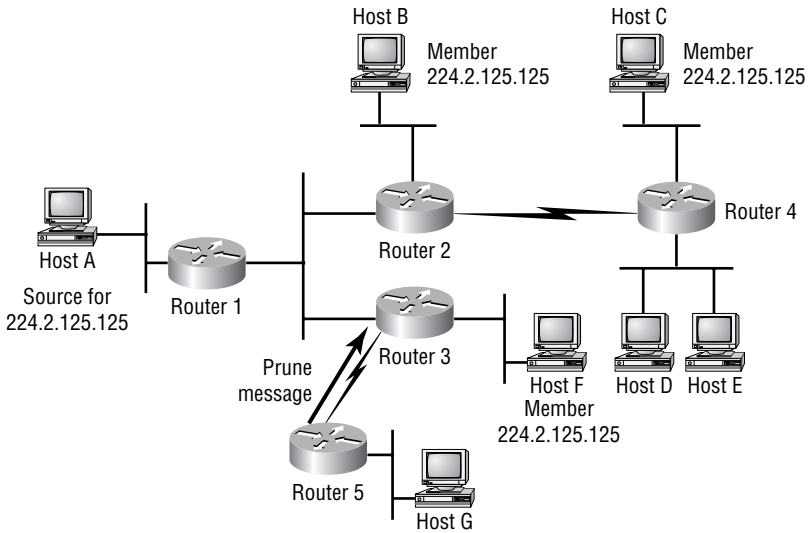
PRUNING

After the initial flooding through the PIM neighbors, pruning starts. *Pruning* is the act of trimming down the SPT. Because the data has been forwarded to every router, regardless of group membership, the routers must now

prune back the distribution of the multicast data to routers that actually have active group members connected.

Figure 8.18 shows the pruning action that occurs for the PIM DM routers that don't have active group members. Router 5 does not have any active group members, so it sends a prune message to Router 3. Even though Router 4 has a network that does not have members, it does have an interface that does, so it will not send a prune message.

FIGURE 8.18 PIM DM pruning



Four criteria merit a prune message being sent by a router:

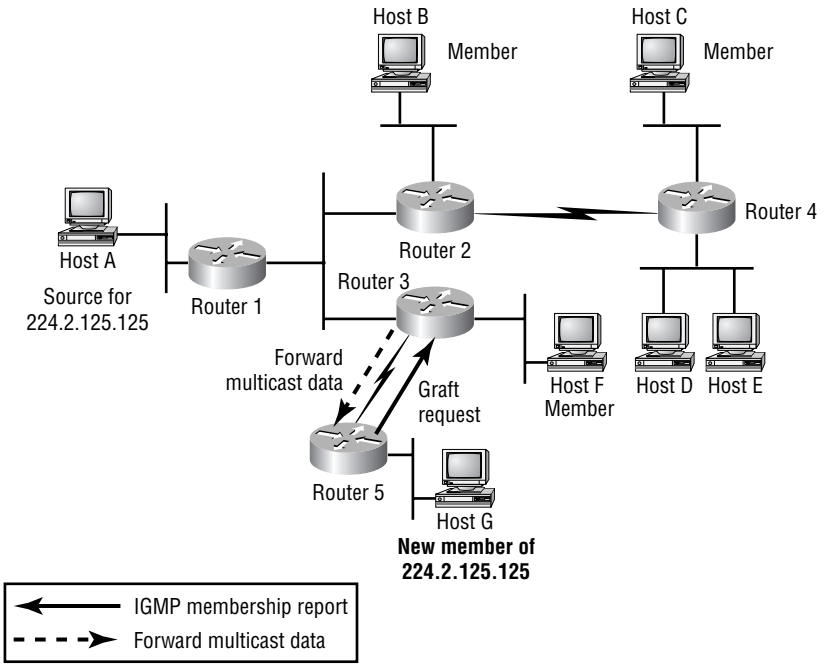
- The incoming interface fails the RPF check.
- There are no directly connected active group members and no PIM neighbors (considered a leaf router because it has no downstream PIM neighbors).
- A point-to-point non-leaf router receives a prune request from a neighbor.
- A LAN non-leaf router receives a prune request from another router, and no other router on the segment overrides the prune request.

If any of these criteria are met, a prune request is sent to the PIM neighbor and the SPT is pruned back.

GRAFTING

PIM DM is also ready to forward multicast data after a previously inactive interface becomes active. This is done through the process of *grafting*. When a host sends an IGMP group membership report to the router, the router then sends a Graft message to the nearest upstream PIM neighbor. After this message is acknowledged, multicast data begins to be forwarded to the router and on to the host. Figure 8.19 depicts the grafting process.

FIGURE 8.19 PIM DM grafting



Sparse Mode Routing Protocols

Sparse mode protocols use shared tree distribution as their forwarding methods. This is done to create a more efficient method of multicast distribution. Two sparse mode protocols will be discussed in this section:

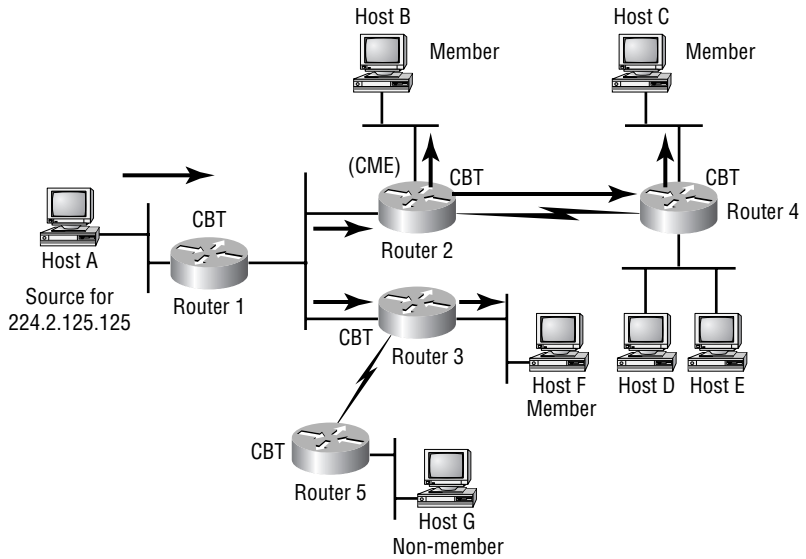
- Core-based trees (CBT)
- Protocol Independent Multicast sparse mode (PIM SM)

Core-Based Trees

When we discussed shared trees, you learned that there were two types, unidirectional and bidirectional. CBT utilizes the bidirectional method for its multicast data distribution. Because CBT uses a shared tree system, it designates a *core* router that is used as the root of the tree, enabling data to flow up or down the tree.

Data forwarding in a CBT multicast system is similar to the shared tree distribution covered earlier. If a source to a multicast group sends multicast data to the CBT-enabled router, the router then forwards the data out all interfaces that are included in the tree, not just the interface that leads to the core router. In this manner, data flows up and down the tree. After the data gets to the core router, the core router then forwards the information to the other routers that are in the tree. Figure 8.20 depicts this process.

FIGURE 8.20 CBT data distribution



It is important to see the difference between this sparse mode method and the dense mode method. In sparse mode operation, routers are members of the tree only if they have active members directly connected. Notice in Figure 8.20 that Router 5 is not participating. Dense mode operates on the initial premise that all PIM neighbors have active members directly connected. The tree changes when the directly connected routers request to be pruned from the tree.

A CBT router might become part of the tree after a host sends an IGMP Membership Record to the directly connected router. The router then sends a join tree request to the *core* router. If the request reaches a CBT tree member first, that router will add the *leaf* router to the tree and begin forwarding multicast data.

Pruning the tree is done much the same way. When there are no more active members on a router's interfaces, the router will send a prune request to the upstream router. The answering router will remove the interface from the forwarding cache if it is on a point-to-point circuit, or it will wait for a timer to expire it if is on a shared access network. The timer gives enough time for other CBT routers on the segment to override the prune request.

PIM SM

PIM sparse mode (PIM SM) also uses the architecture of shared tree distribution. There is an RP (rendezvous point) router that acts as the root of the shared tree. Unlike CBT, however, PIM SM uses the unidirectional shared tree distribution mechanism. Because PIM SM uses the unidirectional method, all multicast sources for any group must register with the RP of the shared tree. This enables the RP and other routers to establish the RPT, or RP tree (synonymous with SPT in source tree distribution).

Just as with CBT, PIM SM routers join the shared tree when they are notified via IGMP that a host requests membership of a multicast group. If the existing group entry (*, G) does not already exist in the router's table, it is created and the join tree request is sent to the next hop toward the RP. The next router receives the request. Depending on whether it has an exiting entry for (*, G), two things can happen:

- If an entry for (*, G) exists, the router simply adds the interface to the shared tree and no further join requests are sent toward the RP.
- If an entry for (*, G) does not exist, the router creates an entry for the (*, G) group and adds the link to the forwarding cache. In addition to doing this, the router sends its own join request toward the RP.

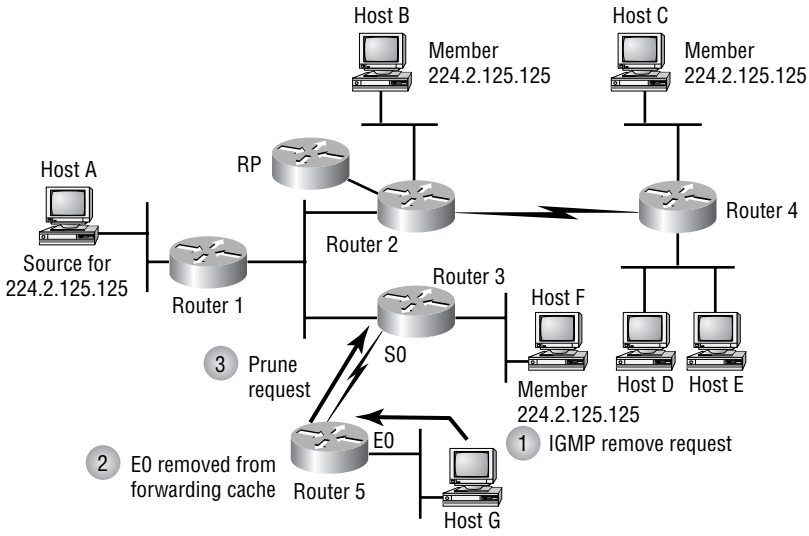
This happens until the join request reaches a router that already has the (*, G) entry or a join request reaches the RP.

The next facet of PIM SM is the shared tree pruning. With PIM SM, pruning turns out to be just the opposite of the explicit Join mechanism used to construct the shared tree.

When a member leaves a group, it does so via IGMP. When it happens to be the last member on a segment, the router removes the interface from the forwarding cache entry and then sends a prune request toward the RP of

the shared tree. If there is another router with active members connected to the router requesting the prune, it is removed from the outgoing interface list and no additional Prune messages are sent to the RP. See Figure 8.21 for a visual description.

FIGURE 8.21 PIM SM pruning



Router 5 receives an IGMP message requesting the removal of Host G from the group. Because Host G was the last active member of the group, the (*, G) entry is set to null 0 and a prune request is sent by Router 5 to Router 3. When Router 3 receives the request, it removes the link for interface S0 from the forwarding table. Because Host F is a directly connected active member of the group, the entry for (*, G) is not null 0, so no prune request is sent to Router 2 (the RP for this example).

If Host F were not active, the entry for (*, G) would have been set to null 0 also and a prune request would have been sent to the RP.

Summary

In this chapter, we described the many facets of IP multicast. We started with an overview of multicast and compared it to unicast and broadcast communication. We then discussed how IP addresses were designated as multicast addresses. You learned how to convert them to layer 2 MAC addresses also.

The implementation of multicast can have a significant impact on a network. This merited the topics regarding managing multicast distribution. After you understood the basics of multicast and how hosts and sources participate, we were able to move on and cover the types of routing protocols that were made for multicast routing. Finally, we discussed PIM-DM, PIM-SM, and CBT. These are independent protocols that use tree distribution to manage multicast data delivery in a network.

Because this chapter focused on theory instead of configuration, this chapter doesn't include a written lab or hands-on lab. You'll learn more about configuring multicast in Chapter 9.

Exam Essentials

Know the difference between the IGMP and IGMPv2. Understand that ICMP and ICMP v2 are almost the same thing. The major difference is that ICMPv2 has a message that the client will send when it doesn't want to receive the multicast stream anymore. Know that they don't work well together and that you should have only one version running.

Know the difference between CGMP and IGMP Snooping. Although CGMP and IGMP Snooping both allow a switch to get involved in a multicast stream, they are rather different. CGMP is a communication from the router to the switch. The router receives IGMP packets and forwards specific information to the switch. IGMP Snooping enables the switch to learn information from watching IGMP packets go through the switch. CGMP is a Cisco proprietary protocol, whereas IGMP Snooping is being considered by the IETF as a standard.

Know the difference between the multicast routing protocols. Understand that DVMRP is a distance vector-based routing protocol and that MOSPF uses OSPF. Also know that neither is the recommended method of doing multicast routing with Cisco equipment. Cisco recommends that PIM be used to route multicast streams because it learns from the preexisting routing protocol. This means that EIGRP can be used to route multicast information.

Know the difference between PIM dense mode and sparse mode. PIM has two broad modes, sparse and dense. In dense mode PIM, each router will automatically be included in the multicast table and will have to prune itself off if no clients need the stream. Sparse mode assumes no routers wish to participate. Routers are added as connected clients request access to the multicast streams.

Key Terms

Before you take the exam, be sure you're familiar with the following terms:

bidirectional shared tree	multicast
broadcast	multicast group
Cisco Group Management Protocol (CGMP)	Multicast Open Shortest Path First (MOSPF)
Distance Vector Multicast Routing Protocol (DVMRP)	PIM dense mode (PIM DM)
flooding	PIM sparse mode (PIM SM)
grafting	Protocol Independent Multicast (PIM)
IGMP Join process	pruning
IGMP Leave process	shared trees
IGMP Query process	source trees
Internet Group Management Protocol version 1 (IGMPv1)	unicast
Internet Group Management Protocol version 2 (IGMPv2)	unidirectional shared tree

Review Questions

1. Which of the following is the valid range of IP multicast addresses?
   - **A.** 223.0.0.0–239.255.255.255
   - **B.** 224.0.0.0–225.255.255.255
   - **C.** 224.0.0.0–239.0.0.0
   - **D.** 224.0.0.0–239.255.255.255

2. Which of the following addresses is within the range of valid IP multicast addresses? (Choose all that apply.)
   - **A.** 242.127.1.1
   - **B.** 224.0.0.1
   - **C.** 239.255.255.254
   - **D.** 225.128.1.1

3. What is the main difference between broadcast and multicast communication?
   - **A.** Multicast data is distributed to subscribed hosts on specific groups.
   - **B.** Broadcast data is distributed to subscribed hosts on specific groups.
   - **C.** Multicast data uses unicast route tables to flood the network instead of using the network's broadcast address.
   - **D.** There really is no difference.

4. What is the purpose of the reserved IP multicast address 224.0.0.1?
   - **A.** All MOSPF routers
   - **B.** All multicast routers
   - **C.** All hosts
   - **D.** All CGMP-enabled hosts

5. What is the purpose of the reserved IP multicast address 224.0.0.2?

   A. All DVMRP routers

   B. All routers

   C. All hosts

   D. All CGMP-enabled routers

6. What is the MAC prefix (first 24 bits) that identifies a multicast MAC address?

   A. 01-00-5E

   B. 01-00-5F

   C. FF-FF-FF

   D. 01-00-50

7. How many bits of the layer 3 IP address are used to map to the layer 2 MAC address?

   A. 24

   B. 22

   C. 25

   D. 23

8. How many layer 3 IP addresses can be represented by the same layer 2 MAC address?

   A. 1

   B. 23

   C. 32

   D. 24

9. What is the layer 2 MAC address for the layer 3 IP address 224.2.127.254?

   A. 01-00-5E-02-7E-FF

   B. 01-00-5E-02-7F-FE

   C. 01-00-5E-00-7E-FF

   D. 01-00-5E-00-7F-FE

10. What is the layer 2 MAC address for the layer 3 IP address 224.224.155.155?

    A. 01-00-5E-70-9B-9B

    B. 01-00-5E-40-9B-9B

    C. 01-00-5E-60-9B-9B

    D. 01-00-5E-30-9B-9B

11. What is the layer 2 MAC address for the layer 3 IP address 224.215.145.230?

    A. 01-00-5E-57-91-E6

    B. 01-00-5E-D7-91-E6

    C. 01-00-5E-5B-91-E6

    D. 01-00-5E-55-91-E6

12. Which of the following protocols can hosts use to subscribe to a multicast group? (Choose all that apply.)

    A. IBMP

    B. IGMPv1

    C. IGMPv2

    D. CGMP

    E. DVMRP

    F. MOSPF

    G. PIM (DM/SM)

    H. CBT

13. Why do Cisco Catalyst switches use CGMP instead of just using IGMP?

    A. Cisco's proprietary code is easier to compile into IOS.

    B. Cisco catalysts don't understand IGMP packets.

    C. Routers need switches to translate IGMP requests into CGMP requests in order to process them.

    D. Catalysts can't distinguish between membership report packets and actual multicast data packets.

14. How does a host connected to a Catalyst switch subscribe to a multicast group? (Choose all that apply.)

    A. It sends an IGMP request directly to the sc0 interface on the switch.

    B. It sends an IGMP membership report to the router.

    C. It sends a CGMP membership report to the router.

    D. It sends a CGMP membership report to the switch.

    E. The router converts the CGMP to IGMP and forwards it to the switch for processing.

    F. The router converts the IGMP membership request to a CGMP join request and forwards it to the switch for processing.

15. What two address values does CGMP use compared to IGMP?

    A. CGMP utilizes the USA and GDA.

    B. CGMP utilizes the MAC address and IP address.

    C. CGMP utilizes the GSA and UDA.

    D. CGMP uses the MAC address and switch port.

16. What are the two types of distribution trees?

    A. RP trees

    B. Multicast trees

    C. Shared root trees

    D. Source root trees

17. What are two types of shared root tree distributions?

A. Unidirectional

B. Unicast

C. Multidirectional

D. Bidirectional

18. What multicast attribute can be applied to multicast router interfaces to limit the scope of multicast group and data distribution?

A. TTY

B. IP access lists

C. TTL thresholds

D. Multicast disabled on the router

19. How does PIM DM differ from PIM SM? (Choose all that apply.)

A. PIM DM assumes that all PIM neighbors have active members directly connected and initially forwards multicast data out every interface.

B. PIM SM requires an explicit join from a router before the router is added to the shared tree.

C. PIM DM is based on a source root tree distribution mechanism.

D. PIM SM is based on bidirectional shared root tree distribution.

20. How does CBT differ from PIM SM?

A. CBT uses unidirectional shared root tree distribution.

B. CBT uses bidirectional shared root tree distribution.

C. CBT routers are included in the tree only when there are active hosts directly connected.

D. PIM SM uses the unicast route table to verify the RPF.

Answers to Review Questions

1. D. The valid range of IP addresses for multicast starts at 224.0.0.0. Anything lower than that is not within the specified range. The range continues until 239.255.255.255, which specifies the entire Class D network. That makes the last answer correct.
2. B, C, D. The first response is outside of the valid range for IP multicast addresses. The other choices are valid host addresses within the range.
3. A. Broadcast communications use the broadcast IP or MAC address to communicate information to all hosts. Multicast data is sent only to hosts subscribing to groups that are active on the network.
4. C. IANA reserved the address 224.0.0.1 for all multicast hosts on a local segment. This address is not routed or forwarded by routers.
5. B. IANA reserved the address 224.0.0.2 to indicate all local multicast routers. Again, this address is not forwarded by any routers in the network.
6. A. The first 24 bits of a MAC address were assigned the value of 0x01005e for all multicast addresses. The other values do not designate a multicast MAC address.
7. D. Because only one half of one OEM was allocated for individual multicast MAC addresses, only 23 bits transfer from the layer 3 IP address.
8. C. Due to the lost 5 bits in the mapping, 32 IP addresses may be represented by the same multicast MAC address. $2^5 = 32$.
9. B. The MAC prefix is 01-00-5E. You know you don't have to worry about the lost bits because the second octet of the IP address is less than 127. Therefore, the value is 02. The last two octets are mapped with no problem.
10. C. Again, the MAC prefix is 01-00-5E. Now that the second octet is greater than 127, you need to remember that it is possible that the value in the high order bit will be discarded. In this case, it was discarded, which leaves a binary value of 1100000 that needs to be converted to hex. In turn, that leaves 60 as the value for the fourth octet of the MAC address.

11. A. Again, the MAC prefix is 01-00-5E. Now that the second octet is greater than 127, you need to remember that it is possible that the value in the high order bit will be discarded. In this case, it was, which leaves a binary value of 1010111 that needs to be converted to hex. In turn, that leaves 57 as the value for the fourth octet of the MAC address.

12. B, C. CGMP is Cisco's proprietary version of IGMP. IBMP is not a valid protocol. The other protocols are for routing purposes and group management within a network.

13. D. Because IGMP is an overloaded protocol, the switches cannot distinguish between membership report packets and normal IGMP packets containing data. The router must run CGMP in order to translate the IGMP requests received from the hosts into something the switch can process.

14. B, F. There is a little more detail involved than just these two steps, but the host can speak only IGMP, and it sends its requests directly to the router. The router must then communicate with the switch to activate the port.

15. A. The USA is the Unicast Source Address (the unique MAC address of the machine), and the GDA is the Group Destination Address (the newly mapped layer 2 multicast MAC address). By using these two values, the switch knows which port to make a CAM entry for.

16. C, D. Multicast trees don't exist. Some protocols that are based in shared root trees can create RPTs (or RP trees) that are parallel to the shortest path tree, but this is a flavor of shared root tree distribution.

17. A, D. We are discussing multicast in this chapter, so unicast is not a valid answer. Because there are only two directions on a tree, the correct answers are bidirectional and unidirectional.

18. C. TTY is a telecommunications term, and IP access lists are not multicast attributes. TTL thresholds are used to compare against the TTL value of a multicast packet. Disabling multicast on the router works, but it isn't necessarily an attribute.

19. A, B, C. The problem with the last answer is that PIM SM is based on unidirectional shared root tree distribution.

20. B. The last two answers are actually similarities between the two protocols. PIM SM uses unidirectional shared root tree distribution.

Chapter

9

Configuring Multicast

THE CCNP EXAM TOPICS COVERED IN THIS CHAPTER INCLUDE THE FOLLOWING:

- ✓ **Enable CGMP on the distribution layer devices**
- ✓ **Describe the functionality of CGMP**
- ✓ **Describe how switches facilitate Multicast Traffic**

This chapter will cover the steps and syntax for configuring IP multicast on Cisco routers and switches. You will see several new commands in this chapter. Learning about multicast and actually getting it working on a network are two different things. By the time you finish this chapter, questions, and lab, you will be thoroughly familiar with multicast and its implementation. Pay attention to small details that would usually seem unimportant. They are often the key to a successful implementation of an IP multicast network.

First you will need to understand how to deploy an IP multicast network. After you have a plan in place, you can move on to configuring equipment. Not only do the routers have to be IP multicast enabled, but you must enable a multicast protocol on every interface through which you want to be able to forward multicast traffic.

An IP multicast network won't work too well without a couple of (or at least one) rendezvous points (RPs), so you'll have to configure them as well. Then, to keep your multicast local to the enterprise network, you'll need to configure the Time to Live (TTL) thresholds on your external interfaces.

After the routers have been configured, you can concentrate on the hosts. Of course, we won't discuss host configuration in this chapter, but we will enable Cisco Group Management Protocol (CGMP) on the routers and switches, so that after the hosts are configured, the network will be available.

Planning and Preparing for Using IP Multicast

As you learned in Chapter 8, "Multicast," multicast networks behave differently than unicast networks. It is important to keep this in mind when planning the deployment of an IP multicast network. You should take

several factors into consideration, including bandwidth implications, use of multicast applications, application requirements, user requirements, the location of the recipients, required equipment, cost, and most importantly, what multicast source(s) will be used.

All these factors require attention and planning for a successful deployment of IP multicast throughout the network. You must also think upside down when thinking about multicast routing. As discussed in the preceding chapter, distribution trees are built based on the position of the root (source) of the tree. Therefore, when planning the routing for the multicast network, you must know where your sources or RPs will be located.

By taking the time to plan and prepare for a multicast deployment, you will avoid headaches later. You must become familiar with the customer's requirements as well as the effects that multicast will have on the existing network.

There are many methods of implementing multicast on a network. Commonly, institutions will want to connect with the Multicast Backbone (MBONE) multicast sessions; therefore, they must implement multicast through a Distance Vector Multicast Routing Protocol (DVMRP) tunnel or with Multicast Border Gateway Protocol (MBGP). If the multicast source is within the network and meant to stay within the confines of the network, other design issues come into play. It is important that you understand what each multicast routing protocol brings to the table when it comes to operational functionality.

By better understanding the many protocols and possible implementations of multicast, you will be able to better plan and prepare for its deployment. With so many options, there is bound to be a solution for almost any requirement. Through understanding requirements, and through preparing and planning, you can successfully implement an IP multicast network.

End-to-End IP Multicast

Part of deploying multicast is the determination of how much of the network should be multicast enabled. This is an important decision because it directly affects many aspects of multicast implementation. To strategically place the *rendezvous points (RPs)*, you must know where all the multicast leaf routers will be. Knowing the approximate number of potential multicast subscribers can have an effect on which protocols are run in the network to allow efficient multicast forwarding and routing.

The decision to use end-to-end deployment can be based on the applications that will be used or the intent of multicast implementation. If you are enabling multicast for a corporate application, you would need to enable multicast on every interface on every router throughout the enterprise. However, if you need to provide access to only the MBONE for the engineering department, or some other department within the organization, perhaps the most efficient method would not include end-to-end configuration and deployment.

It is important to keep in mind that the state of technology is dynamic. Today, you might receive a request from a single department for multicast access. Before jumping on the project and planning for just that department, consider that in the near future, it is likely that other departments will also request access. Applications that will require end-to-end multicast capability might be purchased or integrated into the enterprise. It is far better to plan an end-to-end deployment and initially activate only the routers and interfaces that are needed than to plan your implementation on a limited initial activation. It will be easier to "build it right the first time" than to try to come back and work around or rebuild a poor IP multicast deployment.

Configuring IP Multicast Routing

When configuring multicast, keep in mind that many options and protocols can be configured. This is why it is so important that you have previously prepared and planned for the actual configuration. It isn't something that you can just sit down and throw together (not without a lot of problems anyway).

Configuring routers for IP multicast is different from enabling CGMP on switches. You must also remember that switches do not understand Internet Group Management Protocol (IGMP) by default, and that you will need to enable multicasting on switches and routers for hosts to be able to subscribe to a multicast group.

This section of the chapter covers the basics of configuring multicast on routers and switches. It also covers the configuration of rendezvous points. This is a very important task because without a rendezvous point, you will not be able to send or receive multicast packets across a network. We will also cover the individual interface configurations on routers. CGMP processes will be discussed in a little more detail than in the preceding chapter. Later, we

will describe the multicast settings that can be made on a multicast-enabled router (and switches). "Enabling IP Multicast Routing" and "Enabling PIM on an Interface" describe required configuration, whereas the configuration described in the rest of this section is optional.

It is best to prepare a configuration task list before setting out to configure a group of routers. The configuration list should be specific to the device that will be configured. That fact makes it hard to present a set list of configuration tasks that would apply to all scenarios. However, two items definitely must be configured on a router in order for multicast to even begin working: enabling multicast routing and enabling Protocol Independent Multicast (PIM) on the interfaces that will carry multicast traffic.

Enabling IP Multicast Routing

As we have said, multicast routing must be enabled on the router. This step is very straightforward, but without it, multicast will not work. Let's look at a configuration of a router that does not have multicast enabled:

```
Current configuration:
!
version 12.0
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname RouterA
!
aaa new-model
aaa authentication login default tacacs+ line
aaa authentication login oldstyle line
aaa accounting exec default start-stop tacacs+
enable secret 5 $1$G7Dq$em.LpM4Huem9uqjZDHLe4.
!
!
!
ip subnet-zero
ip telnet source-interface FastEthernet3/0
[Output Truncated]
```

Notice that no multicast information is running on this machine. If we were to try to execute a multicast-related command, we wouldn't get any information returned. For example, look at what happens when the `show ip mroute` command is issued:

```
RouterA#sho ip mroute
IP Multicast Routing Table
Flags: D - Dense, S - Sparse, C - Connected, L - Local,
P - Pruned R - RP-bit set, F - Register flag,
 T - SPT-bit set,J - Join SPT, M - MSDP created entry,
   X - Proxy Join Timer Running
       A - Advertised via MSDP
Timers: Uptime/Expires
Interface state: Interface, Next-Hop or VCD, State/Mode


RouterA#
```

The syntax for the command is `ip multicast-routing`, and an example of the execution follows:

```
RouterA#configure terminal
Enter configuration commands, one per line.  End with
  CNTL/Z.
RouterA(config)#ip multicast-routing
RouterA(config)#^Z
RouterA#
```

This enables the multicast on the router. Notice that it was executed while in global configuration mode. However, the router still cannot exchange multicast information with any neighbors because none of the interfaces have been enabled. This step is next.

Enabling PIM on an Interface

Protocol Independent Multicast (PIM) is one of the required elements for multicast configuration. It enables IGMP on the router and enables it to receive and forward traffic on the specified interface. PIM must be enabled on every interface that is to participate in the multicast network.

PIM interface configuration has many options. Take a look at the available options in IOS 12.0(10)S1, shown in Table 9.1. Most of these options are for advanced multicast configuration that won't be addressed in detail

here. The ones that will be discussed are `dense-mode`, `sparse-mode`, and `sparse-dense-mode`.

TABLE 9.1 IP PIM Configuration Options

IP PIM Options	Description
`bsr-border`	Specifies border of PIM domain
`dense-mode`	Enables PIM dense mode operation
`nbma-mode`	Specifies use of Non-Broadcast Multi-Access (NBMA) mode on interface
`neighbor-filter`	Specifies PIM peering filter
`query-interval`	Specifies PIM router query interval
`sparse-dense-mode`	Enables PIM sparse-dense mode operation
`sparse-mode`	Enables PIM sparse mode operation
`version`	Displays PIM version

IP PIM Dense Mode

Dense mode was discussed in Chapter 8. PIM dense mode functions by using the source root shared tree. It also assumes that all PIM neighbors have active multicast members directly connected and, therefore, it initially forwards multicast group data out all PIM-enabled interfaces.

The syntax for this command is simple: `ip pim dense-mode`. An example of placing an interface in PIM dense mode follows:

```
RouterA#configure terminal
Enter configuration commands, one per line.  End with
  CNTL/Z.
RouterA(config)#interface FastEthernet3/0
RouterA(config-if)#ip pim dense-mode
RouterA(config-if)#^Z
RouterA#
```

This is what the interface configuration looks like now:

```
!
interface FastEthernet3/0
 ip address 172.16.21.4 255.255.255.0
 no ip directed-broadcast
 ip pim dense-mode
!
```

IP PIM Sparse Mode

Sparse mode was developed to use shared root source tree distribution and relies on the knowledge of an RP. If an RP cannot be found, the router is unable to forward multicast information, strictly because it does not know where the source of the multicast traffic should come from. If it can't determine where the traffic is supposed to be coming from, the Reverse Path Forwarding (RPF) check will fail and no interfaces will be added to the multicast forwarding table.

Configuration of PIM sparse mode is just as simple as it is for IP dense mode. The command for enabling IP PIM sparse mode is `ip pim sparse-mode`. Sparse mode PIM will also activate IGMP on the interface, allowing the interface to listen for IGMP membership reports. Here is an example of enabling IP PIM sparse mode multicast on an interface:

```
RouterA#configure terminal
Enter configuration commands, one per line.  End with
  CNTL/Z.
RouterA(config)#interface FastEthernet3/0
RouterA(config-if)#ip pim sparse-mode
RouterA(config-if)#^Z
RouterA#
```

Here is a look at the interface configuration after the preceding execution:

```
!
interface FastEthernet3/0
 ip address 172.16.21.4 255.255.255.0
 no ip directed-broadcast
 ip pim sparse-mode
!
```

All forms of sparse mode also require a rendezvous point to be configured.

IP PIM Sparse-Dense Mode

The name of this command gives an indication of the functionality it provides. Due to the increasing use of multicast and the variety of applications available today, it is best to configure an interface to be able to use both sparse mode and dense mode. With the previous commands, the interface was assigned the operating mode, and the interface could not change between modes depending on the need at the time.

PIM sparse-dense mode configuration now enables the interface to use whichever forwarding method is needed by the application or multicast group. The interface uses the multicast group notation to decide which mode it needs to operate in. If the interface sees something with the notation (S, G), it will operate in dense mode. If the interface sees notation similar to (*, G), the interface will operate in sparse mode.

An added benefit of implementing sparse-dense mode on the interfaces is the elimination of the need to hard-configure the RP at every leaf router. The Auto-RP information is sent out across the network by using dense mode forwarding.

IP PIM sparse-dense mode is enabled by using `ip pim sparse-dense-mode` on the interface command line. Here is an example:

```
RouterA#configure terminal
Enter configuration commands, one per line.  End with
  CNTL/Z.
RouterA(config)#interface FastEthernet3/0
RouterA(config-if)#ip pim sparse-dense-mode
RouterA(config-if)#^Z
RouterA#
```

Again, here is what the interface looks like after the preceding lines have been entered:

```
!
interface FastEthernet3/0
 ip address 172.16.21.4 255.255.255.0
 no ip directed-broadcast
 ip pim sparse-dense-mode
!
```

In summary, when using the sparse-dense mode configuration on an interface, you need to understand that three criteria will activate the interface and place it into the multicast forwarding table. The first criterion applies to either sparse or dense mode; the others will cause the interface to operate specifically for sparse or dense mode. Table 9.2 provides the details.

TABLE 9.2 Interface Activation Criteria for Sparse-Dense Mode Interfaces

Criteria	Mode of Operation
Directly connected group members or DVMRP neighbors	Sparse and dense
Non-pruned PIM neighbors	Dense
Join request received	Sparse

Configuring a Rendezvous Point

If you are using PIM-DM throughout the multicast network, configuring a rendezvous point is an optional task. There are two ways of configuring a rendezvous point for a router. Notice that we did not say, "configuring a router *to be*" a rendezvous point. You can manually specify the IP address of the RP on a router, or you can enable Auto-RP. Both are described in this section.

Manual RP Configuration

The syntax for the manual RP configuration command is simple: `ip pim rp-address` *`ip_address group_access_list_number`* `[override]`. The *`ip_address`* is the IP address of the router that is the RP. The *`access_list_number`* is for a standard IP access list (1–99) or an expanded range from 1300 to 1999. These lists are used to define which multicast groups can or cannot use this RP. If no access list is specified, all multicast groups will use the configured RP. Finally, the `override` option can be used to override any RP information that might be learned via an Auto-RP update. The static RP takes precedence over any Auto-RP-learned RP. Here is a sample configuration for manual RP configuration:

```
RouterA#configure terminal
Enter configuration commands, one per line.  End with
  CNTL/Z.
```

```
RouterA(config)#ip pim rp-address 172.16.1.253 50 override
RouterA(config)#^Z
RouterA#
```

Here is a look at the router after the execution. Notice that the command is a global command. Following the global configuration, you will see `access-list 50`. The list allows only groups within the range of 224.0.0.0 to 224.255.255.255 to use 172.16.1.253 as the RP. Other groups will need Auto-RP information or another statically configured RP in order to work properly:

```
!
no ip classless
ip route 0.0.0.0 0.0.0.0 172.16.22.2
ip pim rp-address 172.16.1.253 50 override
!
access-list 50 permit 224.0.0.0 0.255.255.255
access-list 50 deny   any
!
```

Auto-RP Configuration

Because multiple RPs can exist in a multicast network, the *Auto-RP* function aids by distributing the RP information across a multicast network. Different multicast groups can use different RPs, so this feature keeps track of which groups are using which RP. It will also fine-tune the leaf router's RP by choosing the RP nearest to the leaf. If you don't like to use static routes in a unicast network, you probably don't want to statically configure multicast RPs either.

There are also two procedures that can be used to enable Auto-RP; which one you use depends on the state of your multicast network. If you are beginning a new deployment, it isn't necessary to create a default RP. If you are modifying an existing multicast network, you will need to designate a default RP router in the network.

Here is a list of configuration tasks that must be completed to successfully implement Auto-RP in a multicast network:

- Designate a default RP (only when modifying an existing multicast network).
- Advertise each RP and the multicast groups associated with the RP.
- Enable an RP Mapping Agent.

As you can see, the list is short and simple. Now that you know what has to be done, let's discuss each step individually.

Designate a Default RP

This step is somewhat tricky, not so much because the configuration is tricky, but because of the decision regarding when to execute the step. The only time you need to designate a default RP is when you are running sparse mode only on any of your interfaces in an existing multicast network. If you are using sparse-dense mode, as suggested, you will not need to execute this step.

This step is executed as described in "Manual RP Configuration" earlier in this chapter. The default RP becomes the statically mapped RP on all the leaf routers. The default RP should serve all global multicast groups. That is all that has to be done.

Advertise RP Group Assignments

From each RP, a statement needs to be added that assigns and advertises multicast groups to that RP. The multicast groups are then advertised so the RP Mapping Agent can keep track of which RP hosts which multicast groups and resolve conflicts when necessary.

The syntax for the command is `ip pim send-rp-announce` *`type number scope ttl group_list access_list_number`*. The command is entered in global configuration mode. The first two options, *`type`* and *`number`*, are the interface type and number that indicate the RP IP address. *`Scope`* defines the boundary of the RP advertisement by using a high TTL value that will be effectively blocked by interfaces with the TTL threshold set. The *`group_list`* uses the specified access list to determine which multicast group ranges the RP is allowed to announce.

Here is an example of the command as well as a valid access list:

```
RouterA#configure terminal
Enter configuration commands, one per line.  End with
  CNTL/Z.
RouterA(config)#access-list 5 permit 224.0.0.0 0.0.255.255
RouterA(config)#ip pim send-rp-announce fastethernet4/0
  scope 230 group-list 5
RouterA(config)#^Z
RouterA#

RouterA#write terminal
. . .
```

```
!
ip pim send-rp-announce FastEthernet4/0 scope 230
  group-list 5
!
access-list 5 permit 224.0.0.0 0.0.255.255
!
. . .
```

Configure the RP Mapping Agent

This router is in charge of learning all the rendezvous point routers in the network along with the multicast group assignments that each RP advertises. The Mapping Agent will then tell all the routers within the multicast network which RP should be used for their source.

This is done with the `ip pim send-rp-discovery scope` *`ttl`* command. As you can see, this command is similar to the command in the preceding section. The scope defines the TTL value for the discovery. After the TTL is reached, the discovery packets are dropped. Here is an example:

```
RouterA#configure terminal
Enter configuration commands, one per line.  End with
  CNTL/Z.
RouterA(config)#ip pim send-rp-discovery scope 23
RouterA(config)#^Z
RouterA#
```

In this example, you can see that the TTL value was set to 23. This means that after 23 hops, the discovery has expired. This command actually assigns to the router the role of RP Mapping Agent.

This concludes the tasks for configuring a rendezvous point in a multicast network. Keep in mind that the RP Mapping Agent can be an RP, although it doesn't have to be. The Mapping Agent's role is to learn of all the deployed rendezvous points throughout the network and then advertise which groups are available via the closest RP for all multicast-enabled routers in the network.

Configuring TTL

Time to Live (TTL) threshold configuration is done to limit the boundary of scope of the IP multicast network. As you learned in Chapter 8, limiting

the scope of a multicast network is based on the TTL value in the multicast packet. Because this command is used to create a boundary, it must be executed on each border interface.

The default value for the TTL threshold is zero. The value can be changed with the `ip multicast ttl-threshold` *`ttl`* command. The syntax is straightforward, and the *`ttl`* value that is used is up to the discretion of the network administrator. The range of valid values for this option is between 0 and 255. However, the value should be high enough to stop multicast packets from exiting the interface. Here is an example:

```
RouterA#configure terminal
Enter configuration commands, one per line.  End with
  CNTL/Z.
RouterA(config)#interface FastEthernet0/0
RouterA(config-if)#ip multicast ttl-threshold 230
RouterA(config-if)#^Z
RouterA#

!
interface FastEthernet0/0
 ip address 172.16.5.1 255.255.255.0
 no ip directed-broadcast
 ip pim sparse-dense-mode
 ip multicast ttl-threshold 230
 no ip route-cache
 no ip mroute-cache
 full-duplex
!
```

Joining a Multicast Group

After the main configuration is done on the router to enable multicast, PIM, rendezvous points, and RP Mapping Agents, the only other major task is enabling hosts to join multicast groups.

Within Cisco IOS, the network administrator has the opportunity to verify functionality and connectivity before users use the multicast system and applications. You can configure a router to join any number of IP multicast groups and, thus, verify functionality.

This is achieved through the `ip igmp join-group` *`group_address`* command. The *`group_address`* is the multicast address of the group you want the router to join. An example follows:

```
RouterA(config)#interface FastEthernet4/0
RouterA(config-if)#ip igmp join-group 224.2.127.254
RouterA(config-if)#^Z
RouterA#
```

This tells the router to become a member of the 224.2.127.254 multicast group. Joining a group facilitates troubleshooting multicast connectivity issues as well.

Troubleshooting IP Multicast Connectivity

Multicast can be a difficult protocol to troubleshoot. However, a few basic tools (mostly `show` commands) can provide enough information for you to verify that connectivity is active or to determine whether other steps, such as debugging, are needed to troubleshoot the problem.

If you do need to debug a multicast-enabled interface, you must first disable the multicast fast switching on the interface. This is done so that the debug messages can be logged. The command to disable fast switching is `no ip mroute-cache`. The standard unicast fast (or other forms of) switching can be left enabled.

You are familiar with the troubleshooting tools for unicast connectivity, Ping and traceroute. Well, these tools are also available for troubleshooting multicast connectivity. There is one minor difference, though: multicast requires a special version of traceroute—called mtrace, or "multicast-traceroute."

Ping

After a device on the network becomes a member of a group, it can be identified by its layer 3 multicast address as well as the layer 2 MAC address. Because the device has an active address on its interface, it can respond to ICMP request packets. Here is an example:

```
RouterA#ping
Protocol [ip]:
Target IP address: 224.2.143.55
Repeat count [1]: 5
Datagram size [100]:
```

```
Timeout in seconds [2]:
Extended commands [n]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 224.2.143.55, timeout is
  2 seconds:
.!!!!
RouterA#
```

This tool can be used to verify connectivity among RPs or other multicast routers.

mtrace

Cisco also provides a multicast traceroute tool. The multicast version of traceroute is somewhat different from the unicast version. The complete syntax for *mtrace* is `mtrace` *`source_ip destination_ip group`*. The *`source_ip`* is the unicast IP address for the source of the multicast group. The *`destination_ip`* is used when following the forwarding path established by the source or shared tree distribution toward a unicast destination. The *`group`* option is used to establish the tree for the specified group. If no destination or group options are specified, the mtrace will work from the incoming multicast interfaces back toward the multicast source. Here are a few samples of the command and its output:

```
RouterB#mtrace 198.32.163.74
Type escape sequence to abort.
Mtrace from 198.32.163.74 to 172.16.25.9 via RPF
From source (blaster.oregon-gigapop.net) to destination
  (?)
Querying full reverse path...
 0  172.16.25.9
-1  172.16.25.9 PIM/MBGP  [198.32.163.0/24]
-2  172.16.25.10 PIM/MBGP  [198.32.163.0/24]
-3  ogig-den.oregon-gigapop.net (198.32.163.13) [AS 4600]
  PIM  [198.32.163.64/26]
-4  0car-0gw.oregon-gigapop.net (198.32.163.26) [AS 4600]
  PIM  [198.32.163.64/26]
-5  blaster.oregon-gigapop.net (198.32.163.74)
RouterB#
```

```
RouterB#mtrace 198.32.163.74 224.2.243.55
Type escape sequence to abort.
Mtrace from 198.32.163.74 to 172.16.25.9 via group
  224.2.243.55
From source (blaster.oregon-gigapop.net) to destination
  (?)
Querying full reverse path...
 0  172.16.25.9
-1  172.16.25.9 PIM/MBGP Reached RP/Core [198.32.163.0/24]
-2  172.16.25.10 PIM/MBGP Reached RP/Core [198.32.163.0/24]
-3  ogig-den.oregon-gigapop.net (198.32.163.13) [AS 4600]
  PIM Reached RP/Core [198.32.163.64/26]
-4  Ocar-Ogw.oregon-gigapop.net (198.32.163.26) [AS 4600]
  PIM  [198.32.163.64/26]
RouterB#
```

As you can see, the outputs differ very little, but it is important to see how the paths are established. From the first sample output, no group or destination was specified, so the router strictly used RPF to calculate the path from the source to the router. In the other output, a group address was specified. This caused the router to specifically use the existing forwarding tree for group 224.2.243.55 to get back to the router.

These tools can be useful to determine connectivity as well as effectiveness of placement of RPs and multicast sources. There are other `show` commands that can aid you as well, but they are not related to the topic of this chapter.

Changing the IGMP Version

Several settings can be tweaked in the router to enhance or change performance. The majority of them are beyond the scope of this chapter. However, in this section, we will discuss one important feature: changing the IGMP version. It is important that you understand and know how to perform this change because of the compatibility issues between IGMP versions, as discussed in Chapter 8.

To put it simply, the IGMP version that runs on the hosts must also run on the router. Cisco routers use IGMPv2 by default and do not auto-detect the IGMP version that the host is using. The command to change from IGMPv2 to IGMPv1, or vice versa, is `ip igmp version (2 | 1)`. Because the

IGMP version needs to match only on the subnet, the command must be entered on the interface that connects to the subnet housing the IGMPv1 hosts. The other interfaces on the router can remain on IGMPv2.

Enabling CGMP and IGMP Snooping

When hosts connect to a router via a Catalyst switch, either CGMP or *IGMP Snooping* can be used to enable the switch to learn appropriate information. As we discussed in Chapter 8, Catalysts run both so they can manage multicast membership reports from the router accordingly and so they can manage multicast ports on the switch. The router is the device that listens for the IGMP membership report; it then tells the switch which port needs to be activated. CGMP or IGMP Snooping must be activated on both the router and the switch.

CGMP Router Configuration

The router configuration syntax is simple. It must be applied to the interface connected to the Catalyst switch. The command is `ip cgmp` *`proxy`*. The *`proxy`* option is used for routers that are not CGMP capable. It enables them to use the proxy router for CGMP. Here is a sample configuration:

```
RouterA#configure terminal
Enter configuration commands, one per line.  End with
  CNTL/Z.
RouterA(config)#interface FastEthernet4/0
RouterA(config-if)#ip cgmp
RouterA(config-if)#^Z
RouterA#
```

Use the command `show running-config` to see whether CGMP is enabled or disabled on a particular router interface, as shown here:

```
!
interface FastEthernet4/0
 ip address 172.16.10.1 255.255.255.0
 no ip directed-broadcast
 ip pim sparse-dense-mode
 no ip route-cache
 ip igmp join-group 224.2.127.254
 ip cgmp
!
```

Catalyst Switch Configuration

The Catalyst syntax is just as simple, if not more so, as the syntax for the router configuration. By default, CGMP is turned off on the switch. If you want multicast to work properly, you must enable CGMP or IGMP Snooping on the switch. Enabling CGMP is done by using the syntax `set cgmp enable`. Here is a sample:

```
switch1> (enable) set cgmp enable
CGMP support for IP multicast enabled.
switch1> (enable)
switch1> (enable) show cgmp statistics
CGMP enabled

CGMP statistics for vlan 1:
valid rx pkts received          6
invalid rx pkts received        0
valid cgmp joins received       6
valid cgmp leaves received      0
valid igmp leaves received      0
valid igmp queries received     0
igmp gs queries transmitted     0
igmp leaves transmitted         0
failures to add GDA to EARL     0
topology notifications received 0
number of packets dropped       0
switch1> (enable)
```

After CGMP is enabled, you can look at statistics by using the `show cgmp statistics` command. This is all that is needed to enable CGMP on the switch so that it can communicate with the router.

A CGMP-enabled switch can also be configured to detect IGMPv2 leave messages generated by clients. To do this, simply use the command `set cgmp leave enable`. This command takes place globally on the switch.

The switch will collect multicast group MAC addresses for each group address. To see what multicast groups your switch knows about, use the command `show multicast group cgmp`.

IGMP Snooping

IGMP Snooping can be configured to enable the switch to learn multicast information by examining the frames as they pass through the switch. The

switch doesn't depend wholly on information received from the multicast router.

To configure IGMP Snooping on the switch, use the command `set igmp enable`. You cannot have CGMP and IGMP Snooping enabled on the same switch at the same time. To enable IGMP Snooping on the router, use the command `ip igmp snooping` while in global configuration mode.

Fast Leave processing is a new feature that works only with IGMP Snooping and is one of the main reasons for its use. Fast Leave processing enables a switch to receive an IGMP leave message and immediately remove the interface from the table that lists which ports receive the multicast stream. Thus, if a client on port 2/5 generates a leave message, the switch will immediately remove port 2/5 from the list of ports receiving the multicast stream. To enable Fast Leave processing on the switch, use the command `set igmp fastleave enable`.

Real World Scenario

The Fast Leave Trap

Fast Leave is a great tool in an organization that uses quite a bit of multicasting. There can be a problem though, when using it in a network where Spanning Tree changes frequently.

When a switch configured for Fast Leave receives a leave message, the switch will remove the port at which the message arrived from the forwarding table for the particular stream. What happens if this occurs on a core switch, on the port going out to a closet switch or stack? The core switch will remove all entries associated with that port. If several clients were listening to the stream and one leaves, the core switch will remove them all.

Whenever possible, only enable fast leave processing on switches that have clients terminating at individual ports. Turn this feature on at the closets but think twice before doing so at core and distribution layer switches.

Just as with CGMP, IGMP Snooping has a way of displaying the configuration and statistics. Using the command `show igmp statistics` will display the status of IGMP Snooping on the switch as well as the amount of traffic that has been processed.

Summary

This chapter has been dedicated to the syntax and method of IP multicast configuration in Cisco routers and switches. Several points were discussed about the importance of planning the IP multicast deployment.

In addition to learning the commands for rendezvous points and hosts, you learned a few troubleshooting commands that will aid you in verifying that the multicast network has full functionality.

Exam Essentials

Know how to enable IGMP Snooping. IGMP Snooping is one of the ways that a switch can learn multicast client information. Snooping can't be enabled if CGMP is enabled, so you first need to make sure that CGMP is turned off. Next, enable IGMP Snooping with the `ip igmp snooping` command.

Know how to enable the switch to listen to multicast leave messages. The Catalyst switch can listen for client leave messages with both CGMP and IGMP Snooping. A switch configured for CGMP can listen for IGMPv2 leave messages by being configured with the command `set cgmp leave enable`. A switch configured for IGMP Snooping can be configured for IGMP Fast Leave processing with the command `set igmp fastleave enable`.

Know the difference between sparse mode and dense mode. Because sparse mode assumes that clients do not want to receive streams until they ask for them, a special router is used as the base for the entire tree. This router, a rendezvous point, needs to be referenced in each multicast router's configuration. Use the command `rp pim ip-address` *`ip_address`* to define the IP address of the rendezvous point.

Know how to troubleshoot your multicast setup. By now, you should be comfortable with the `show` commands that can be done on the router and switch to show communication but how do you test transport? You can use the `ping` command to reach out and touch a particular multicast IP address. If you want to do a traceroute, then use the command `mtrace`.

Key Terms

Before you take the exam, be sure you're familiar with the following terms:

Auto-RP	PIM sparse-dense mode
IGMP Snooping	Protocol Independent Multicast (PIM)
mtrace	rendezvous points (RPs)

Written Lab

Write the answers to the following questions:

1. Write the command that enables multicast routing on a router.
2. Write the commands that will enable PIM SM on interface FastEthernet 4/0.
3. Write the configuration commands that will enable PIM DM on interface FastEthernet 3/0.
4. Write the configuration for enabling PIM sparse-dense mode on interface FastEthernet 0/0.
5. Write the command that will show you the multicast route table.
6. Manually configure a router to be an RP by using the IP address of 172.16.25.3 and apply access list number 30.
7. Write the command that is used when implementing Auto-RP so that the RP will announce only specific multicast groups. Use access list number 10 and interface FastEthernet 4/0. Use a TTL value of 220.
8. Write the command that enables an RP Mapping Agent. Use a TTL value of 32.

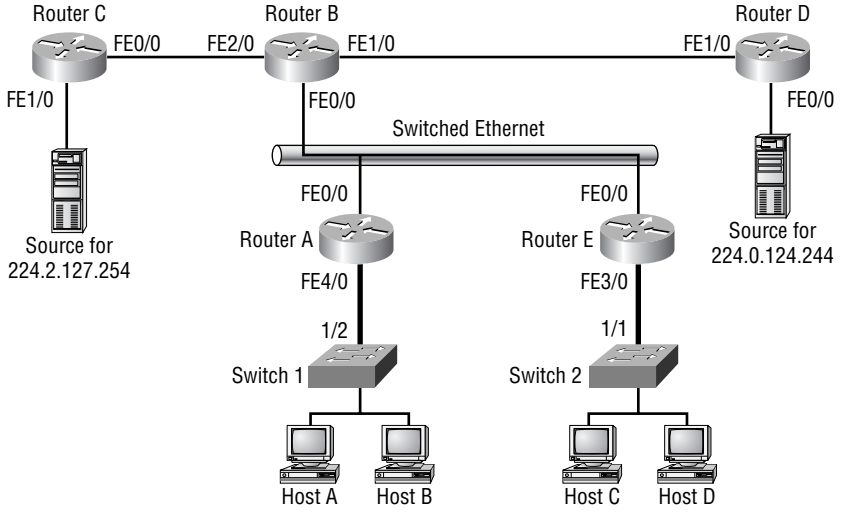
9. Apply a command that sets a TTL threshold of 235 on interface FastEthernet 2/0.

10. Write the commands that will enable CGMP on a router for interface FastEthernet 3/0, and then write the command that will enable CGMP on a switch.

Hands-On Lab

Refer to Figure 9.1 as the diagram for this lab. The objective of this lab is to configure an IP multicast network from scratch. You will implement Auto-RP, PIM sparse-dense mode, and CGMP on all routers and switches. You will not have to configure host applications in this lab. Assume that Routers C and D have multicast sources attached to them.

FIGURE 9.1 Configuring an IP multicast network



1. Because you are starting from scratch, the first step is to enable multicast on all routers:

```
RouterA#configure terminal
Enter configuration commands, one per line.  End with
  CNTL/Z.
```

```
RouterA(config)#ip multicast-routing
RouterA(config)#^Z
RouterA#

RouterB#configure terminal
Enter configuration commands, one per line.  End with
  CNTL/Z.
RouterB(config)#ip multicast-routing
RouterB(config)#^Z
RouterB#

RouterC#configure terminal
Enter configuration commands, one per line.  End with
  CNTL/Z.
RouterC(config)#ip multicast-routing
RouterC(config)#^Z
RouterC#

RouterD#configure terminal
Enter configuration commands, one per line.  End with
  CNTL/Z.
RouterD(config)#ip multicast-routing
RouterD(config)#^Z
RouterD#

RouterE#configure terminal
Enter configuration commands, one per line.  End with
  CNTL/Z.
RouterE(config)#ip multicast-routing
RouterE(config)#^Z
RouterE#
```

2. Now, enable PIM sparse-dense mode on all shown connected interfaces:

```
RouterA#configure terminal
Enter configuration commands, one per line.  End with
  CNTL/Z.
```

```
RouterA(config)#interface FastEthernet4/0
RouterA(config-if)#ip pim sparse-dense-mode
RouterA(config-if)#interface fastethernet0/0
RouterA(config-if)#ip pim sparse-dense-mode
RouterA(config-if)#^Z
RouterA#

RouterE#configure terminal
Enter configuration commands, one per line.  End with
  CNTL/Z.
RouterE(config)#interface fastethernet3/0
RouterE(config-if)#ip pim sparse-dense-mode
RouterE(config-if)#interface fastethernet0/0
RouterE(config-if)#ip pim sparse-dense-mode
RouterE(config-if)#^Z
RouterE#

RouterB#configure terminal
Enter configuration commands, one per line.  End with
  CNTL/Z.
RouterB(config)#interface fastethernet0/0
RouterB(config-if)#ip pim sparse-dense-mode
RouterB(config-if)#interface fastethernet1/0
RouterB(config-if)#ip pim sparse-dense-mode
RouterB(config-if)#interface fastethernet2/0
RouterB(config-if)#ip pim sparse-dense-mode
RouterB(config-if)#^Z
RouterB#

RouterC#configure terminal
Enter configuration commands, one per line.  End with
  CNTL/Z.
RouterC(config)#interface fastethernet0/0
RouterC(config-if)#ip pim sparse-dense-mode
RouterC(config-if)#interface fastethernet1/0
RouterC(config-if)#ip pim sparse-dense-mode
RouterC(config-if)#^Z
RouterC#
```

```
RouterD#configure terminal
Enter configuration commands, one per line.  End with
  CNTL/Z.
RouterD(config)#interface fastethernet0/0
RouterD(config-if)#ip pim sparse-dense-mode
RouterD(config-if)#interface fastethernet1/0
RouterD(config-if)#ip pim sparse-dense-mode
RouterD(config-if)#^Z
RouterD#
```

3. Enable CGMP on all router interfaces and switches (some many not be shown):

```
RouterA#configure terminal
Enter configuration commands, one per line.  End with
  CNTL/Z.
RouterA(config)#interface fastethernet0/0
RouterA(config-if)#ip cgmp
RouterA(config-if)#interface fastethernet4/0
RouterA(config-if)#ip cgmp
RouterA(config-if)#^Z
RouterA#

RouterE#configure terminal
Enter configuration commands, one per line.  End with
  CNTL/Z.
RouterE(config)#interface fastethernet0/0
RouterE(config-if)#ip cgmp
RouterE(config-if)#interface fastethernet3/0
RouterE(config-if)#ip cgmp
RouterE(config-if)#^Z
RouterE#

RouterB#configure terminal
Enter configuration commands, one per line.  End with
  CNTL/Z.
RouterB(config)#interface fastethernet0/0
RouterB(config-if)#ip cgmp
RouterB(config-if)#interface fastethernet1/0
RouterB(config-if)#ip cgmp
```

```
RouterB(config-if)#interface fastethernet2/0
RouterB(config-if)#ip cgmp
RouterB(config-if)#^Z
RouterB#

RouterC#configure terminal
Enter configuration commands, one per line.  End with
  CNTL/Z.
RouterC(config)#interface fastethernet0/0
RouterC(config-if)#ip cgmp
RouterC(config-if)#interface fastethernet1/0
RouterC(config-if)#ip cgmp
RouterC(config-if)#^Z
RouterC#

RouterD#configure terminal
Enter configuration commands, one per line.  End with
  CNTL/Z.
RouterD(config)#interface fastethernet0/0
RouterD(config-if)#ip cgmp
RouterD(config-if)#interface fastethernet1/0
RouterD(config-if)#ip cgmp
RouterD(config-if)#^Z
RouterD#

switch1> (enable) set cgmp enable
CGMP support for IP multicast enabled.
switch1> (enable)
switch2> (enable) set cgmp enable
CGMP support for IP multicast enabled.
```

4. Assign multicast group 224.2.127.254 to Router C via access list 5. This assignment will allow only Router C to advertise that group. Assign a TTL value of 12. Then assign group 224.0.124.244 to Router D via access list 6:

```
RouterC#configure terminal
Enter configuration commands, one per line.  End with
  CNTL/Z.
```

```
RouterC(config)#access-list 5 permit 224.2.127.254
  0.0.0.0
RouterC(config)#ip pim send-rp-announce fastethernet1/0
  scope 12 group-list 5
RouterC(config)#^Z
RouterC#

RouterD#configure terminal
Enter configuration commands, one per line.  End with
  CNTL/Z.
RouterD(config)#access-list 6 permit 224.0.124.244
  0.0.0.0
RouterD(config)#ip pim send-rp-announce fastethernet1/0
  scope 12 group-list 6
RouterD(config)#^Z
RouterD#
```

5. Now configure Router B to be the RP Mapping Agent; use a scope of 12:

```
RouterB#configure terminal
Enter configuration commands, one per line.  End with
  CNTL/Z.
RouterB(config)#ip pim send-rp-discovery scope 12
RouterB(config)#^Z
RouterB#
```

Review Questions

1. Which of the following commands are necessary in order for multicast to work? (Choose all that apply.)

   A. `ip mroute cache`

   B. `ip pim [sparse-mode | dense-mode | sparse-dense-mode]`

   C. `ip cgmp`

   D. `ip multicast-routing`

2. What are the valid ranges for access lists when an RP address is manually configured? (Choose all that apply.)

   A. 1–100

   B. 1–99

   C. 100–199

   D. 800–899

   E. 1300–1999

3. What three configuration tasks are necessary to enable multicast Auto-RP? (Choose all that apply.)

   A. Perform IP multicast routing

   B. Assign the default RP (for existing multicast networks)

   C. Assign the RP Mapping Agent

   D. Advertise RP/group associations

4. What do the options *`type`* and *`number`* mean in the command `ip pim send-rp-announce` *`type number`* `scope` *`ttl`* `group-list` *`access-list-number`*? (Choose all that apply.)

   A. PIM mode

   B. IGMP

   C. RP unicast IP address

   D. Interface

   E. Interface number

5. What does the following command accomplish?

```
RouterA#configure terminal
Enter configuration commands, one per line.  End with
  CNTL/Z.
RouterA(config)#ip multicast-routing
RouterA(config)#^Z
RouterA#
```

   A. It enables the multicast forwarding process on the router.

   B. It allows IP multicast routing protocols to be configured on the router.

   C. It defines the RP for the network.

   D. It is a multicast route source tree.

6. Which of the following multicast route notations indicate dense mode?

   A. (*, G)

   B. (G, *)

   C. (S, G)

   D. (G, S)

7. Which of the following multicast route notations indicates the operation of sparse mode?

   A. (*, G)

   B. (G, *)

   C. (S, G)

   D. (G, S)

8. What are the primary functions of RP Mapping Agents? (Choose all that apply.)

   A. Mapping unicast addresses of all RP routers in a multicast network

   B. Sourcing multicast traffic

   C. Resolving multicast group/RP conflicts

   D. Providing member topologies to the RP routers in the network

9. Which of the following is a method of limiting the scope of a multicast network?

   A. Passive interface applied to border interfaces

   B. Distribution lists within an IGP such as EIGRP or OSPF

   C. TTL threshold setting on border interfaces

   D. RPF settings within the RP routers

10. Which of the following are valid reasons for configuring a router to be a member?

    A. To allow multicast forwarding

    B. To allow the RP to be a source for the specified group

    C. To allow source root tree forwarding

    D. To allow troubleshooting and verification of multicast functionality

11. Which are tools that can be used to troubleshoot multicast connectivity? (Choose all that apply.)

    A. Ping

    B. `show ip mroute`

    C. traceroute

    D. mtrace

12. What are two methods mtrace utilizes to establish the path between the source and router? (Choose all that apply.)

    A. SRT

    B. RPF

    C. Multicast group

    D. PIM

13. From which direction is the mtrace established?
    A. From the default RP of the multicast network to the source
    B. From the source to the RP
    C. From the source to the router interface
    D. From the router interface to the source

14. Where is it necessary to run IGMPv1?
    A. Entire multicast network
    B. All members of a group whose source is IGMPv1
    C. All interfaces on the router
    D. The interface or subnet whose hosts use IGMPv1

15. Which device answers IGMP requests? (Choose all that apply.)
    A. Hub
    B. ATM switch
    C. Switch
    D. Router

16. What command is used to manually configure a router to be an RP?
    A. `ip multicast RP` *`ip_address`*
    B. `ip pim RP` *`ip_address`*
    C. `ip pim rp-address` *`ip_address`*
    D. `ip igmp rp-address` *`ip_address`*

17. Which of the following criteria will activate an interface that is configured to use dense mode? (Choose all that apply.)
    A. Directly connected hosts
    B. Directly connected PIM routers
    C. Router configured as a border router
    D. When the interface receives a prune statement from a directly connected PIM router

18. Which of the following criteria will activate an interface in sparse mode? (Choose all that apply.)

    A. A sparse mode interface is always active.

    B. A directly connected DVMRP neighbor.

    C. An explicit join request on that interface.

    D. A prune request is received on the interface.

19. Which criteria will activate an interface in sparse mode when the interface is configured to use sparse-dense mode? (Choose all that apply.)

    A. Directly connected DVMRP neighbor.

    B. Explicit join request.

    C. Any PIM-configured interface is made active.

    D. The interface has directly connected hosts.

20. Which of the following will activate an interface in dense mode if it is configured for sparse-dense mode operation? (Choose all that apply.)

    A. Non-pruned PIM interface

    B. Directly connected hosts

    C. DVMRP neighbor on that interface

    D. An explicit join request

Answers to Written Lab

1. ip multicast-routing
2. configure terminal
   interface fastethernet4/0
   ip pim sparse-mode
3. configure terminal
   interface fastethernet3/0
   ip pim dense-mode
4. configure terminal
   interface fastethernet0/0
   ip pim sparse-dense-mode
5. show ip mroute
6. ip pim rp-address 172.16.25.3 30
7. ip pim send-rp-announce fastethernet 4/0 scope 220
   group-list 10
8. ip pim send-rp-discovery scope 32
9. configure terminal
   interface fastethernet2/0
   ip multicast ttl-threshold 235
10. configure terminal
    interface fastethernet3/0
    ip cgmp

    set cgmp enable

Answers to Review Questions

1. B, D. These two commands must be entered for multicast forwarding to work. The `ip mroute cache` command enhances performance but is not necessary. CGMP is necessary only when hosts are connected to a router via a Catalyst switch using CGMP.
2. B, E. 1–100 is an invalid range; the range has to be 1–99. 100–199 is used for extended access lists, and 800–899 is used for IPX. 1300–1999 is the range for expanded standard access lists.
3. B, C, D. IP multicast routing is not part of the Auto-RP configuration.
4. D, E. *Type* means interface type, and *number* means the interface number.
5. A. The command enables the multicast process on the router, thereby permitting multicast packets to be forwarded.
6. C. (S, G) and (*, G) are the only valid notations. (S, G) indicates a source root tree distribution. Dense mode uses source root trees.
7. A. (S, G) and (*, G) are the only valid notations. (*, G) indicates a shared root tree distribution. Sparse mode uses shared root trees.
8. A, C. RP Mapping Agents keep track of all RP routers in the network via their unicast addresses. They then provide the nearest RP for the multicast groups it sources to all leaf routers in the multicast network.
9. C. The correct way to limit the scope of the multicast network is to configure TTL thresholds for external or border interfaces. RPF is used strictly for reverse path lookup.
10. D. By subscribing to a multicast group, the router can execute certain commands to troubleshoot and verify multicast connectivity.
11. A, B, D. Traceroute is used for unicast connectivity; mtrace, however, is used for multicast connectivity.
12. B, C. As shown in the examples in Chapter 9, the traceroute path can be established via RPF information or via multicast group forwarding information.
13. C. From the examples given in Chapter 9, you can see that the path is established from the source toward the multicast router interface.

14. D. The only interfaces that need to be made compatible with IGMPv1 are the interfaces with hosts that are directly connected and use IGMPv1.

15. C, D. Routers and switches are the devices that respond to IGMP membership records. Switches process CGMP from the routers unless they are using IGMP Snooping when they can respond directly. Hubs have no intelligence whatsoever.

16. C. The correct syntax is provided by the third answer. The other answers are not valid.

17. A, B. Hosts activate the interface through membership reports. PIM interfaces automatically receive multicast forwarding until a prune request is received.

18. B, C. For a sparse mode interface to be active, there must be either a directly connected host, or a DVMRP neighbor or a join request must be made. Sparse mode interfaces are inactive otherwise.

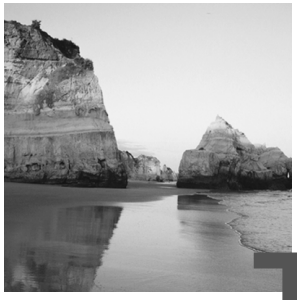
19. A, B, D. A PIM-configured interface is considered active only when in dense mode.

20. A, B, C. Join requests are used only in sparse mode operation.

Appendix

A

Commands Used in This Book



This appendix provides all the different commands used in this book and their meanings. Use this to help you study and as a desk reference.

The following list includes the access layer commands used in this book. These are the commands we used for the 1900 switches in this book.

Command	Meaning	Chapter
Ctrl+Shift+6, then X	Used as an escape sequence	Chapter 2
`duplex`	Sets the duplex of an interface, with half- or full-duplex	Chapter 2
`enable password level`	Sets the usermode (level 1) and the enable password (level 15) of the switch	Chapter 2
`hostname`	Assigns a name to the Catalyst 1900 or 2800 series switch	Chapter 2
`interface`	Used to select an interface	Chapter 3
`interface ethernet` *`module/port`*	Used to identify or set parameters on an interface on the 1900 or 2820 switch	Chapter 2
`interface fastethernet` *`module/port`*	Displays or changes parameters on the two available FastEthernet interfaces	Chapter 2
`ip address`	Assigns an IP address to the 1900 or 2820 switch	Chapter 2
`no spantree`	Turns off spanning tree for a VLAN	Chapter 4
`no trunk-vlan`	Removes VLANs from a trunked link	Chapter 3

Command	Meaning	Chapter
`port-channel mode`	Enables an EtherChannel bundle	Chapter 5
`show run`	Displays the running-config of the 1900 and 2820 switch	Chapter 2
`show spantree`	Used to view spanning tree information on a VLAN	Chapters 4, 5
`show uplink-fast`	Shows the UplinkFast parameters	Chapter 5
`show uplink-fast statistics`	Shows the UplinkFast statistics	Chapter 5
`show vtp`	Shows the switches' VTP configuration	Chapter 3
`shutdown`	Disables a particular interface	Chapter 2
`spantree`	Turns on spanning tree for a VLAN	Chapter 4
`spantree cost`	Configures a cost for an interface	Chapter 5
`spantree priority`	Configures the priority for an interface	Chapter 5
`spantree start-forwarding`	Enables PortFast on an interface	Chapter 5
`trunk`	Turns trunking on or off of interface fa0/26 and fa0/27	Chapter 3
`uplink-fast`	Turns on UplinkFast for the switch	Chapter 5
`vlan`	Sets VLAN information	Chapter 3
`vlan-membership`	Sets an interface to a VLAN	Chapter 3
`vtp mode`	Changes the VTP mode to server, transparent, or client	Chapter 3
`vtp name`	Configures the VTP domain name	Chapter 3
`vtp password`	Sets an optional VTP password	Chapter 3

The following list includes commands used for configuring the distribution layer switch. These commands were used on the 5000 series switch in this book.

Command	Meaning	Chapter
`clear mls entry destination` *`ip_addr_spec source ip_addr_spec flow protocol src_port dst_port`* `[all]`	Allows all MLS entries to be cleared in addition to allowing specific entries to be terminated.	Chapter 7
`clear trunk`	Clears VLANs from a trunked port.	Chapter 3
Ctrl+C	Used as a break sequence.	Chapter 2
Ctrl+Shift+6, then X	Used as an escape sequence.	Chapter 2
`show spantree uplinkfast`	Shows the UplinkFast parameters and statistics.	Chapter 5
`interface vlan #`	Enables interface configuration mode for the specified VLAN interface.	Chapter 6
`ip cgmp` *`proxy`*	Enables CGMP on the specified interface on routers.	Chapter 9
`ip igmp join-group` *`group_address`*	Makes the router become an active member of the specified multicast group.	Chapter 9
`ip igmp version (2|1)`	Applied to the interface and used to change the version of IGMP used on that interface.	Chapter 9
`ip multicast ttl-threshold` *`ttl`*	Applied to all border interfaces to enforce the scope or boundary of the IP multicast network.	Chapter 9
`ip multicast-routing`	Enables IP multicast forwarding on the router.	Chapter 9
`ip pim dense-mode`	Enables PIM dense mode operation on the interface.	Chapter 9
`ip pim rp-address` *`ip_address group_access_list_number`* `[override]`	Manually configures an RP address on a multicast router.	Chapter 9

Command	Meaning	Chapter
`ip pim send-rp-announce` *`type number scope ttl group_list access_list_number`*	Assigns specific multicast group addresses to an RP. The RP can then only announce that it knows multicast groups permitted by the access list specified.	Chapter 9
`ip pim send-rp-discovery scope` *`ttl`*	Configures RP Mapping Agent and allows the router to discover all RPs and group assignments.	Chapter 9
`ip pim sparse-dense-mode`	Enables PIM sparse-dense mode operation on the interface.	Chapter 9
`ip pim sparse-mode`	Enables PIM sparse mode operation on the interface.	Chapter 9
`mac-address`	Sets a specific MAC address on an interface.	Chapter 6
`mls rp ip`	Enables MLS on an external router, both global and interface specific.	Chapter 7
`mls rp management-interface`	Assigns the interface to the MLS-RP. This allows MLSP updates to use this interface.	Chapter 7
`mls rp vlan-id` *`vlan_id_number`*	Assigns the interface the proper VLAN number.	Chapter 7
`mls rp vtp-domain` *`domain_name`*	Assigns the interface to the VTP domain.	Chapter 7
`mtrace`	Displays the forwarding path based on group membership or the RPF.	Chapter 9
`ping`	Used for testing reachability.	Chapter 9
`session`	Connects the CLI to a session on a route processor module.	Chapter 6
`set cgmp enable`	Used on Catalyst switches to enable CGMP.	Chapter 9
`set enablepass`	Configures the enable password on a set-based device.	Chapter 2
`set interface sco`	Assigns an IP address to the management interface of the set-based switch.	Chapter 2

Command	Meaning	Chapter
`set ip route`	Configures a default route on a set-based switch.	Chapter 6
`set mls agingtime` *`agingtime`*	Sets the MLS aging time value to the specified value.	Chapter 7
`set mls agingtime fast` *`fastagingtime pkt_threshold`*	Allows the fast aging time and packet threshold to be set.	Chapter 7
`set mls enable`	Enables MLS on Catalyst switches. For most switches, this is set to on by default.	Chapter 7
`set password`	Configures the usermode password on a set-based device.	Chapter 2
`set port channel`	Creates an EtherChannel bundle.	Chapter 5
`set port duplex`	Sets the duplex of a port.	Chapter 2
`set port speed`	Sets the speed of a port.	Chapter 2
`set system name`	Assigns a name to the Catalyst switch.	Chapter 2
`set spantree`	Turns spanning tree off or on for a VLAN.	Chapter 4
`set spantree backbonefast`	Enables BackboneFast for a switch.	Chapter 5
`set spantree fwddelay`	Changes the forward delay time on a switch.	Chapter 5
`set spantree hello`	Changes the BPDU hello time on a switch.	Chapter 5
`set spantree maxage`	Sets how long a BPDU that is received will stay valid until another BPDU is received.	Chapter 5
`set spantree portcost`	Sets the STP port cost.	Chapter 5
`set spantree portfast`	Enables PortFast on a port.	Chapter 5

Command	Meaning	Chapter
`set spantree portpri`	Sets the STP port priority.	Chapter 5
`set spantree portvlanpri`	Configures links to forward only certain VLANs.	Chapter 5
`set spantree root`	Makes a set-based switch a root bridge.	Chapter 5
`set spantree uplinkfast`	Enables UplinkFast on a port.	Chapter 5
`set trunk`	Configures trunking on a port.	Chapter 3
`set vlan`	Creates a VLAN and also assigns a port to a VLAN.	Chapter 3
`set vtp domain`	Sets the VTP domain name.	Chapter 3
`set vtp mode`	Sets the VTP mode of the switch.	Chapter 3
`set vtp passwd`	Sets the optional VTP password.	Chapter 3
`show port capabilities` *`slot/port`*	Shows the configuration of individual ports.	Chapter 5
`show config`	Shows the configuration of the 5000 series switch.	Chapters 2, 6
`show mls`	Shows MLS information on a switch.	Chapter 7
`show mls entry`	Provides MLS entry data on the MLS-SE.	Chapter 7
`show mls rp`	Provides global MLS information.	Chapter 7
`show mls rp interface` *`interface`*	Provides interface-specific MLS information.	Chapter 7
`show mls rp vtp-domain` *`domain_name`*	Provides MLS information for the VTP domain.	Chapter 7
`show module`	Shows the module and numbers of cards in the switch.	Chapter 6

Command	Meaning	Chapter
`show port channel`	Shows the status of an EtherChannel bundle.	Chapter 5
`show spantree`	Shows the state of the STP per VLAN.	Chapters 4, 5
`show vlan`	Shows the configured VLANs.	Chapter 3
`show vtp domain`	Shows the VTP domain configurations.	Chapter 3
`show vtp domain`	Provides VTP domain information on the switch.	Chapter 7

Appendix

B

Internet Multicast Addresses

Certain Class D IP networks in the range of 224.0.0.0 through 239.255.255.255 are used for host extensions for IP multicasting as specified in the Request for Comments (RFC) 1112 standard created by the Internet Engineering Task Force (IETF). The well-known addresses are assigned and maintained by the Internet Address Number Authority (IANA). RFC 1112 specifies the extensions required of a host implementation of the Internet Protocol (IP) to support multicasting.

A lot of abbreviations and acronyms are used in this appendix. The most important, found in the well-known addresses, are listed here:

DVMRP Distance Vector Multicast Routing Protocol

DHCP Dynamic Host Configuration Protocol

OSPF Open Shortest Path First

RIP Routing Information Protocol

RP Route processor

PIM Protocol Independent Multicast

This appendix will describe the multicast addresses, the purpose of each address, and the RFC or contact acronym.

These addresses are subject to change. If you cannot find an address listed here that appears to be assigned, refer to the following location: `www.iana.org/assignments/multicast-addresses`.

TABLE B.1 Multicast Addresses

Address	Purpose	Reference/Contact Acronym
224.0.0.0	Base Address (Reserved)	RFC1112/JBP
224.0.0.1	All Systems on this Subnet	RFC1112/JBP
224.0.0.2	All Routers on this Subnet	JBP
224.0.0.3	Unassigned	JBP
224.0.0.4	DVMRP Routers	RFC1075/JBP
224.0.0.5	OSPFIGP All Routers	RFC2328/JXM1
224.0.0.6	OSPFIGP Designated Routers	RFC2328/JXM1
224.0.0.7	ST Routers	RFC1190/KS14
224.0.0.8	ST Hosts	RFC1190/KS14
224.0.0.9	RIP2 Routers	RFC1723/GSM11
224.0.0.10	IGRP Routers	Farinacci
224.0.0.11	Mobile-Agents	Bill Simpson
224.0.0.12	DHCP Server/Relay Agent	RFC1884
224.0.0.13	All PIM Routers	Farinacci
224.0.0.14	RSVP-ENCAPSULATION	Braden
224.0.0.15	All-cbt-routers	Ballardie
224.0.0.16	Designated-sbm	Baker
224.0.0.17	All-sbms	Baker
224.0.0.18	VRRP	Hinden

TABLE B.1 Multicast Addresses *(continued)*

Address	Purpose	Reference/Contact Acronym
224.0.0.19	IP All L1Iss	Przygienda
224.0.0.20	IP All L2Iss	Przygienda
224.0.0.21	IP All Intermediate Systems	Przygienda
224.0.0.22	IGMP	Deering
224.0.0.23	GLOBECAST-ID	Scannell
224.0.0.24	Unassigned	JBP
224.0.0.25	Router-to-Switch	Wu
224.0.0.26	Unassigned	JBP
224.0.0.27	AI MPP Hello	Martinicky
224.0.0.28	ETC Control	Zmudzinski
224.0.0.101	Cisco-hnap	Bakke
224.0.0.102	HSRP	Wilson
224.0.0.103	MDAP	Deleu
224.0.0.251	mDNS	Cheshire
224.0.1.0	VMTP Managers Group	RFC1045/DRC3
224.0.1.1	NTP Network Time Protocol	RFC1119/DLM1
224.0.1.2	SGI-Dogfight	AXC
224.0.1.3	Rwhod	SXD
224.0.1.4	VNP	DRC3

TABLE B.1 Multicast Addresses *(continued)*

Address	Purpose	Reference/Contact Acronym
224.0.1.5	Artificial Horizons-Aviator	BXF
224.0.1.6	NSS-Name Service Server	BXS2
224.0.1.7	AUDIONEWS-Audio News Multicast	MXF2
224.0.1.8	SUN NIS+ Information Service	CXM3
224.0.1.9	MTP Multicast Transport Protocol	SXA
224.0.1.10	IETF-1-LOW-AUDIO	SC3
224.0.1.11	IETF-1-AUDIO	SC3
224.0.1.12	IETF-1-VIDEO	SC3
224.0.1.13	IETF-2-LOW-AUDIO	SC3
224.0.1.14	IETF-2-AUDIO	SC3
224.0.1.15	IETF-2-VIDEO	SC3
224.0.1.16	MUSIC-SERVICE	Guido Van Rossum
224.0.1.17	SEANET-TELEMETRY	Andrew Maffei
224.0.1.18	SEANET-IMAGE	Andrew Maffei
224.0.1.19	MLOADD	Braden
224.0.1.20	Any private experiment	JBP
224.0.1.21	DVMRP on MOSPF	John Moy
224.0.1.22	SVRLOC	Veizades

TABLE B.1 Multicast Addresses *(continued)*

Address	Purpose	Reference/Contact Acronym
224.0.1.23	XINGTV	Gordon
224.0.1.24	Microsoft-DS	arnoldm@microsoft.com
224.0.1.25	NBC-PRO	bloomer@birch.crd.ge.com
224.0.1.26	NBC-PFN	bloomer@birch.crd.ge.com
224.0.1.31	Ampr-info	Janssen
224.0.1.32	Mtrace	Casner
224.0.1.33	RSVP-encap-1	Braden
224.0.1.34	RSVP-encap-2	Braden
224.0.1.35	SVRLOC-DA	Veizades
224.0.1.36	RLN-server	Kean
224.0.1.37	Proshare-mc	Lewis
224.0.1.38	Dantz	Yackle
224.0.1.39	Cisco-rp-announce	Farinacci
224.0.1.40	Cisco-rp-discovery	Farinacci
224.0.1.41	Gatekeeper	Toga
224.0.1.42	Iberiagames	Marocho
224.0.1.43	NWN-Discovery	Zwemmer
224.0.1.44	NWN-Adaptor	Zwemmer
224.0.1.45	ISMA-1	Dunne
224.0.1.46	ISMA-2	Dunne

TABLE B.1 Multicast Addresses *(continued)*

Address	Purpose	Reference/Contact Acronym
224.0.1.47	Telerate	Peng
224.0.1.48	Ciena	Rodbell
224.0.1.49	DCAP-servers	RFC2114
224.0.1.50	DCAP-clients	RFC2114
224.0.1.51	MCNTP-directory	Rupp
224.0.1.52	MBONE-VCR-directory	Holfelder
224.0.1.53	Heartbeat	Mamakos
224.0.1.54	Sun-mc-grp	DeMoney
224.0.1.55	Extended-sys	Poole
224.0.1.56	Pdrncs	Wissenbach
224.0.1.57	TNS-adv-multi	Albin
224.0.1.58	Vcals-dmu	Shindoh
224.0.1.59	Zuba	Jackson
224.0.1.60	Hp-device-disc	Albright
224.0.1.61	TMS-production	Gilani
224.0.1.62	Sunscalar	Gibson
224.0.1.63	MMTP-poll	Costales
224.0.1.64	Compaq-peer	Volpe
224.0.1.65	IAPP	Meier
224.0.1.66	Multihasc-com	Brockbank

TABLE B.1 Multicast Addresses *(continued)*

Address	Purpose	Reference/Contact Acronym
224.0.1.67	Serv-Discovery	Honton
224.0.1.68	Mdhcpdisover	RFC2730
224.0.1.69	MMP-bundle-Discovery1	Malkin
224.0.1.70	MMP-bundle-Discovery2	Malkin
224.0.1.71	XYPOINT DGPS Data Feed	Green
224.0.1.72	GilatSkySurfer	Gal
224.0.1.73	SharesLive	Rowatt
224.0.1.74	NorthernData	Sheers
224.0.1.75	SIP	Schulzrinne
224.0.1.76	IAPP	Moelard
224.0.1.77	AGENTVIEW	Iyer
224.0.1.78	Tibco Multicast1	Shum
224.0.1.79	Tibco Multicast2	Shum
224.0.1.80	MSP	Caves
224.0.1.81	OTT (One-way Trip Time)	Schwartz
224.0.1.82	TRACKTICKER	Novick
224.0.1.83	DTN-mc	Gaddie
224.0.1.84	Jini-announcement	Scheifler
224.0.1.85	Jini-request	Scheifler
224.0.1.86	SDE-Discovery	Aronson

TABLE B.1 Multicast Addresses *(continued)*

Address	Purpose	Reference/Contact Acronym
224.0.1.87	DirecPC-SI	Dillon
224.0.1.88	B1Rmonitor	Purkiss
224.0.1.89	3Com-AMP3 dRMON	Banthia
224.0.1.90	ImFtmSvc	Bhatti
224.0.1.91	NQDS4	Flynn
224.0.1.92	NQDS5	Flynn
224.0.1.93	NQDS6	Flynn
224.0.1.94	NLVL12	Flynn
224.0.1.95	NTDS1	Flynn
224.0.1.96	NTDS2	Flynn
224.0.1.97	NODSA	Flynn
224.0.1.98	NODSB	Flynn
224.0.1.99	NODSC	Flynn
224.0.1.100	NODSD	Flynn
224.0.1.101	NQDS4R	Flynn
224.0.1.102	NQDS5R	Flynn
224.0.1.103	NQDS6R	Flynn
224.0.1.104	NLVL12R	Flynn
224.0.1.105	NTDS1R	Flynn
224.0.1.106	NTDS2R	Flynn

TABLE B.1 Multicast Addresses *(continued)*

Address	Purpose	Reference/Contact Acronym
224.0.1.107	NODSAR	Flynn
224.0.1.108	NODSBR	Flynn
224.0.1.109	NODSCR	Flynn
224.0.1.110	NODSDR	Flynn
224.0.1.111	MRM	Wei
224.0.1.112	TVE-FILE	Blackketter
224.0.1.113	TVE-ANNOUNCE	Blackketter
224.0.1.114	Mac Srv Loc	Woodcock
224.0.1.115	Simple Multicast	Crowcroft
224.0.1.116	SpectraLinkGW	Hamilton
224.0.1.117	Dieboldmcast	Marsh
224.0.1.118	Tivoli Systems	Gabriel
224.0.1.119	PQ-Lic-mcast	Sledge
224.0.1.120	HYPERFEED	Kreutzjans
224.0.1.121	Pipesplatform	Dissett
224.0.1.122	LiebDevMgmg-DM	Velten
224.0.1.123	TRIBALVOICE	Thompson
224.0.1.124	UDLR-DTCP	Cipiere
224.0.1.125	PolyCom Relay1	Coutiere
224.0.1.126	Infront Multi1	Lindeman
224.0.1.127	XRX DEVICE DISC	Wang

TABLE B.1 Multicast Addresses *(continued)*

Address	Purpose	Reference/Contact Acronym
224.0.1.128	CNN	Lynch
224.0.1.129	PTP-primary	Eidson
224.0.1.130	PTP-alternate1	Eidson
224.0.1.131	PTP-alternate2	Eidson
224.0.1.132	PTP-alternate3	Eidson
224.0.1.133	ProCast	Revzen
224.0.1.134	3Com Discp	White
224.0.1.135	CS-Multicasting	Stanev
224.0.1.136	TS-MC-1	Sveistrup
224.0.1.137	Make Source	Daga
224.0.1.138	Teleborsa	Strazzera
224.0.1.139	SUMAConfig	Wallach
224.0.1.140	Unassigned	
224.0.1.141	DHCP-SERVERS	Hall
224.0.1.142	CN Router-LL	Armitage
224.0.1.143	EMWIN	Querubin
224.0.1.144	Alchemy Cluster	O'Rourke
224.0.1.145	Satcast One	Nevell
224.0.1.146	Satcast Two	Nevell
224.0.1.147	Satcast Three	Nevell
224.0.1.148	Intline	Sliwinski

TABLE B.1 Multicast Addresses *(continued)*

Address	Purpose	Reference/Contact Acronym
224.0.1.149	8x8 Multicast	Roper
224.0.1.150	Unassigned	JBP
224.0.1.166	Marratech-cc	Parnes
224.0.1.167	EMS-InterDev	Lyda
224.0.1.168	Itb301	Rueskamp
224.0.2.1	"RWHO" Group (BSD) (unofficial)	JBP
224.0.2.2	SUN RPC PMAPPROC_ CALLIT	BXE1
224.2.127.254	SAPv1 Announcements	SC3
224.2.127.255	SAPv0 Announcements	SC3

TABLE B.2 Multicast Group Assignments for Class D IP Addresses

Multicast Address	Group Assigned	Contact
224.0.0.0-224.0.0.255	Routing Protocols	
224.0.1.27-224.0.1.30	Lmsc-Calren-1 to 4	Uang
224.0.1.151-224.0.1.165	Intline 1 to 15	Sliwinski
224.0.1.169-224.0.1.255	Unassigned	JBP
224.0.2.064-224.0.2.095	SIAC MDD Service	Tse
224.0.2.096-224.0.2.127	CoolCast	Ballister
224.0.2.128-224.0.2.191	WOZ-Garage	Marquardt

TABLE B.2 Multicast Group Assignments for Class D IP Addresses *(continued)*

Multicast Address	Group Assigned	Contact
224.0.2.192-224.0.2.255	SIAC MDD Market Service	Lamberg
224.0.3.000-224.0.3.255	RFE Generic Service	DXS3
224.0.4.000-224.0.4.255	RFE Individual Conferences	DXS3
224.0.5.000-224.0.5.127	CDPD Groups	Bob Brenner
224.0.5.128-224.0.5.191	SIAC Market Service	Cho
224.0.5.192-224.0.5.255	Unassigned	IANA
224.0.6.000-224.0.6.127	Cornell ISIS Project	Tim Clark
224.0.6.128-224.0.6.255	Unassigned	IANA
224.0.7.000-224.0.7.255	Where-Are-You	Simpson
224.0.8.000-224.0.8.255	INTV	Tynan
224.0.9.000-224.0.9.255	Invisible Worlds	Malamud
224.0.10.000-224.0.10.255	DLSw Groups	Lee
224.0.11.000-224.0.11.255	NCC.NET Audio	Rubin
224.0.12.000-224.0.12.063	Microsoft and MSNBC	Blank
224.0.13.000-224.0.13.255	UUNET PIPEX Net News	Barber
224.0.14.000-224.0.14.255	NLANR	Wessels
224.0.15.000-224.0.15.255	Hewlett Packard	Van Der Meulen

TABLE B.2 Multicast Group Assignments for Class D IP Addresses *(continued)*

Multicast Address	Group Assigned	Contact
224.0.16.000-224.0.16.255	XingNet	Uusitalo
224.0.17.000-224.0.17.031	Mercantile & Commodity Exchange	Gilani
224.0.17.032-224.0.17.063	NDQMD1	Nelson
224.0.17.064-224.0.17.127	ODN-DTV	Hodges
224.0.18.000-224.0.18.255	Dow Jones	Peng
224.0.19.000-224.0.19.063	Walt Disney Company	Watson
224.0.19.064-224.0.19.095	Cal Multicast	Moran
224.0.19.096-224.0.19.127	SIAC Market Service	Roy
224.0.19.128-224.0.19.191	IIG Multicast	Carr
224.0.19.192-224.0.19.207	Metropol	Crawford
224.0.19.208-224.0.19.239	Xenoscience, Inc.	Timm
224.0.19.240-224.0.19.255	HYPERFEED	Felix
224.0.20.000-224.0.20.063	MS-IP/TV	Wong
224.0.20.064-224.0.20.127	Reliable Network Solutions	Vogels
224.0.20.128-224.0.20.143	TRACKTICKER Group	Novick
224.0.20.144-224.0.20.207	CNR Rebroadcast MCA	Sautter
224.0.21.000-224.0.21.127	Talarian MCAST	Mendal
224.0.22.000-224.0.22.255	WORLD MCAST	Stewart
224.0.252.000-224.0.252.255	Domain Scoped Group	Fenner

TABLE B.2 Multicast Group Assignments for Class D IP Addresses *(continued)*

Multicast Address	Group Assigned	Contact
224.0.253.000-224.0.253.255	Report Group	Fenner
224.0.254.000-224.0.254.255	Query Group	Fenner
224.0.255.000-224.0.255.255	Border Routers	Fenner
224.1.0.0-224.1.255.255	ST Multicast Groups	RFC1190/ KS14
224.2.0.0-224.2.127.253	Multimedia Conference Calls	SC3
224.2.128.0-224.2.255.255	SAP Dynamic Assignments	SC3
224.252.0.0-224.255.255.255	DIS transient groups	Joel Snyder
225.0.0.0-225.255.255.255	MALLOC	Handley
232.0.0.0-232.255.255.255	VMTP transient groups	DRC3
233.0.0.0-233.255.255.255	Static Allocations	Meyer2
239.000.000.000-239.255.255.255	Administratively Scoped	IANA/ RFC2365
239.000.000.000-239.063.255.255	Reserved	IANA
239.064.000.000-239.127.255.255	Reserved	IANA
239.128.000.000-239.191.255.255	Reserved	IANA
239.192.000.000-239.251.255.255	Organization-Local Scope	Meyer/ RFC2365
239.252.000.000-239.252.255.255	Site-Local Scope	Meyer/ RFC2365

TABLE B.2 Multicast Group Assignments for Class D IP Addresses *(continued)*

Multicast Address	Group Assigned	Contact
239.253.000.000-239.253.255.255	Site-Local Scope	Meyer/ RFC2365
239.254.000.000-239.254.255.255	Site-Local Scope	Meyer/ RFC2365
239.255.000.000-239.255.255.255	Site-Local Scope	Meyer/ RFC2365

TABLE B.3 Multicast RFCs

Reference RFC	RFC Title
RFC1045	VMTP: Versatile Message Transaction Protocol Specification
RFC1075	Distance Vector Multicast Routing Protocol
RFC1112	Host Extensions for IP Multicasting
RFC1119	Network Time Protocol (Version 1), Specification and Implementation
RFC1190	Experimental Internet Stream Protocol, Version 2 (ST-II)
RFC2328	OSPF Version 2
RFC1723	RIP Version 2: Carrying Additional Information
RFC1884	IP Version 6 Addressing Architecture
RFC2114	Data Link Switching Client Access Protocol
RFC2365	Administratively Scoped IP Multicast
RFC2730	Multicast Address Dynamic Client Allocation Protocol (MADCAP)

TABLE B.4 Contact Name and Address for the Assigned Multicast Addresses

Contact Acronym	Contact Name	E-Mail Address
Albin	Jerome Albin	albin@taec.enet.dec.com
Albright	Shivaun Albright	shivaun_albright@hp.com
Armitage	Ian Armitage	ian@coactive.com
Aronson	Peter Aronson	paronson@esri.com
AXC	Andrew Cherenson	arc@SGI.COM
Baker	Fred Baker	fred@cisco.com
Bakke	Mark Bakke	mbakke@cisco.com
Ballardie	Tony Ballardie	a.ballardie@cs.ucl.ac.uk
Ballister	Tom Ballister	tballister@starguidedigital.com
Banthia	Prakash Banthia	prakash_banthia@3com.com
Barber	Tony Barber	tonyb@pipex.com
Bhatti	Zia Bhatti	zia@netright.com
Blackketter	Dean Blackketter	dean@corp.webtv.net
Blank	Tom Blank	tomblank@microsoft.com
Braden	Bob Braden	braden@isi.edu
Bob Brenner	No Contact Information	
Brockbank	Darcy Brockbank	darcy@hasc.com
BXE1	Brendan Eic	brendan@illyria.wpd.sgi.com

TABLE B.4 Contact Name and Address for the Assigned Multicast Addresses *(continued)*

Contact Acronym	Contact Name	E-Mail Address
BXF	Bruce Factor	ahi!bigapple!bruce@uunet.UU.NET
BXS2	Bill Schilit	schilit@parc.xerox.com
Carr	Wayne Carr	Wayne_Carr@ccm.intel.com
Casner	Steve Casner	casner@isi.edu
Caves	Evan Caves	evan@acc.com
Cheshire	Stuart Cheshire	cheshire@apple.com
Chiang	Steve Chiang	schiang@cisco.com
Cho	Joan Cho	jcho@siac.com
Cipiere	Patrick Cipiere	Patrick.Cipiere@sophia.inria.fr
Costales	Bryan Costales	bcx@infobeat.com
Crawford	James Crawford	jcrawford@metropol.net
Crowcroft	Jon Crowcroft	jon@hocus.cs.ucl.ac.uk
CXM3	Chuck McManis	cmcmanis@sun.com
Tim Clark	No Contact Information	
Daga	Anthony Daga	anthony@mksrc.com
Deering	Steve Deering	deering@cisco.com
Deleu	Johan Deleu	Johan.deleu@alcatel.be
DeMoney	Michael DeMoney	demoney@eng.sun.com
Dillon	Doug Dillon	dillon@hns.com.

TABLE B.4 Contact Name and Address for the Assigned Multicast Addresses *(continued)*

Contact Acronym	Contact Name	E-Mail Address
Dissett	Daniel Dissett	ddissett@peerlogic.com
DLM1	David Mills	Mills@huey.udel.edu
DRC3	Dave Cheriton	cheriton@dsg.stanford.edu
Dunne	Stephen Dunne	sdun@isma.co.uk
DXS3	Daniel Steinberg	daniel.steinberg@eng.sun.com
Eidson	John Eidson	eidson@hpl.hp.com
Fenner	Bill Fenner	fenner@parc.xerox.com
Farinacci	Dino Farinacci	dino@cisco.com
Felix	Ken Felix	kfelix@pcquote.com
Flynn	Edward Flynn	flynne@nasdaq.com
Gabriel	Jon Gabriel	grabriel@tivoli.com
Gaddie	Bob Gaddie	bobg@dtn.com
Gal	Yossi Gal	yossi@gilat.com
Gibson	Terry Gibson	terry.gibson@sun.com
Gilani	Asad Gilani	agilani@nymex.com
GSM11	Gary S. Malkin	gmalkin@xylogics.com
Goland	Yaron Goland	yarong@microsoft.com
Gordon	Howard Gordon	hgordon@xingtech.com
Green	Cliff Green	cgreen@xypoint.com
Guttman	Erik Guttman	erik.guttman@eng.sun.com

TABLE B.4 Contact Name and Address for the Assigned Multicast Addresses *(continued)*

Contact Acronym	Contact Name	E-Mail Address
Hall	Eric Hall	ehall@ntrg.com
Hamilton	Mark Hamilton	mah@spectralink.com
Handley	Mark Handley	mjh@ISI.EDU
Hinden	Bob Hinden	hinden@Ipsilon.com
Hodges	Richard Hodges	rh@source.net
Hodgson	Robert Hodgson	robert@paratek.co.uk
Holfelder	Wieland Holdfelder	whd@pi4.informatik.uni-mannheim.de
Honton	Chas Honton	chas@secant.com
IANA	IANA	iana@iana.org
Iyer	Ram Iyer	ram@aaccorp.com
Jackson	Dan Jackson	jdan@us.ibm.com
Janssen	Rob Janssen	rob@pe1chl.ampr.org
JBP	Jon Postel	postel@isi.edu
JXM1	Jim Miner	miner@star.com
Kean	Brian Kean	bkean@dca.com
Koopman	Dirk Koopman	djk@tobit.co.uk
Kreutzjans	Michael Kreutzjans	mike@pcquote.com
KS14	Karen Seo	kseo@bbn.com

TABLE B.4 Contact Name and Address for the Assigned Multicast Addresses *(continued)*

Contact Acronym	Contact Name	E-Mail Address
Kutscher	Dirk Kutscher	dku@tzi.org
Lamberg	Mike Lamberg	mlamberg@siac.com
Lee	Choon Lee	cwl@nsd.3com.com
Lewis	Mark Lewis	Mark_Lewis@ccm.jf.intel.com
Lindeman	Morten Lindeman	Morten.Lindeman@os.telia.no
Lyda	Stephen T. Lyda	slyda@emsg.com
Lynch	Joel Lynch	joel.lynch@cnn.com
Malamud	Carl Malamud	carl@invisible.net
Andrew Maffei	No Contact Information	
Malkin	Gary Scott Malkin	gmalkin@baynetworks.com
Mamakos	Louis Mamakos	louie@uu.net
Manning	Bill Manning	bmanning@isi.edu
Marocho	Jose Luis Marocho	73374.313@compuserve.com
Marquardt	Douglas Marquardt	dmarquar@woz.org
Marsh	Gene Marsh	MarshM@diebold.com

TABLE B.4 Contact Name and Address for the Assigned Multicast Addresses *(continued)*

Contact Acronym	Contact Name	E-Mail Address
Martinicky	Brian Martinicky	Brian_Martinicky@automationintelligence.com
Meier	Bob Meier	meierb@norand.com
Mendal	Geoff Mendal	mendal@talarian.com
Meyer	David Meyer	meyer@ns.uoregon.edu
Meyer2	David Meyer	dmm@cisco.com
Moelard	Henri Moelard	hmoelard@wcnd.nl.lucent.com
Moran	Ed Moran	admin@cruzjazz.com
John Moy	John Moy	jmoy@casc.com
MXF2	Martin Forssen	maf@dtek.chalmers.se
Nelson	Gunnar Nelson	gunnar.nelson@nazdaq.com
Nevell	Julian Nevell	jnevell@vbs.bt.co.uk
Novick	Alan Novick	anovick@tdc.com
O'Rourke	Stacey O'Rourke	stacey@network-alchemy.com
Parnes	Peter Parnes	peppar@marratech.com
Peng	Wenjie Peng	wpeng@tts.telerate.com
Poole	David Poole	davep@extendsys.com
Przygienda	Tony Przygienda	prz@siara.com
Purkiss	Ed Purkiss	epurkiss@wdmacodi.com

TABLE B.4 Contact Name and Address for the Assigned Multicast Addresses *(continued)*

Contact Acronym	Contact Name	E-Mail Address
Querubin	Antonio Querubin	tony@lava.net
Revzen	Shai Revzen	shrevz@nmcfast.com
Rodbell	Mike Rodbell	mrodbell@ciena.com
Roper	Mike Roper	mroper@8x8.com
Guido Van Rossum	No Contact Information	
Rowatt	Shane Rowatt	shane.rowatt@star.com.au
Roy	George Roy	owens@appliedtheory.com
Rubin	David Rubin	drubin@ncc.net
Rupp	Heiko Rupp	hwr@xlink.net
Rueskamp	Bodo Rueskamp	br@itchigo.com
Sautter	Robert Sautter	rsautter@acdnj.itt.com
SC3	Steve Casner	casner@precept.com
Scannell	Piers Scannell	piers@globecastne.com
Scheifler	Bob Scheifler	bob.scheifler@sun.com
Schwartz	Beverly Schwartz	bschwart@bbn.com
Shindoh	Masato Shindoh	jl11456@yamato.ibm.co.jp
Shum	Raymond Shum	rshum@ms.com
Simpson	Bill Simpson	bill.simpson@um.cc.umich.edu

TABLE B.4 Contact Name and Address for the Assigned Multicast Addresses *(continued)*

Contact Acronym	Contact Name	E-Mail Address
Sledge	Bob Sledge	bob@pqsystems.com
Sliwinski	Robert Sliwinski	sliwinre@mail1st.com
Stanev	Nedelcho Stanev	nstanev@csoft.bg
Stewart	Ian Stewart	iandbige@yahoo.com
Strazzera	Paolo Strazzera	p.strazzera@telematica.it
Sveistrup	Darrell Sveistrup	darrells@truesolutions.net
SXA	Susie Armstrong	armstrong.wbst128@xerox.com
SXD	Steve Deering	deering@parc.xerox.com
Thaler	Dave Thaler	dthaler@microsoft.com
Thompson	Nigel Thompson	nigelt@tribal.com
Timm	Mary Timm	mary@xenoscience.com
Tynan	Dermot Tynan	dtynan@claddagh.ie
Toga	Jim Toga	jtoga@ibeam.jf.intel.com
Tse	Geordie Tse	gtse@siac.com
Uang	Yea Uang	uang@force.decnet.lockheed.com
Uusitalo	Mika Uusitalo	msu@xingtech.com
Van Der Muelen	Ron van der Muelen	ronv@lsid.hp.com
Veizades	John Veizades	veizades@tgv.com
Velten	Mike Velten	mike_velten@liebert.com

TABLE B.4 Contact Name and Address for the Assigned Multicast Addresses *(continued)*

Contact Acronym	Contact Name	E-Mail Address
Vogels	Werner Vogels	vogels@rnets.com
Volpe	Victor Volpe	vvolpe@smtp.microcom.com
Wallach	Walter Wallach	walt@sumatech.com
Wang	Michael Wang	michael.wang@usa.xerox.com
Watson	Scott Watson	scott@disney.com
Wei	Liming Wei	lwei@cisco.com
Wessels	Duane Wessels	wessels@nlanr.net
White	Peter White	peter_white@3com.com
Wilson	Ian Wilson	iwilson@cisco.com
Wissenbach	Paul Wissenbach	paulwi@vnd.tek.com
Wong	Tony Wong	wongt@ms.com
Woodcock	Bill Woodcock	woody@zocalo.net
Wu	Ishan Wu	iwu@cisco.com
Yackle	Dotty Yackle	ditty_yackle@dantz.com
Zwemmer	Arnoud Zwemmer	arnoud@nwn.nl
Zmudzinski	Krystof Zmudzinski	kzmudzinski@etcconnect.com

Glossary

A&B bit signaling Used in T1 transmission facilities and sometimes called "24th channel signaling." Each of the 24 T1 subchannels in this procedure uses one bit of every sixth frame to send supervisory signaling information.

AAA Authentication, authorization, and accounting. A Cisco description of the processes that are required to provide a remote access security solution. Each is implemented separately, but each can rely on the others for functionality.

AAL ATM Adaptation Layer: A service-dependent sublayer of the Data Link layer, which accepts data from other applications and brings it to the ATM layer in 48-byte ATM payload segments. CS and SAR are the two sublayers that form AALs. Currently, the four types of AAL recommended by the ITU-T are AAL1, AAL2, AAL3/4, and AAL5. AALs are differentiated by the source-destination timing they use, whether they are CBR or VBR, and whether they are used for connection-oriented or connectionless mode data transmission. *See also: AAL1, AAL2, AAL3/4, AAL5, ATM,* and *ATM layer.*

AAL1 ATM Adaptation Layer 1: One of four AALs recommended by the ITU-T, it is used for connection-oriented, time-sensitive services that need constant bit rates, such as isochronous traffic and uncompressed video. *See also: AAL.*

AAL2 ATM Adaptation Layer 2: One of four AALs recommended by the ITU-T, it is used for connection-oriented services that support a variable bit rate, such as voice traffic. *See also: AAL.*

AAL3/4 ATM Adaptation Layer 3/4: One of four AALs (a product of two initially distinct layers) recommended by the ITU-T, supporting both connectionless and connection-oriented links. Its primary use is in sending SMDS packets over ATM networks. *See also: AAL.*

AAL5 ATM Adaptation Layer 5: One of four AALs recommended by the ITU-T, it is used to support connection-oriented VBR services primarily to transfer classical IP over ATM and LANE traffic. This least complex of the AAL recommendations uses SEAL, offering lower bandwidth costs and simpler processing requirements but also providing reduced bandwidth and error-recovery capacities. *See also: AAL.*

AARP AppleTalk Address Resolution Protocol: The protocol in an AppleTalk stack that maps Data Link addresses to Network addresses.

AARP probe packets Packets sent by the AARP to determine whether a given node ID is being used by another node in a nonextended AppleTalk network. If the node ID is not in use, the sending node appropriates that node's ID. If the node ID is in use, the sending node will select a different ID and then send out more AARP probe packets. *See also: AARP.*

ABM Asynchronous Balanced Mode: When two stations can initiate a transmission, ABM is an HDLC (or one of its derived protocols) communication technology that supports peer-oriented, point-to-point communications between both stations.

ABR Area Border Router: An OSPF router that is located on the border of one or more OSPF areas. ABRs are used to connect OSPF areas to the OSPF backbone area. *Compare to: CBR* and *VBR.*

access control Used by Cisco routers to control packets as they pass through a router. Access lists are created and then applied to router interfaces to accomplish this.

access layer One of the layers in Cisco's three-layer hierarchical model. The access layer provides users with access to the internetwork.

access link A link used with switches. Only part of one Virtual LAN (VLAN). Trunk links carry information from multiple VLANs.

access list A set of test conditions kept by routers that determines "interesting traffic" to and from the router for various services on the network.

access method The manner in which network devices approach gaining access to the network itself.

access rate Defines the bandwidth rate of the circuit. For example, the access rate of a T1 circuit is 1.544Mbps. In Frame Relay and other technologies, there may be a fractional T1 connection—256Kbps, for example—however, the access rate and clock rate is still 1.544Mbps.

access server Also known as a "network access server," it is a communications process connecting asynchronous devices to a LAN or WAN through network and terminal emulation software, providing synchronous or asynchronous routing of supported protocols.

acknowledgment Verification sent from one network device to another signifying that an event has occurred. May be abbreviated as ACK. *Contrast with: NAK.*

accounting One of the three components in AAA. Accounting provides auditing and logging functionalities to the security model.

ACR Allowed Cell Rate: A designation defined by the ATM Forum for managing ATM traffic. Dynamically controlled by using congestion control measures, the ACR varies between the Minimum Cell Rate (MCR) and the Peak Cell Rate (PCR). *See also: MCR* and *PCR*.

active monitor The mechanism used to manage a Token Ring. The network node with the highest MAC address on the ring becomes the active monitor and is responsible for management tasks such as preventing loops and ensuring that tokens are not lost.

address learning Used with transparent bridges to learn the hardware addresses of all devices on an internetwork. The switch then filters the network with the known hardware (MAC) addresses.

address mapping A methodology that translates network addresses from one format to another so that different protocols can operate interchangeably.

address mask A bit combination descriptor identifying which portion of an address refers to the network or subnet and which part refers to the host. Sometimes simply called the "mask." *See also: subnet mask*.

address resolution The process used for resolving differences between computer addressing schemes. Address resolution typically defines a method for tracing Network-layer (layer 3) addresses to Data Link–layer (layer 2) addresses. *See also: address mapping*.

adjacency The relationship made between defined neighboring routers and end nodes, using a common media segment, to exchange routing information.

administrative distance A number between 0 and 255 that expresses the value of trustworthiness of a routing information source. The lower the number, the higher the integrity rating.

administrative weight A value designated by a network administrator to rate the preference given to a network link. It is one of four link metrics exchanged by PTSPs to test ATM network resource availability.

ADSU ATM Data Service Unit: The terminal adapter used to connect to an ATM network through an HSSI-compatible mechanism. *See also: DSU*.

advertising The process whereby routing or service updates are transmitted at given intervals, enabling other routers on the network to maintain a record of viable routes.

AEP AppleTalk Echo Protocol: A test for connectivity between two AppleTalk nodes whereby one node sends a packet to another and receives an echo, or copy, in response.

AFI Authority and Format Identifier: The part of an NSAP ATM address that delineates the type and format of the IDI section of an ATM address.

AFP AppleTalk Filing Protocol: A Presentation-layer protocol, supporting AppleShare and Mac OS File Sharing, that permits users to share files and applications on a server.

AIP ATM Interface Processor: Supporting AAL3/4 and AAL5, this interface for Cisco 7000 series routers minimizes performance bottlenecks at the UNI. *See also: AAL3/4* and *AAL5*.

algorithm A set of rules or process used to solve a problem. In networking, algorithms are typically used for finding the best route for traffic from a source to its destination.

alignment error An error occurring in Ethernet networks, in which a received frame has extra bits, that is, a number not divisible by eight. Alignment errors are generally the result of frame damage caused by collisions.

all-routes explorer packet An explorer packet that can move across an entire SRB network, tracing all possible paths to a given destination. Also known as an "all-rings explorer packet." *See also: explorer packet, local explorer packet,* and *spanning explorer packet.*

AM Amplitude Modulation: A modulation method that represents information by varying the amplitude of the carrier signal. *See also: modulation.*

AMI Alternate Mark Inversion: A line-code type on T1 and E1 circuits that shows zeros as "01" during each bit cell, and ones as "11" or "00," alternately, during each bit cell. The sending device must maintain ones density in AMI but not independently of the data stream. Also known as "binary-coded, Alternate Mark Inversion." *Contrast with: B8ZS. See also: ones density.*

amplitude An analog or digital waveform's highest value.

analog Analog signaling is a technique to carry voice and data over copper and wireless media. When analog signals are transmitted over wires or through the air, the transmission conveys information through a variation of some type of signal amplitude, frequency, and phase.

analog connection Provides signaling via an infinitely variable waveform. This differs from a digital connection, in which a definite waveform is used to define values. Traditional phone service is an analog connection.

analog transmission Signal messaging whereby information is represented by various combinations of signal amplitude, frequency, and phase.

ANSI American National Standards Institute: The organization of corporate, government, and other volunteer members that coordinates standards-related activities, approves U.S. national standards, and develops U.S. positions in international standards organizations. ANSI assists in the creation of international and U.S. standards in disciplines such as communications, networking, and a variety of technical fields. It publishes over 13,000 standards for engineered products and technologies ranging from screw threads to networking protocols. ANSI is a member of the International Engineering Consortium (IEC) and International Organization for Standardization (ISO).

anycast An ATM address that can be shared by more than one end system, enabling requests to be routed to a node that provides a particular service.

AppleTalk Currently in two versions, the group of communication protocols designed by Apple Computer for use in Macintosh environments. The earlier Phase 1 protocols support one physical network with only one network number that resides in one zone. The later Phase 2 protocols support more than one logical network on a single physical network, enabling networks to exist in more than one zone. *See also: zone.*

Application layer Layer 7 of the OSI reference network model, supplying services to application procedures (such as electronic mail or file transfer) that are outside the OSI model. This 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.

ARA AppleTalk Remote Access: A protocol for Macintosh users establishing their access to resources and data from a remote AppleTalk location.

area A logical, rather than physical, set of segments (based on either CLNS, DECnet, or OSPF) along with their attached devices. Areas are commonly connected to others by using routers to create a single autonomous system. *See also: autonomous system.*

ARM Asynchronous Response Mode: An HDLC communication mode using one primary station and at least one additional station, in which transmission can be initiated from either the primary or one of the secondary units.

ARP Address Resolution Protocol: Defined in RFC 826, the protocol that traces IP addresses to MAC addresses. *See also: RARP.*

ASBR Autonomous System Boundary Router: An area border router placed between an OSPF autonomous system and a non-OSPF network that operates both OSPF and an additional routing protocol, such as RIP. ASBRs must be located in a non-stub OSPF area. *See also: ABR, non-stub area,* and *OSPF.*

ASCII American Standard Code for Information Interchange: An 8-bit code for representing characters, consisting of 7 data bits plus 1 parity bit.

ASICs Application-specific integrated circuits: Used in layer 2 switches to make filtering decisions. The ASIC looks in the filter table of MAC addresses and determines which port the destination hardware address of a received hardware address is destined for. The frame will be allowed to traverse only that one segment. If the hardware address is unknown, the frame is forwarded out all ports.

ASN.1 Abstract Syntax Notation One: An OSI language used to describe types of data that are independent of computer structures and depicting methods. Described by ISO International Standard 8824.

ASP AppleTalk Session Protocol: A protocol employing ATP to establish, maintain, and tear down sessions, as well as sequence requests. *See also: ATP.*

AST Automatic Spanning Tree: A function that supplies one path for spanning explorer frames traveling from one node in the network to another, supporting the automatic resolution of spanning trees in SRB networks. AST is based on the IEEE 802.1 standard. *See also: IEEE 802.1* and *SRB.*

asynchronous connection Defines the start and stop of each octet. As a result, each byte in asynchronous connections requires 2 bytes of overhead. Synchronous connections use a synchronous clock to mark the start and stop of each character.

asynchronous dial-up Asynchronous dial-up is interchangeable with analog dial-up. Both terms refer to traditional modem-based connections.

asynchronous transmission Digital signals sent without precise timing, usually with different frequencies and phase relationships. Asynchronous transmissions generally enclose individual characters in control bits (called start and stop bits) that show the beginning and end of each character. *Contrast with: isochronous transmission* and *synchronous transmission.*

ATCP AppleTalk Control Program: The protocol for establishing and configuring AppleTalk over PPP, defined in RFC 1378. *See also: PPP.*

ATDM Asynchronous Time-Division Multiplexing: A technique for sending information, it differs from standard TDM in that the time slots are assigned when necessary rather than preassigned to certain transmitters. *Contrast with: FDM, statistical multiplexing,* and *TDM.*

ATG Address Translation Gateway: The mechanism within Cisco DECnet routing software that enables routers to route multiple, independent DECnet networks and to establish a user-designated address translation for chosen nodes between networks.

ATM Asynchronous Transfer Mode: The international standard, identified by fixed-length 53-byte cells, for transmitting cells in multiple service systems, such as voice, video, or data. Transit delays are reduced because the fixed-length cells permit processing to occur in the hardware. ATM is designed to maximize the benefits of high-speed transmission media, such as SONET, E3, and T3.

ATM ARP server A device that supplies logical subnets running classical IP over ATM with address-resolution services.

ATM endpoint The initiating or terminating connection in an ATM network. ATM endpoints include servers, workstations, ATM-to-LAN switches, and ATM routers.

ATM Forum The international organization founded jointly by Northern Telecom, Sprint, Cisco Systems, and NET/ADAPTIVE in 1991 to develop and promote standards-based implementation agreements for ATM technology. The ATM Forum broadens official standards developed by ANSI and ITU-T and creates implementation agreements before official standards are published.

ATM layer A sublayer of the Data Link layer in an ATM network that is service independent. To create standard 53-byte ATM cells, the ATM layer receives 48-byte segments from the AAL and attaches a 5-byte header to each. These cells are then sent to the Physical layer for transmission across the physical medium. *See also: AAL.*

ATMM ATM Management: A procedure that runs on ATM switches, managing rate enforcement and VCI translation. *See also: ATM.*

ATM user-user connection A connection made by the ATM layer to supply communication between at least two ATM service users, such as ATMM processes. These communications can be uni- or bidirectional, using one or two VCCs, respectively. *See also: ATM layer* and *ATMM.*

ATP AppleTalk Transaction Protocol: A Transport-level protocol that enables reliable transactions between two sockets, whereby one requests the other to perform a given task and to report the results. ATP fastens the request and response together, ensuring a loss-free exchange of request-response pairs.

attenuation In communication, weakening or loss of signal energy, typically caused by distance.

AURP AppleTalk Update-based Routing Protocol: A technique for encapsulating AppleTalk traffic in the header of a foreign protocol that allows the connection of at least two noncontiguous AppleTalk internetworks through a foreign network (such as TCP/IP) to create an AppleTalk WAN. The connection made is called an AURP tunnel. By exchanging routing information between exterior routers, the AURP maintains routing tables for the complete AppleTalk WAN. *See also: AURP tunnel.*

AURP tunnel A connection made in an AURP WAN that acts as a single, virtual link between AppleTalk internetworks separated physically by a foreign network such as a TCP/IP network. *See also: AURP.*

authentication The first component in the AAA model. Users are typically authenticated via a username and password, which are used to uniquely identify them.

authority zone A portion of the domain-name tree associated with DNS for which one name server is the authority. *See also: DNS.*

authorization The act of permitting access to a resource based on authentication information in the AAA model.

auto duplex A setting on layer 1 and 2 devices that sets the duplex of a switch port automatically.

auto-negotiation The process of two network devices communicating, trying to decide what duplex and speed will be used for data transport.

automatic call reconnect A function that enables automatic call rerouting away from a failed trunk line.

autonomous confederation A collection of self-governed systems that depend more on their own network accessibility and routing information than on information received from other systems or groups.

autonomous switching The ability of Cisco routers to process packets more quickly by using the ciscoBus to switch packets independently of the system processor.

autonomous system (AS) A group of networks under mutual administration that share the same routing methodology. Autonomous systems are subdivided by areas and must be assigned an individual 16-bit number by the IANA. *See also: area.*

auto-reconfiguration A procedure executed by nodes within the failure domain of a Token Ring, wherein nodes automatically perform diagnostics, trying to reconfigure the network around failed areas.

Auto-RP An IOS feature that allows multicast-enabled routers to detect RP and forward the summary information to other routers and hosts.

auxiliary port The console port on the back of Cisco routers that enables you to dial the router and make console configuration settings.

AVVID Architecture for Voice, Video, and Integrated Data: This is a Cisco marketing term to group their convergence efforts. Convergence is the integration of historically distinct services into a single service.

B8ZS Binary 8-Zero Substitution: A line-code type, interpreted at the remote end of the connection, that uses a special code substitution whenever eight consecutive zeros are transmitted over the link on T1 and E1 circuits. This technique assures ones density independent of the data

stream. Also known as "Bipolar 8-Zero Substitution." *Contrast with: AMI. See also: ones density.*

backbone The basic portion of the network that provides the primary path for traffic sent to and initiated from other networks.

BackboneFast A method whereby, if the switch receives an inferior BPDU on a root port, the switch will begin figuring out who the new root bridge is in less time than normal spanning tree convergence. This accelerates spanning tree convergence after the failure of a non-directly connected network link.

back end A node or software program supplying services to a front end. *See also: server.*

bandwidth The gap between the highest and lowest frequencies employed by network signals. More commonly, it refers to the rated throughput capacity of a network protocol or medium.

BoD Bandwidth on Demand: This function enables an additional B channel to be used to increase the amount of bandwidth available for a particular connection.

baseband A feature of a network technology that uses only one carrier frequency, for example Ethernet. Also named "narrowband." *Contrast with: broadband.*

Basic Management Setup Used with Cisco routers when in setup mode. Provides only enough management and configuration to get the router working so someone can telnet into the router and configure it.

baud Synonymous with bits per second (bps), if each signal element represents 1 bit. It is a unit of signaling speed equivalent to the number of separate signal elements transmitted per second.

B channel Bearer channel: A full-duplex, 64Kbps channel in ISDN that transmits user data. *Compare to: D channel, E channel,* and *H channel.*

beacon An FDDI device or Token Ring frame that points to a serious problem with the ring, such as a broken cable. The beacon frame carries the address of the station thought to be down. *See also: failure domain.*

bearer service Used by service providers to provide DS0 service to ISDN customers. A DS0 is one 64KB channel. An ISDN bearer service provides

either two DS0s, called two bearer channels, for a Basic Rate Interface (BRI), or 24 DS0s, called a Primary Rate Interface (PRI).

BECN Backward Explicit Congestion Notification: The bit set by a Frame Relay network in frames moving away from frames headed into a congested path. A DTE that receives frames with the BECN may ask higher-level protocols to take necessary flow control measures. *Contrast with: FECN.*

BGP4 BGP Version 4: Version 4 of the interdomain routing protocol most commonly used on the Internet. BGP4 supports CIDR and uses route-counting mechanisms to decrease the size of routing tables. *See also: CIDR.*

bidirectional shared tree A method of shared tree multicast forwarding. This method enables group members to receive data from the source or the RP, whichever is closer. *See also: RP (rendezvous point).*

binary A two-character numbering method that uses ones and zeros. The binary numbering system underlies all digital representation of information.

BIP Bit Interleaved Parity: A method used in ATM to monitor errors on a link, sending a check bit or word in the link overhead for the previous block or frame. This enables bit errors in transmissions to be found and delivered as maintenance information.

BISDN Broadband ISDN: ITU-T standards created to manage high-bandwidth technologies such as video. BISDN presently employs ATM technology along SONET-based transmission circuits, supplying data rates between 155Mbps and 622Mbps and beyond. *See also: BRI, ISDN,* and *PRI.*

bit-oriented protocol Regardless of frame content, the class of Data Link–layer communication protocols that transmits frames. Bit-oriented protocols, as compared with byte-oriented, supply more efficient and trustworthy, full-duplex operation. *Compare to: byte-oriented protocol.*

Boot ROM Used in routers to put the router into bootstrap mode. Bootstrap mode then boots the device with an operating system. The ROM can also hold a small Cisco IOS.

border gateway A router that facilitates communication with routers in different autonomous systems.

border router Typically defined within Open Shortest Path First (OSPF) as a router that connected an area to the backbone area. However, a

border router can be a router that connects a company to the Internet as well. *See also: OSPF.*

BPDU Bridge Protocol Data Unit: A Spanning Tree Protocol initializing packet that is sent at definable intervals for the purpose of exchanging information among bridges in networks.

BRI Basic Rate Interface: The ISDN interface that facilitates circuit-switched communication between video, data, and voice; it is made up of two B channels (64Kbps each) and one D channel (16Kbps). *Compare to: PRI. See also: BISDN.*

bridge A device for connecting two segments of a network and transmitting packets between them. Both segments must use identical protocols to communicate. Bridges function at the Data Link layer, layer 2 of the OSI reference model. The purpose of a bridge is to filter, send, or flood any incoming frame, based on the MAC address of that particular frame.

bridge ID Used to find and elect the root bridge in a layer 2 switched internetwork. The bridge ID is a combination of the bridge priority and base MAC address.

bridging A layer 2 process to block or forward frames based on MAC layer addresses. Bridges are lower speed, lower port density switches.

broadband A transmission methodology for multiplexing several independent signals onto one cable. In telecommunications, broadband is classified as any channel with bandwidth greater than 4kHz (typical voice grade). In LAN terminology, it is classified as a coaxial cable on which analog signaling is employed. Also known as "wideband." *Contrast with: baseband.*

broadcast A data frame or packet that is transmitted to every node on the local network segment (as defined by the broadcast domain). Broadcasts are known by their broadcast address, which is a destination network and host address with all the bits turned on. Also called "local broadcast." *Compare to: directed broadcast.*

broadcast domain A group of devices receiving broadcast frames initiating from any device within the group. Because they do not forward broadcast frames, broadcast domains are generally surrounded by routers.

broadcast storm An undesired event on the network caused by the simultaneous transmission of any number of broadcasts across the network

segment. Such an occurrence can overwhelm network bandwidth, resulting in time-outs.

brute force attack A type of attack that bombards the resource with attempted connections until successful. In the most common brute force attack, different passwords are repeatedly tried until a match that is then used to compromise the network is found.

buffer A storage area dedicated to handling data while in transit. Buffers are used to receive/store sporadic deliveries of data bursts, usually received from faster devices, compensating for the variations in processing speed. Incoming information is stored until everything is received prior to sending data on. Also known as an "information buffer."

bursting Some technologies, including ATM and Frame Relay, are considered burstable. This means that user data can exceed the bandwidth normally reserved for the connection; however, this cannot exceed the port speed. An example of this is a 128Kbps Frame Relay CIR on a T1—depending on the vendor, it might be possible to send more than 128Kbps for a short time.

bus topology A linear LAN architecture in which transmissions from various stations on the network are reproduced over the length of the medium and are accepted by all other stations. *Contrast with: ring topology* and *star topology*.

bus Any physical path, typically wires or copper, through which a digital signal can be used to send data from one part of a computer to another.

BUS Broadcast and unknown servers: In LAN emulation, the hardware or software responsible for resolving all broadcasts and packets with unknown (unregistered) addresses into the point-to-point virtual circuits required by ATM. *See also: LANE, LEC, LECS,* and *LES.*

BX.25 AT&T's use of X.25. *See also: X.25.*

bypass mode An FDDI and Token Ring network operation that deletes an interface.

bypass relay A device that enables a particular interface in the Token Ring to be closed down and effectively taken off the ring.

byte-oriented protocol Any type of Data Link communication protocol that, in order to mark the boundaries of frames, uses a specific character

from the user character set. These protocols have generally been superseded by bit-oriented protocols. *Compare to: bit-oriented protocol.*

cable modem A cable modem is not actually an analog device, like an asynchronous modem, but rather a customer access device for linking to a broadband cable network. These devices are typically bridges that have a COAX connection to link to the cable network and a 10BaseT Ethernet connection to link to the user's PC.

cable range In an extended AppleTalk network, the range of numbers allotted for use by existing nodes on the network. The value of the cable range can be anywhere from a single number to a sequence of several touching network numbers. Node addresses are determined by their cable range value.

CAC Connection Admission Control: The sequence of actions executed by every ATM switch while connection setup is performed in order to determine whether a request for connection is violating the guarantees of QoS for established connections. Also, CAC is used to route a connection request through an ATM network.

call admission control A device for managing traffic in ATM networks, determining the possibility of a path containing adequate bandwidth for a requested VCC.

call priority In circuit-switched systems, the defining priority given to each originating port; it specifies in which order calls will be reconnected. Additionally, call priority identifies which calls are allowed during a bandwidth reservation.

call setup time The length of time necessary to effect a switched call between DTE devices.

candidate packets Packets identified by the MLS-SE as having the potential for establishing a flow cache. This determination is made based on the destination MAC (DMAC) address. The DMAC address must be a MAC addresses associated with a known MLS-RP. *See also: MLS-SE* and *MLS-RP*.

CBR Constant Bit Rate: An ATM Forum QoS class created for use in ATM networks. CBR is used for connections that rely on precision clocking to guarantee trustworthy delivery. *Compare to: ABR* and *VBR*.

CD Carrier Detect: A signal indicating that an interface is active or that a connection generated by a modem has been established.

CDP Cisco Discovery Protocol: Cisco's proprietary protocol that is used to tell a neighbor Cisco device about the type of hardware, software version, and active interfaces that the Cisco device is using. It uses a SNAP frame between devices and is not routable.

CDVT Cell Delay Variation Tolerance: A QoS parameter for traffic management in ATM networks specified when a connection is established. The allowable fluctuation levels for data samples taken by the PCR in CBR transmissions are determined by the CDVT. *See also: CBR* and *PCR*.

cell In ATM networking, the basic unit of data for switching and multiplexing. Cells have a defined length of 53 bytes, including a 5-byte header that identifies the cell's data stream and 48 bytes of payload. *See also: cell relay*.

cell payload scrambling The method by which an ATM switch maintains framing on some medium-speed edge and trunk interfaces (T3 or E3 circuits). Cell payload scrambling rearranges the data portion of a cell to maintain the line synchronization with certain common bit patterns.

cell relay A technology that uses small packets of fixed size, known as cells. Their fixed length enables cells to be processed and switched in hardware at high speeds, making this technology the foundation for ATM and other high-speed network protocols. *See also: cell*.

Centrex A local exchange carrier service, providing local switching that resembles that of an on-site PBX. Centrex has no on-site switching capability. Therefore, all customer connections return to the CO. *See also: CO*.

CER Cell Error Ratio: In ATM, the ratio of the number of transmitted cells having errors to the total number of cells sent in a transmission within a certain span of time.

CGMP Cisco Group Management Protocol: A proprietary protocol developed by Cisco. The router uses CGMP to send multicast membership commands to Catalyst switches.

Challenge Used to provide authentication in Challenge Handshake Authentication Protocol (CHAP) as part of the handshake process. This numerically unique query is sent to authenticate the user without sending the password unencrypted across the wire. *See also: CHAP*.

channelized E1 Operating at 2.048Mpbs, an access link that is sectioned into 29 B-channels and one D-channel, supporting DDR, Frame Relay, and X.25. *Compare to: channelized T1.*

channelized T1 Operating at 1.544Mbps, an access link that is sectioned into 23 B-channels and 1 D-channel of 64Kbps each, where individual channels or groups of channels connect to various destinations, supporting DDR, Frame Relay, and X.25. *Compare to: channelized E1.*

CHAP Challenge Handshake Authentication Protocol: Supported on lines using PPP encapsulation, it is a security feature that identifies the remote end, helping keep out unauthorized users. After CHAP is performed, the router or access server determines whether a given user is permitted access. It is a newer, more secure protocol than PAP. *Compare to: PAP.*

character mode connections Character mode connections are typically terminated at the access server and include Telnet and console connections.

checksum A test for ensuring the integrity of sent data. It is a number calculated from a series of values taken through a sequence of mathematical functions, typically placed at the end of the data from which it is calculated, and then recalculated at the receiving end for verification. *Compare to: CRC.*

choke packet When congestion exists, it is a packet sent to inform a transmitter that it should decrease its sending rate.

CIDR Classless Interdomain Routing: A method supported by classless routing protocols, such as OSPF and BGP4, based on the concept of ignoring the IP class of address, permitting route aggregation and VLSM that enable routers to combine routes in order to minimize the routing information that needs to be conveyed by the primary routers. It allows a group of IP networks to appear to other networks as a unified, larger entity. In CIDR, IP addresses and their subnet masks are written as four dotted octets, followed by a forward slash and the numbering of masking bits (a form of subnet notation shorthand). *See also: BGP4.*

CIP Channel Interface Processor: A channel attachment interface for use in Cisco 7000 series routers that connects a host mainframe to a control unit. This device eliminates the need for a Front-End Processor (FEP) to attach channels.

CIR Committed Information Rate: Averaged over a minimum span of time and measured in bits per second (bps), a Frame Relay network's agreed-upon minimum rate of transferring information.

circuit switching Used with dial-up networks such as PPP and ISDN. Passes data, but needs to set up the connection first—just like making a phone call.

Cisco FRAD Cisco Frame-Relay Access Device: A Cisco product that supports Cisco IPS Frame Relay SNA services, connecting SDLC devices to Frame Relay without requiring an existing LAN. Can be upgraded to a fully functioning multiprotocol router. Can activate conversion from SDLC to Ethernet and Token Ring, but does not support attached LANs. *See also: FRAD*.

Cisco hierarchical model A Cisco model for building switched networks. The model consists of access layer devices, distribution layer devices, and core layer devices.

Cisco IOS software Cisco Internetworking Operating System software. The kernel of the Cisco line of routers and switches that supplies shared functionality, scalability, and security for all products under its CiscoFusion architecture. *See also: CiscoFusion*.

CiscoFusion Cisco's name for the internetworking architecture under which its Cisco IOS operates. It is designed to "fuse" together the capabilities of its disparate collection of acquired routers and switches.

CiscoView GUI-based management software for Cisco networking devices, enabling dynamic status, statistics, and comprehensive configuration information. Displays a physical view of the Cisco device chassis and provides device-monitoring functions and fundamental troubleshooting capabilities. Can be integrated with a number of SNMP-based network management platforms.

Class A network Part of the Internet Protocol hierarchical addressing scheme. Class A networks have only 8 bits for defining networks and 24 bits for defining hosts on each network. *Compare to: Class B network* and *Class C network*.

Class B network Part of the Internet Protocol hierarchical addressing scheme. Class B networks have 16 bits for defining networks and 16 bits for defining hosts on each network. *Compare to: Class A network* and *Class C network*.

Class C network Part of the Internet Protocol hierarchical addressing scheme. Class C networks have 24 bits for defining networks and only 8 bits for defining hosts on each network. *Compare to: Class A network* and *Class B network*.

classical IP over ATM Defined in RFC 1577, the specification for running IP over ATM that maximizes ATM features. Also known as "CIA."

classless routing Routing that sends subnet mask information in the routing updates. Classless routing allows Variable-Length Subnet Mask (VLSM) and supernetting. Routing protocols that support classless routing are RIP version 2, EIGRP, and OSPF.

CLI Command-line interface: Enables you to configure Cisco routers and switches with maximum flexibility.

clocking Used in synchronous connections to provide a marker for the start and end of data bytes. This is similar to the beat of a drum with a speaker talking only when the drum is silent.

CLP Cell Loss Priority: The area in the ATM cell header that determines the likelihood of a cell being dropped during network congestion. Cells with CLP = 0 are considered insured traffic and are not apt to be dropped. Cells with CLP = 1 are considered best-effort traffic that might be dropped during congested episodes, delivering more resources to handle insured traffic.

CLR Cell Loss Ratio: The ratio of discarded cells to successfully delivered cells in ATM. CLR can be designated a QoS parameter when establishing a connection.

CO Central Office: The local telephone company office where all loops in a certain area connect and where circuit switching of subscriber lines occurs.

collapsed backbone A nondistributed backbone where all network segments are connected to each other through an internetworking device. A collapsed backbone can be a virtual network segment at work in a device such as a router, hub, or switch.

collapsed core One switch performing both core and distribution layer functions. Typically found in a small network, the functions of the core and distribution layer are still distinct.

collision The effect of two nodes sending transmissions simultaneously in Ethernet. When they meet on the physical media, the frames from each node collide and are damaged. *See also: collision domain.*

collision domain The network area in Ethernet over which frames that have collided will spread. Collisions are propagated by hubs and repeaters, but not by LAN switches, routers, or bridges. *See also: collision.*

Common Spanning Tree (CST) *See: CST.*

composite metric Used with routing protocols, such as IGRP and EIGRP, that use more than one metric to find the best path to a remote network. IGRP and EIGRP both use bandwidth and delay of the line by default. However, Maximum Transmission Unit (MTU), load, and reliability of a link can be used as well.

compression A technique to send more data across a link than would be normally permitted by representing repetitious strings of data with a single marker.

configuration register A 16-bit configurable value stored in hardware or software that determines how Cisco routers function during initialization. In hardware, the bit position is set by using a jumper. In software, it is set by specifying specific bit patterns used to set startup options, configured by using a hexadecimal value with configuration commands.

congestion Traffic that exceeds the network's capability to handle it.

congestion avoidance To minimize delays, the method an ATM network uses to control traffic entering the system. Lower-priority traffic is discarded at the edge of the network when indicators signal it cannot be delivered, thus using resources efficiently.

congestion collapse The situation that results from the retransmission of packets in ATM networks where little or no traffic successfully arrives at destination points. It usually happens in networks made of switches with ineffective or inadequate buffering capabilities combined with poor packet discard or ABR congestion feedback mechanisms.

connection ID Identifications given to each Telnet session into a router. The `show sessions` command will give you the connections a local router will have to a remote router. The `show users` command will show the connection IDs of users telnetted into your local router.

connectionless Data transfer that occurs without the creation of a virtual circuit. No overhead, best-effort delivery, not reliable. *Contrast with: connection-oriented. See also: virtual circuit.*

connection-oriented Data transfer method that sets up a virtual circuit before any data is transferred. Uses acknowledgments and flow control for reliable data transfer. *Contrast with: connectionless. See also: virtual circuit.*

console port Typically an RJ-45 port on a Cisco router and switch that allows command-line interface capability.

contention media Media access method that is a baseband media—that is, first come, first served. Ethernet is an example of a contention media access.

control direct VCC One of three control connections defined by Phase I LAN Emulation; a bi-directional virtual channel connection (VCC) established in ATM by an LEC to an LES. *See also: control distribute VCC* and *data direct VCC.*

control distribute VCC One of three control connections defined by Phase 1 LAN Emulation; a unidirectional virtual channel connection (VCC) set up in ATM from an LES to an LEC. Usually, the VCC is a point-to-multipoint connection. *See also: control direct VCC* and *data direct VCC.*

convergence The process required for all routers in an internetwork to update their routing tables and create a consistent view of the network, using the best possible paths. No user data is passed during a convergence time.

core block If you have two or more switch blocks, the Cisco rule of thumb states that you need a core block. No routing is performed at the core, only transferring of data. It is a pass-through for the switch block, the server block, and the Internet. The core is responsible for transferring data to and from the switch blocks as quickly as possible. You can build a fast core with a frame, packet, or cell (ATM) network technology.

core layer Top layer in the Cisco three-layer hierarchical model, which helps you design, build, and maintain Cisco hierarchical networks. The core layer passes packets quickly to distribution-layer devices only. No packet filtering should take place at this layer.

cost An arbitrary value, based on hop count, bandwidth, or other calculation, that is typically assigned by a network administrator and used by the routing protocol to compare different routes through an internetwork. Routing protocols use cost values to select the best path to a certain destination: the lowest cost identifies the best path. Also known as "path cost." *See also: routing metric.*

count to infinity A problem occurring in routing algorithms that are slow to converge where routers keep increasing the hop count to particular networks. To avoid this problem, various solutions have been implemented into each of the different routing protocols. Some of those solutions include defining a maximum hop count (defining infinity), route poisoning, poison reverse, and split horizon.

CPCS Common Part Convergence Sublayer: One of two AAL sublayers that is service-dependent, it is further segmented into the CS and SAR sublayers. The CPCS prepares data for transmission across the ATM network; it creates the 48-byte payload cells that are sent to the ATM layer. *See also: AAL* and *ATM layer.*

CPE Customer Premises Equipment: Items such as telephones, modems, and terminals installed at customer locations and connected to the telephone company network.

crankback In ATM, a correction technique used when a node somewhere on a chosen path cannot accept a connection setup request, blocking the request. The path is rolled back to an intermediate node, which then uses GCAC to attempt to find an alternate path to the final destination.

CRC Cyclic redundancy check: A methodology that detects errors, whereby the frame recipient makes a calculation by dividing frame contents with a prime binary divisor and compares the remainder to a value stored in the frame by the sending node. *Compare to: checksum.*

CSMA/CD Carrier Sense Multiple Access/Collision Detect: A technology defined by the Ethernet IEEE 802.3 committee. Each device senses the cable

for a digital signal before transmitting. Also, CSMA/CD allows all devices on the network to share the same cable, but one at a time. If two devices transmit at the same time, a frame collision will occur and a jamming pattern will be sent; the devices will stop transmitting, wait a predetermined amount of time, and then try to transmit again.

CST Common Spanning Tree: One spanning tree instance encompassing every VLAN in the switched network.

CSU Channel Service Unit: A digital mechanism that connects end-user equipment to the local digital telephone loop. Frequently referred to along with the data service unit as "CSU/DSU." *See also: DSU.*

CTD Cell Transfer Delay: For a given connection in ATM, the time period between a cell exit event at the source user-network interface (UNI) and the corresponding cell entry event at the destination. The CTD between these points is the sum of the total inter-ATM transmission delay and the total ATM processing delay.

custom queuing Used by Cisco router IOS to provide a queuing method to slower serial links. Custom queuing enables an administrator to configure the type of traffic that will have priority over the link.

cut-through *See: cut-through frame switching.*

cut-through frame switching A frame-switching technique that flows data through a switch so that the leading edge exits the switch at the output port before the packet finishes entering the input port. Frames will be read, processed, and forwarded by devices that use cut-through switching as soon as the destination address of the frame is confirmed and the outgoing port is identified.

data compression *See: compression.*

data direct VCC A bidirectional point-to-point virtual channel connection (VCC) set up between two LECs in ATM and one of three data connections defined by Phase 1 LAN Emulation. Because data direct VCCs do not guarantee QoS, they are generally reserved for UBR and ABR connections. *See also: control direct VCC* and *control distribute VCC.*

data encapsulation The process in which the information in a protocol is wrapped, or contained, in the data section of another protocol. In the OSI

reference model, each layer encapsulates the layer immediately above it as the data flows down the protocol stack.

data frame Protocol Data Unit encapsulation at the Data Link layer of the OSI reference model. Encapsulates packets from the Network layer and prepares the data for transmission on a network medium.

datagram A logical collection of information transmitted as a Network-layer unit over a medium without a previously established virtual circuit. IP datagrams have become the primary information unit of the Internet. At various layers of the OSI reference model, the terms *cell, frame, message, packet,* and *segment* also define these logical information groupings.

Data Link Control layer Layer 2 of the SNA architectural model, it is responsible for the transmission of data over a given physical link and compares somewhat to the Data Link layer of the OSI model.

Data Link layer Layer 2 of the OSI reference model, it 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. The IEEE has further segmented this layer into the MAC sublayer and the LLC sublayer. Also known as the "Link layer." Can be compared somewhat to the Data Link Control layer of the SNA model. *See also: Application layer, LLC, MAC, Network layer, Physical layer, Presentation layer, Session layer,* and *Transport layer*.

DCC Data Country Code: Developed by the ATM Forum, one of two ATM address formats designed for use by private networks. *Compare to: ICD*.

DCE Data communications equipment (as defined by the EIA) or data circuit-terminating equipment (as defined by the ITU-T): The mechanisms and links of a communications network that make up the network portion of the user-to-network interface, such as modems. The DCE supplies the physical connection to the network, forwards traffic, and provides a clocking signal to synchronize data transmission between DTE and DCE devices. *Compare to: DTE*.

D channel 1) Data channel: A full-duplex, 16Kbps (BRI) or 64Kbps (PRI) ISDN channel. *Compare to: B channel*, *E channel*, and *H channel*. 2) In SNA, anything that provides a connection between the processor and main storage with any peripherals.

DDP Datagram Delivery Protocol: Used in the AppleTalk suite of protocols as a connectionless protocol that is responsible for sending datagrams through an internetwork.

DDR Dial-on-demand routing: A technique that enables a router to automatically initiate and end a circuit-switched session per the requirements of the sending station. By mimicking keep-alives, the router fools the end station into treating the session as active. DDR permits routing over ISDN or telephone lines via a modem or external ISDN terminal adapter.

DE Discard Eligibility: Used in Frame Relay networks to tell a switch that a frame can be discarded if the switch is too busy. The DE is a field in the frame that is turned on by transmitting routers if the Committed Information Rate (CIR) is oversubscribed or set to 0.

DE bit The DE bit marks a frame as discard eligible on a Frame Relay network. If a serial link is congested and the Frame Relay network has passed the Committed Information Rate (CIR), then the DE bit will always be on.

default route The static routing table entry used to direct frames whose next hop is not spelled out in the dynamic routing table.

delay The time elapsed between a sender's initiation of a transaction and the first response they receive. Also, the time needed to move a packet from its source to its destination over a path. *See also: latency.*

demarc The demarcation point between the customer premises equipment (CPE) and the telco's carrier equipment.

demodulation A series of steps that return a modulated signal to its original form. When receiving, a modem demodulates an analog signal to its original digital form (and, conversely, modulates the digital data it sends into an analog signal). *See also: modulation.*

demultiplexing The process of converting a single multiplex signal, comprising more than one input stream, back into separate output streams. *Contrast with: multiplexing.*

denial-of-service attack A denial-of-service attack, or DoS, blocks access to a network resource by saturating the device with attacking data. Typically, this is targeted against the link (particularly lower-bandwidth links) or

the server. DDoS attacks, or distributed denial-of-service attacks, make use of multiple originating attacking resources to saturate a more capable resource.

designated bridge In the process of forwarding a frame from a segment to the route bridge, the bridge with the lowest path cost.

designated ports Used with the Spanning Tree Protocol (STP) to designate forwarding ports. If there are multiple links to the same network, STP will shut down a port to stop network loops.

designated router An OSPF router that creates LSAs for a multi-access network and is required to perform other special tasks in OSPF operations. Multi-access OSPF networks that maintain a minimum of two attached routers identify one router that is chosen by the OSPF Hello protocol, which makes possible a decrease in the number of adjacencies necessary on a multi-access network. This in turn reduces the quantity of routing protocol traffic and the physical size of the database.

destination address The address for the network devices that will receive a packet.

dial backup Dial backup connections are typically used to provide redundancy to Frame Relay connections. The backup link is activated over an analog modem.

digital A digital waveform is one in which distinct ones and zeros provide the data representation. *See also: analog.*

directed broadcast A data frame or packet that is transmitted to a specific group of nodes on a remote network segment. Directed broadcasts are known by their broadcast address, which is a destination subnet address with all the bits turned on. *Compare to: broadcast.*

discovery mode Also known as "dynamic configuration," this technique is used by an AppleTalk interface to gain information from a working node about an attached network. The information is subsequently used by the interface for self-configuration.

distance-vector routing algorithm In order to find the shortest path, this group of routing algorithms repeats on the number of hops in a given route,

requiring each router to send its complete routing table with each update, but only to its neighbors. Routing algorithms of this type tend to generate loops, but they are fundamentally simpler than their link-state counterparts. *See also: link-state routing algorithm* and *SPF*.

distribution layer Middle layer of the Cisco three-layer hierarchical model, which helps you design, install, and maintain Cisco hierarchical networks. The distribution layer is the point where access layer devices connect. Routing is performed at this layer.

distribution list Access list used to filter incoming and outgoing route table entries on a router.

DLCI Data-Link Connection Identifier: Used to identify virtual circuits in a Frame Relay network.

DNS Domain Name System: Used to resolve host names to IP addresses.

DSAP Destination Service Access Point: The service access point of a network node, specified in the destination field of a packet. *See also: SSAP* and *SAP*.

DSL Digital Subscriber Line: DSL technologies are used to provide broadband services over a single copper pair, typically to residential customers. Most vendors are providing DSL services at up to 6Mbps downstream, but the technology can support 52Mbps service.

DSR Data Set Ready: When a DCE is powered up and ready to run, this EIA/TIA-232 interface circuit is also engaged.

DSU Data Service Unit: This device is used to adapt the physical interface on a data terminal equipment (DTE) mechanism to a transmission facility such as T1 or E1 and is also responsible for signal timing. It is commonly grouped with the channel service unit and referred to as the "CSU/DSU." *See also: CSU*.

DTE Data terminal equipment: Any device located at the user end of a user-network interface serving as a destination, a source, or both. DTE includes devices such as multiplexers, protocol translators, and computers. The connection to a data network is made through data channel equipment (DCE) such as a modem, using the clocking signals generated by that device. *Compare to: DCE*.

DTR Data terminal ready: An activated EIA/TIA-232 circuit communicating to the DCE the state of preparedness of the DTE to transmit or receive data.

DUAL Diffusing Update Algorithm: Used in Enhanced IGRP, this convergence algorithm provides loop-free operation throughout an entire route's computation. DUAL grants routers involved in a topology revision the ability to synchronize simultaneously, while routers unaffected by this change are not involved. *See also: Enhanced IGRP.*

DVMRP Distance Vector Multicast Routing Protocol: Based primarily on the Routing Information Protocol (RIP), this Internet gateway protocol implements a common, condensed-mode IP multicast scheme, using IGMP to transfer routing datagrams between its neighbors. *See also: IGMP.*

DXI Data Exchange Interface: Described in RFC 1482, DXI defines the effectiveness of a network device such as a router, bridge, or hub to act as an FEP to an ATM network by using a special DSU that accomplishes packet encapsulation.

dynamic entries Used in layer 2 and 3 devices to dynamically create a table of either hardware addresses or logical addresses.

dynamic routing Also known as "adaptive routing," this technique automatically adapts to traffic or physical network revisions.

dynamic VLAN An administrator will create an entry in a special server with the hardware addresses of all devices on the internetwork. The server will then assign dynamically used VLANs.

E1 Generally used in Europe, a wide-area digital transmission scheme carrying data at 2.048Mbps. E1 transmission lines are available for lease from common carriers for private use.

E.164 1) Evolved from the standard telephone numbering system, the standard recommended by ITU-T for international telecommunication numbering, particularly in ISDN, SMDS, and BISDN. 2) Label of field in an ATM address containing numbers in E.164 format.

E channel Echo channel: A 64Kbps ISDN control channel used for circuit switching. Specific description of this channel can be found in the 1984 ITU-T ISDN specification, but was dropped from the 1988 version. *Compare to: B channel, D channel,* and *H channel.*

edge device A device that enables packets to be forwarded between legacy interfaces (such as Ethernet and Token Ring) and ATM interfaces based on information in the Data Link and Network layers. An edge device does not

take part in the running of any Network-layer routing protocol; it merely uses the route description protocol in order to get the forwarding information required.

EEPROM Electronically erasable programmable read-only memory: Programmed after their manufacture, these non-volatile memory chips can be erased if necessary by using electric power and reprogrammed. *Compare to: EPROM, PROM.*

EFCI Explicit Forward Congestion Indication: A congestion feedback mode permitted by ABR service in an ATM network. The EFCI can be set by any network element that is in a state of immediate or certain congestion. The destination end-system is able to carry out a protocol that adjusts and lowers the cell rate of the connection based on value of the EFCI. *See also: ABR.*

80/20 rule The 80/20 rule means that 80 percent of the users' traffic should remain on the local network segment and only 20 percent or less should cross the routers or bridges to the other network segments.

EIGRP *See: Enhanced IGRP.*

EIP Ethernet Interface Processor: A Cisco 7000 series router interface processor card, supplying 10Mbps AUI ports to support Ethernet Version 1 and Ethernet Version 2 or IEEE 802.3 interfaces with a high-speed data path to other interface processors.

ELAN Emulated LAN: An ATM network configured by using a client/server model in order to emulate either an Ethernet or Token Ring LAN. Multiple ELANs can exist at the same time on a single ATM network and are made up of a LAN emulation client (LEC), a LAN Emulation Server (LES), a Broadcast and Unknown Server (BUS), and a LAN Emulation Configuration Server (LECS). ELANs are defined by the LANE specification. *See also: LANE, LEC, LECS,* and *LES.*

ELAP EtherTalk Link Access Protocol: In an EtherTalk network, the link-access protocol constructed above the standard Ethernet Data Link layer.

enable packets Packets that complete the flow cache. After the MLS-SE determines that the packet meets enable criteria, such as source MAC (SMAC) address and destination IP, the flow cache is established and subsequent packets are layer 3 switched. *See also: MLS-SE, MLS-RP.*

encapsulation The technique used by layered protocols in which a layer adds header information to the Protocol Data Unit (PDU) from the layer above. As an example, in Internet terminology, a packet would contain a header from the Physical layer, followed by a header from the Network layer (IP), followed by a header from the Transport layer (TCP), followed by the application protocol data.

encryption The conversion of information into a scrambled form that effectively disguises it to prevent unauthorized access. Every encryption scheme uses some well-defined algorithm, which is reversed at the receiving end by an opposite algorithm in a process known as decryption.

end-to-end VLAN VLAN that spans the switch-fabric from end to end; all switches in end-to-end VLANs understand about all configured VLANs. End-to-end VLANs are configured to allow membership based on function, project, department, and so on.

Enhanced IGRP Enhanced Interior Gateway Routing Protocol: An advanced routing protocol created by Cisco, combining the advantages of link-state and distance-vector protocols. Enhanced IGRP has superior convergence attributes, including high operating efficiency. *See also: IGP, OSPF,* and *RIP.*

enterprise network A privately owned and operated network that connects most major locations in a large company or organization.

enterprise services Services provided to all users on the internetwork. Layer 3 switches or routers are required in this scenario because the services must be close to the core and would probably be based in their own subnet. Examples of these services include Internet access, e-mail, and possibly videoconferencing. If the servers that host these enterprise services were placed close to the backbone, all users would have the same distance to them, but this also means that all users' data would have to cross the backbone to get to these services.

EPROM Erasable programmable read-only memory: Programmed after their manufacture, these non-volatile memory chips can be erased if necessary by using high-power light and reprogrammed. *Compare to: EEPROM, PROM.*

error correction A process that uses a checksum to detect bit errors in the data stream.

ESF Extended Superframe: Made up of 24 frames with 192 bits each, with the 193rd bit providing other functions including timing. This is an enhanced version of SF. *See also: SF.*

Ethernet A baseband LAN specification created by the Xerox Corporation and then improved through joint efforts of Xerox, Digital Equipment Corporation, and Intel. Ethernet is similar to the IEEE 802.3 series standard and, using CSMA/CD, operates over various types of cables at 10Mbps. Also called "DIX (Digital/Intel/Xerox) Ethernet." *Compare to: FastEthernet. See also: 10BaseT* and *IEEE.*

EtherTalk A Data Link product from Apple Computer that permits AppleTalk networks to be connected by Ethernet.

excess rate In ATM networking, traffic exceeding a connection's insured rate. The excess rate is the maximum rate less the insured rate. Depending on the availability of network resources, excess traffic can be discarded during congestion episodes. *Compare to: maximum rate.*

expansion The procedure of directing compressed data through an algorithm, restoring information to its original size.

expedited delivery An option that can be specified by one protocol layer, communicating either with other layers or with the identical protocol layer in a different network device, requiring that identified data be processed faster.

explorer packet An SNA packet transmitted by a source Token Ring device to find the path through a source-route-bridged network.

extended IP access list IP access list that filters the network by logical address, protocol field in the Network-layer header, and even the port field in the Transport-layer header.

extended IPX access list IPX access list that filters the network by logical IPX address, protocol field in the Network-layer header, or even socket number in the Transport-layer header.

Extended Setup Used in setup mode to configure the router with more detail than Basic Setup mode. Allows multiple-protocol support and interface configuration.

external route processor A router that is external to the switch. An external layer 3 routing device can be used to provide routing between VLANs.

failure domain The region in which a failure has occurred in a Token Ring. When a station gains information that a serious problem, such as a cable break, has occurred with the network, it sends a beacon frame that includes the station reporting the failure, its Next Addressable Upstream Neighbor (NAUN), and everything between. This defines the failure domain. Beaconing then initiates the procedure known as auto-reconfiguration. *See also: auto-reconfiguration* and *beacon*.

fallback In ATM networks, this mechanism is used for scouting a path if it isn't possible to locate one by using customary methods. The device relaxes requirements for certain characteristics, such as delay, in an attempt to find a path that meets a certain set of the most important requirements.

Fast EtherChannel Fast EtherChannel uses load distribution to share the links called a bundle, which is a group of links managed by the Fast EtherChannel process. Should one link in the bundle fail, the Ethernet Bundle Controller (EBC) informs the Enhanced Address Recognition Logic (EARL) ASIC of the failure, and the EARL in turn ages out all addresses learned on that link. The EBC and the EARL use hardware to recalculate the source and destination address pair on a different link.

FastEthernet Any Ethernet specification with a speed of 100Mbps. FastEthernet is 10 times faster than 10BaseT, while retaining qualities such as MAC mechanisms, MTU, and frame format. These similarities make it possible for existing 10BaseT applications and management tools to be used on FastEthernet networks. FastEthernet is based on an extension of IEEE 802.3 specification (IEEE 802.3u). *Compare to: Ethernet. See also: 100BaseT, 100BaseTX,* and *IEEE.*

fast switching A Cisco feature that uses a route cache to speed packet switching through a router. *Compare to: process switching.*

FDM Frequency-Division Multiplexing: A technique that permits information from several channels to be assigned bandwidth on one wire based on frequency. *Contrast with: ATDM, TDM,* and *statistical multiplexing.*

FDDI Fiber Distributed Data Interface: A LAN standard, defined by ANSI X3T9.5 that can run at speeds up to 200Mbps and uses token-passing media access on fiber-optic cable. For redundancy, FDDI can use a dual-ring architecture.

FECN Forward Explicit Congestion Notification: A bit set by a Frame Relay network that informs the DTE receptor that congestion was encountered along the path from source to destination. A device receiving frames

with the FECN bit set can ask higher-priority protocols to take flow-control action as needed. *Contrast with: BECN.*

FEIP FastEthernet Interface Processor: An interface processor employed on Cisco 7000 series routers, supporting up to two 100Mbps 100BaseT ports.

firewall A barrier purposefully erected between any connected public networks and a private network, made up of a router or access server or several routers or access servers, that uses access lists and other methods to ensure the security of the private network.

Flash Electronically erasable programmable read-only memory (EEPROM). Used to hold the Cisco IOS in a router by default.

flash memory Developed by Intel and licensed to other semiconductor manufacturers, it is non-volatile storage that can be erased electronically and reprogrammed, physically located on an EEPROM chip. Flash memory permits software images to be stored, booted, and rewritten as needed. Cisco routers and switches use flash memory to hold the IOS by default. *See also: EPROM, EEPROM.*

flat network A network that is one large collision domain and one large broadcast domain.

flooding When traffic is received on an interface, it is then transmitted to every interface connected to that device with the exception of the interface from which the traffic originated. This technique can be used for traffic transfer by bridges and switches throughout the network.

flow A shortcut or MLS cache entry that is defined by the packet properties. Packets with identical properties belong to the same flow. *See also: MLS.*

flow control A methodology used to ensure that receiving units are not overwhelmed with data from sending devices. Pacing, as it is called in IBM networks, means that when buffers at a receiving unit are full, a message is transmitted to the sending unit to temporarily halt transmissions until all the data in the receiving buffer has been processed and the buffer is again ready for action.

forwarding and filtering decision The decision-making process that a switch goes through to determine which ports to forward a frame out of.

FRAD Frame Relay Access Device: Any device affording a connection between a LAN and a Frame Relay WAN. *See also: Cisco FRAD, FRAS.*

fragment Any portion of a larger packet that has been intentionally segmented into smaller pieces. A packet fragment does not necessarily indicate an error and can be intentional. *See also: fragmentation.*

fragmentation The process of intentionally segmenting a packet into smaller pieces when sending data over an intermediate network medium that cannot support the larger packet size.

FragmentFree LAN switch type that reads into the data section of a frame to make sure fragmentation did not occur. Sometimes called "modified cut-through."

frame A logical unit of information sent by the Data Link layer over a transmission medium. The term often refers to the header and trailer, employed for synchronization and error control, that surround the data contained in the unit.

Frame Relay A more efficient replacement of the X.25 protocol (an unrelated packet relay technology that guarantees data delivery). Frame Relay is an industry-standard, shared-access, best-effort, switched Data-Link layer encapsulation that services multiple virtual circuits and protocols between connected mechanisms.

Frame Relay bridging Defined in RFC 1490, this bridging method uses the identical spanning–tree algorithm as other bridging operations but permits packets to be encapsulated for transmission across a Frame Relay network.

Frame Relay switching A process that occurs when a router at a service provider provides packet switching for Frame Relay packets.

frame tagging VLANs can span multiple connected switches, which Cisco calls a switch-fabric. Switches within this switch-fabric must keep track of frames as they are received on the switch ports, and they must keep track of the VLAN they belong to as the frames traverse this switch-fabric. Frame tagging performs this function. Switches can then direct frames to the appropriate port.

framing Encapsulation at the Data Link layer of the OSI model. It is called framing because the packet is encapsulated with both a header and a trailer.

FRAS Frame Relay Access Support: A feature of Cisco IOS software that enables SDLC, Ethernet, Token Ring, and Frame Relay-attached IBM

devices to be linked with other IBM mechanisms on a Frame Relay network. *See also: FRAD*.

frequency The number of cycles of an alternating current signal per time unit, measured in hertz (cycles per second).

FSIP Fast Serial Interface Processor: The Cisco 7000 routers' default serial interface processor, it provides four or eight high-speed serial ports.

FTP File Transfer Protocol: The TCP/IP protocol used for transmitting files between network nodes, it supports a broad range of file types and is defined in RFC 959. *See also: TFTP*.

full duplex The capacity to transmit information between a sending station and a receiving unit at the same time. *See also: half duplex*.

full mesh A type of network topology in which every node has either a physical or a virtual circuit linking it to every other network node. A full mesh supplies a great deal of redundancy but is typically reserved for network backbones because of its expense. *See also: partial mesh*.

Gigabit EtherChannel *See: Fast EtherChannel.*

Gigabit Ethernet 1000Mbps version of the IEEE 802.3. FastEthernet offers a speed increase of 10 times that of the 10BaseT Ethernet specification while preserving qualities such as frame format, MAC, mechanisms, and MTU.

GNS Get Nearest Server: On an IPX network, a request packet sent by a customer for determining the location of the nearest active server of a given type. An IPX network client launches a GNS request to get either a direct answer from a connected server or a response from a router disclosing the location of the service on the internetwork to the GNS. GNS is part of IPX and SAP. *See also: IPX* and *SAP*.

grafting A process that activates an interface that has been deactivated by the pruning process. It is initiated by an IGMP membership report sent to the router.

GRE Generic Routing Encapsulation: A tunneling protocol created by Cisco with the capacity for encapsulating a wide variety of protocol packet types inside IP tunnels, thereby generating a virtual point-to-point connection to Cisco routers across an IP network at remote points. IP tunneling using GRE permits network expansion across a single-protocol backbone

environment by linking multiprotocol subnetworks in a single-protocol backbone environment.

Group of Four Used by Cisco Local Management Interface on Frame Relay networks to manage the permanent virtual circuits (PVCs). *See also: PVC.*

guard band The unused frequency area found between two communications channels, furnishing the space necessary to avoid interference between the two.

half duplex The capacity to transfer data in only one direction at a time between a sending unit and a receiving unit. *See also: full duplex.*

handshake Any series of transmissions exchanged between two or more devices on a network to ensure synchronized operations.

H channel High-speed channel: A full-duplex, ISDN primary rate channel operating at a speed of 384Kbps. *Compare to: B channel, D channel,* and *E channel.*

HDLC High-Level Data Link Control: Using frame characters, including checksums, HDLC designates a method for data encapsulation on synchronous serial links and is the default encapsulation for Cisco routers. HDLC is a bit-oriented synchronous Data Link–layer protocol created by ISO and derived from SDLC. However, most HDLC vendor implementations (including Cisco's) are proprietary. *See also: SDLC.*

helper address The unicast address specified, which instructs the Cisco router to change the client's local broadcast request for a service into a directed unicast to the server.

hierarchical addressing Any addressing plan employing a logical chain of commands to determine location. IP addresses are made up of a hierarchy of network numbers, subnet numbers, and host numbers to direct packets to the appropriate destination.

hierarchical network A multi-segment network configuration providing only one path through intermediate segments, between source segments and destination segments.

hierarchy *See: hierarchical network.*

HIP HSSI Interface Processor: An interface processor used on Cisco 7000 series routers, providing one HSSI port that supports connections to ATM, SMDS, Frame Relay, or private lines at speeds up to T3 or E3.

holddown The state a route is placed in so that routers can neither advertise the route nor accept advertisements about it for a defined time period. Holddown is used to surface bad information about a route from all routers in the network. A route is generally placed in holddown when one of its links fails.

hop The movement of a packet between any two network nodes. *See also: hop count.*

hop count A routing metric that calculates the distance between a source and a destination. RIP employs hop count as its sole metric. *See also: hop* and *RIP.*

host address Logical address configured by an administrator or server on a device. Logically identifies this device on an internetwork.

HSCI High-Speed Communication Interface: Developed by Cisco, a single-port interface that provides full-duplex synchronous serial communications capability at speeds up to 52Mbps.

HSRP Hot Standby Routing Protocol: A protocol that provides high network availability and provides nearly instantaneous hardware failover without administrator intervention. It generates a Hot Standby router group, including a lead router that lends its services to any packet being transferred to the Hot Standby address. If the lead router fails, it will be replaced by any of the other routers—the standby routers—that monitor it.

HSSI High-Speed Serial Interface: A network standard physical connector for high-speed serial linking over a WAN at speeds of up to 52Mbps.

hub Physical-layer devices that are really just multiple port repeaters. When an electronic digital signal is received on a port, the signal is reamplified or regenerated and forwarded out all segments except the segment from which the signal was received.

ICD International Code Designator: Adapted from the subnetwork model of addressing, this assigns the mapping of Network-layer addresses to ATM addresses. HSSI is one of two ATM formats for addressing created by the ATM Forum to be utilized with private networks. *Compare to: DCC.*

ICMP Internet Control Message Protocol: Documented in RFC 792, it is a Network-layer Internet protocol for the purpose of reporting errors and providing information pertinent to IP packet procedures.

IEEE Institute of Electrical and Electronics Engineers: A professional organization that, among other activities, defines standards in a number of fields

within computing and electronics, including networking and communications. IEEE standards are the predominant LAN standards used today throughout the industry. Many protocols are commonly known by the reference number of the corresponding IEEE standard.

IEEE 802.1 The IEEE committee specification that defines the bridging group. The specification for STP (Spanning Tree Protocol) is IEEE 802.1d. The STP uses SPA (spanning-tree algorithm) to find and prevent network loops in bridged networks. The specification for VLAN trunking is IEEE 802.1q.

IEEE 802.3 The IEEE committee specification that defines the Ethernet group, specifically the original 10Mbps standard. Ethernet is a LAN protocol that specifies Physical-layer and MAC-sublayer media access. IEEE 802.3 uses CSMA/CD to provide access for many devices on the same network. FastEthernet is defined as 802.3u, and Gigabit Ethernet is defined as 802.3q. *See also: CSMA/CD*.

IEEE 802.5 IEEE committee that defines Token Ring media access.

IGMP Internet Group Management Protocol: Employed by IP hosts, the protocol that reports their multicast group memberships to an adjacent multicast router. The first version, IGMPv1, enables hosts to subscribe to or join specified multicast groups. Enhancements were made to IGMPv2 to facilitate a host-initiated leave process.

IGMP Snooping An extension to CGMP, IGMP Snooping enables the switch to make multicast decisions directly, without the intervention of a router.

IGMP Join process The process by which hosts may join a multicast session outside of the Membership Query interval.

IGMP Leave process IGMPv1 does not have a formal leave process; a period of three query intervals must pass with no host confirmation before the interface is deactivated. IGMPv2 does allow the host to initiate the leave process immediately.

IGMP Query process The router uses IGMP to query hosts for Membership Reports, thus managing multicast on its interfaces.

IGP Interior Gateway Protocol: Any protocol used by the Internet to exchange routing data within an independent system. Examples include RIP, IGRP, and OSPF.

ILMI Integrated (or Interim) Local Management Interface. A specification created by the ATM Forum, designated for the incorporation of network-management capability into the ATM UNI. Integrated Local Management Interface cells provide for automatic configuration between ATM systems. In LAN emulation, ILMI can provide sufficient information for the ATM end station to find an LECS. In addition, ILMI provides the ATM NSAP (Network Service Access Point) prefix information to the end station.

in-band *See: in-band management.*

in-band management The management of a network device "through" the network. Examples include using Simple Network Management Protocol (SNMP) or Telnet directly via the local LAN. *Compare to: out-of-band management.*

in-band signaling Configuration of a router from within the network. Examples are Telnet, Simple Network Management Protocol (SNMP), or a Network Management Station (NMS).

insured burst In an ATM network, it is the largest, temporarily permitted data burst exceeding the insured rate on a PVC and not tagged by the traffic policing function for being dropped if network congestion occurs. This insured burst is designated in bytes or cells. *Compare to: maximum burst.*

interarea routing Routing between two or more logical areas. *Compare to: intra-area routing. See also: area.*

interface processor Any of several processor modules used with Cisco 7000 series routers. *See also: AIP, CIP, EIP, FEIP, HIP, MIP,* and *TRIP.*

internal route processor Route Switch Modules (RSMs) and Route Switch Feature Cards (RSFCs) are called internal route processors because the processing of layer 3 packets is internal to a switch.

Internet The global "network of networks," whose popularity has exploded in the last few years. Originally a tool for collaborative academic research, it has become a medium for exchanging and distributing information of all kinds. The Internet's need to link disparate computer platforms and technologies has led to the development of uniform protocols and standards that have also found widespread use within corporate LANs. *See also: TCP/IP* and *MBONE.*

internet Before the rise in the use of the Internet, this lowercase form was shorthand for "internetwork" in the generic sense. Now rarely used. *See also: internetwork*.

Internet protocol Any protocol belonging to the TCP/IP protocol stack. *See also: TCP/IP*.

internetwork Any group of private networks interconnected by routers and other mechanisms, typically operating as a single entity.

internetworking Broadly, anything associated with the general task of linking networks to each other. The term encompasses technologies, procedures, and products. When you connect networks to a router, you are creating an internetwork.

inter-VLAN routing Cisco has created the proprietary protocol Inter-Switch Link (ISL) to allow routing between VLANs with only one Ethernet interface. To run ISL, you need to have two VLAN-capable FastEthernet or Gigabit Ethernet devices, such as a Cisco 5000 switch and a 7000 series router.

intra-area routing Routing that occurs within a logical area. *Compare to: interarea routing*.

intruder detection A system that operates by monitoring the data flow for characteristics consistent with security threats. In this manner, an intruder can be monitored or blocked from access. One trigger for an intruder detection system is multiple ping packets from a single resource in a brief period of time.

Inverse ARP Inverse Address Resolution Protocol: A technique by which dynamic mappings are constructed in a network, enabling a device such as a router to locate the logical network address and associate it with a permanent virtual circuit (PVC). Commonly used in Frame Relay to determine the far-end node's TCP/IP address by sending the Inverse ARP request to the local DLCI.

IP Internet Protocol: Defined in RFC 791, it is a Network-layer protocol that is part of the TCP/IP stack and allows connectionless service. IP furnishes an array of features for addressing, type-of-service specification, fragmentation and reassembly, and security.

IP address Often called an "Internet address," this is an address uniquely identifying any device (host) on the Internet (or any TCP/IP network). Each address consists of four octets (32 bits), represented as decimal numbers

separated by periods (a format known as "dotted-decimal"). Every address is made up of a network number, an optional subnetwork number, and a host number. The network and subnetwork numbers together are used for routing, while the host number addresses an individual host within the network or subnetwork. The network and subnetwork information is extracted from the IP address by using the subnet mask. There are five classes of IP addresses (A–E), which allocate different numbers of bits to the network, subnetwork, and host portions of the address. *See also: CIDR, IP,* and *subnet mask*.

IPCP IP Control Program: The protocol used to establish and configure IP over PPP. *See also: IP* and *PPP*.

IP multicast A technique for routing that enables IP traffic to be reproduced from one source to several endpoints or from multiple sources to many destinations. Instead of transmitting only one packet to each individual point of destination, one packet is sent to a multicast group specified by only one IP endpoint address for the group.

IPX Internetwork Packet Exchange: Network-layer protocol (layer 3) used in Novell NetWare networks for transferring information from servers to workstations. Similar to IP and XNS.

IPXCP IPX Control Program: The protocol used to establish and configure IPX over PPP. *See also: IPX and PPP*.

IPX spoofing Provides IPX RIP/SAP traffic without requiring a connection to the opposing network. This allows a per-minute tariffed link, such as ISDN or analog phone, to support IPX without requiring the link to remain active.

IPXWAN Protocol used for new WAN links to provide and negotiate line options on the link by using IPX. After the link is up and the options have been agreed upon by the two end-to-end links, normal IPX transmission begins.

IRDP ICMP Router Discovery Protocol: Enables hosts to use the Internet Control Message Protocol (ICMP) to find a new path when the primary router becomes unavailable. IRDP is an extension to the ICMP protocol and not a dynamic routing protocol. This ICMP extension allows routers to advertise default routes to end stations.

ISDN Integrated Services Digital Network: Offered as a service by telephone companies, a communication protocol that allows telephone networks to carry data, voice, and other digital traffic. *See also: BISDN, BRI,* and *PRI*.

ISL routing Inter-Switch Link routing is a Cisco proprietary method of frame tagging in a switched internetwork. Frame tagging is a way to identify the VLAN membership of a frame as it traverses a switched internetwork.

isochronous transmission Asynchronous data transfer over a synchronous data link, requiring a constant bit rate for reliable transport. *Contrast with: asynchronous transmission* and *synchronous transmission.*

ITU-T International Telecommunication Union Telecommunication Standardization Sector: A group of engineers who develop worldwide standards for telecommunications technologies.

LAN Local area network: Broadly, any network linking two or more computers and related devices within a limited geographical area (up to a few kilometers). LANs are typically high-speed, low-error networks within a company. Cabling and signaling at the physical and Data Link layers of the OSI are dictated by LAN standards. Ethernet, FDDI, and Token Ring are among the most popular LAN technologies. *Compare to: MAN.*

LANE LAN emulation: The technology that enables an ATM network to operate as a LAN backbone. To do so, the ATM network is required to provide multicast and broadcast support, address mapping (MAC-to-ATM), SVC management, in addition to an operable packet format. Additionally, LANE defines Ethernet and Token Ring ELANs. *See also: ELAN.*

LAN switch A high-speed, multiple-interface transparent bridging mechanism, transmitting packets between segments of data links, usually referred to specifically as an Ethernet switch. LAN switches transfer traffic based on MAC addresses. Multi-layer switches are a type of high-speed, special-purpose, hardware-based router. *See also: multi-layer switch* and *store-and-forward packet switching.*

LAPB Link Accessed Procedure, Balanced: A bit-oriented Data Link–layer protocol that is part of the X.25 stack and has its origin in SDLC. *See also: SDLC* and *X.25.*

LAPD Link Access Procedure on the D channel. The ISDN Data Link–layer protocol used specifically for the D channel and defined by ITU-T Recommendations Q.920 and Q.921. LAPD evolved from LAPB and is created to comply with the signaling requirements of ISDN basic access.

latency Broadly, the time it takes a data packet to get from one location to another. In specific networking contexts, it can mean either 1) the time

elapsed (delay) between the execution of a request for access to a network by a device and the time the mechanism actually is permitted transmission, or 2) the time elapsed between when a mechanism receives a frame and the time that frame is forwarded out of the destination port.

layer 2 switching Layer 2 switching is hardware based, which means it uses the MAC address from the hosts' NIC cards to filter the network. Switches use Application-Specific Integrated Circuits (ASICs) to build and maintain filter tables. It is OK to think of a layer 2 switch as a multiport bridge.

layer 3 switch *See: multi-layer switch.*

layer 3 switching A switching decision made with a layer 3 address as opposed to a MAC address.

layer 4 switching A switching decision made with port and protocol or IPX socket information in addition to a layer 3 address.

layered architecture Industry standard way of creating applications to work on a network. Layered architecture allows the application developer to make changes in only one layer instead of the whole program.

LCP Link Control Protocol: The protocol designed to establish, configure, and test Data Link connections for use by PPP. *See also: PPP.*

leaky bucket An analogy for the basic cell rate algorithm (GCRA) used in ATM networks for checking the conformance of cell flows from a user or network. The bucket's "hole" is understood to be the prolonged rate at which cells can be accommodated, and the "depth" is the tolerance for cell bursts over a certain time period.

learning bridge A bridge that transparently builds a dynamic database of MAC addresses and the interfaces associated with each address. Transparent bridges help to reduce traffic congestion on the network.

LE ARP LAN Emulation Address Resolution Protocol: The protocol providing the ATM address that corresponds to a MAC address.

leased lines Permanent connections between two points leased from the telephone companies.

LEC LAN Emulation Client: Software providing the emulation of the Link layer interface that allows the operation and communication of all higher-level protocols and applications to continue. The LEC client runs in all ATM

devices, which include hosts, servers, bridges, and routers. The LANE client is responsible for address resolution, data transfer, address caching, interfacing to the emulated LAN, and driver support for higher-level services. *See also: ELAN* and *LES*.

LECS LAN Emulation Configuration Server: An important part of emulated LAN services, providing the configuration data that is furnished upon request from the LES. These services include address registration for Integrated Local Management Interface (ILMI) support, configuration support for the LES addresses and their corresponding emulated LAN identifiers, and an interface to the emulated LAN. *See also: LES* and *ELAN*.

LES LAN Emulation Server: The central LANE component that provides the initial configuration data for each connecting LEC. The LES typically is located on either an ATM-integrated router or a switch. Responsibilities of the LES include configuration and support for the LEC, address registration for the LEC, database storage and response concerning ATM addresses, and interfacing to the emulated LAN *See also: ELAN, LEC,* and *LECS*.

link compression *See: compression.*

link-state routing algorithm A routing algorithm that enables each router to broadcast or multicast information regarding the cost of reaching all its neighbors to every node in the internetwork. Link-state algorithms provide a consistent view of the network and are therefore not vulnerable to routing loops. However, this is achieved at the cost of somewhat greater difficulty in computation and more widespread traffic (compared with distance-vector routing algorithms). *See also: distance-vector routing algorithm.*

LLAP LocalTalk Link Access Protocol: In a LocalTalk environment, the Data Link–level protocol that manages node-to-node delivery of data. This protocol provides node addressing and management of bus access, and it also controls data sending and receiving to assure packet length and integrity.

LLC Logical Link Control: Defined by the IEEE, the higher of two Data Link–layer sublayers. LLC is responsible for error detection (but not correction), flow control, framing, and software-sublayer addressing. The predominant LLC protocol, IEEE 802.2, defines both connectionless and connection-oriented operations. *See also: Data Link layer* and *MAC*.

LMI An enhancement to the original Frame Relay specification. Among the features it provides are a keep-alive mechanism, a multicast mechanism, global addressing, and a status mechanism.

LNNI LAN Emulation Network-to-Network Interface: In the Phase 2 LANE specification, an interface that supports communication between the server components within one ELAN.

local explorer packet In a Token Ring SRB network, a packet generated by an end system to find a host linked to the local ring. If no local host can be found, the end system will produce one of two solutions: a spanning explorer packet or an all-routes explorer packet.

local loop Connection from a demarcation point to the closest switching office.

local services Users trying to get to network services that are located on the same subnet or network are defined as local services. Users do not cross layer 3 devices, and the network services are in the same broadcast domain as the users. This type of traffic never crosses the backbone.

LocalTalk Utilizing CSMA/CD, in addition to supporting data transmission at speeds of 230.4Kbps, LocalTalk is Apple Computer's proprietary baseband protocol, operating at the Data Link and Physical layers of the OSI reference model.

local VLAN A VLAN configured by geographic location; this location can be a building or just a closet in a building, depending on switch size. Geographically configured VLANs are designed around the fact that the business or corporation is using centralized resources, such as a server farm.

loop avoidance If multiple connections between switches are created for redundancy, network loops can occur. STP is used to stop network loops and allow redundancy.

LSA Link State Advertisement: Contained inside of link-state packets (LSPs), these advertisements are usually multicast packets, containing information about neighbors and path costs, that are employed by link-state protocols. Receiving routers use LSAs to maintain their link-state databases and, ultimately, routing tables.

LUNI LAN Emulation User-to-Network Interface: Defining the interface between the LAN Emulation Client (LEC) and the LAN Emulation Server,

LUNI is the ATM Forum's standard for LAN Emulation on ATM networks. *See also: LES* and *LECS*.

LZW algorithm A data compression process named for its inventors, Lempel, Ziv, and Welch. The algorithm works by finding longer and longer strings of data to compress with shorter representations.

MAC Media Access Control: The lower sublayer in the Data Link layer, it is responsible for hardware addressing, media access, and error detection of frames. *See also: Data Link layer* and *LLC*.

MAC address A Data Link–layer hardware address that every port or device needs in order to connect to a LAN segment. These addresses are used by various devices in the network for accurate location of logical addresses. MAC addresses are defined by the IEEE standard, and their length is six characters, typically using the burned-in address (BIA) of the local LAN interface. Variously called "hardware address," "physical address," "burned-in address," or "MAC-layer address."

MacIP In AppleTalk, the Network-layer protocol encapsulating IP packets in Datagram Delivery Protocol (DDP) packets. MacIP also supplies substitute ARP services.

MAN Metropolitan area network: Any network that encompasses a metropolitan area; that is, an area typically larger than a LAN but smaller than a WAN. *Compare to: LAN*.

Manchester encoding A method for digital coding in which a mid-bit–time transition is employed for clocking, and a 1 (one) is denoted by a high voltage level during the first half of the bit time. This scheme is used by Ethernet and IEEE 802.3.

maximum burst Specified in bytes or cells, the largest burst of information exceeding the insured rate that will be permitted on an ATM permanent virtual connection for a short time and will not be dropped even if it goes over the specified maximum rate. *Compare to: insured burst. See also: maximum rate*.

maximum rate The maximum permitted data throughput on a particular virtual circuit, equal to the total of insured and uninsured traffic from the traffic source. Should traffic congestion occur, uninsured information might be deleted from the path. Measured in bits or cells per second, the maximum

rate represents the highest throughput of data that the virtual circuit is ever able to deliver and cannot exceed the media rate. *Compare to: excess rate. See also: maximum burst.*

MBS Maximum Burst Size: In an ATM signaling message, this metric, coded as a number of cells, is used to convey the burst tolerance.

MBONE Multicast backbone: The multicast backbone of the Internet, it is a virtual multicast network made up of multicast LANs, including point-to-point tunnels interconnecting them.

MCDV Maximum Cell Delay Variation: The maximum two-point CDV objective across a link or node for the identified service category in an ATM network. The MCDV is one of four link metrics that are exchanged by using PTSPs to verify the available resources of an ATM network. Only one MCDV value is assigned to each traffic class.

MCLR Maximum Cell Loss Ratio: The maximum ratio of cells in an ATM network that fail to transit a link or node compared with the total number of cells that arrive at the link or node. MCDV is one of four link metrics that are exchanged using PTSPs to verify the available resources of an ATM network. The MCLR applies to cells in VBR and CBR traffic classes whose CLP bit is set to zero. *See also: CBR, CLP,* and *VBR.*

MCR Minimum Cell Rate: A parameter determined by the ATM Forum for traffic management of the ATM networks. MCR is specifically defined for ABR transmissions and specifies the minimum value for the allowed cell rate (ACR). *See also: ACR* and *PCR.*

MCTD Maximum Cell Transfer Delay: In an ATM network, the total of the maximum cell delay variation and the fixed delay across the link or node. MCTD is one of four link metrics that are exchanged by using PNNI topology state packets to verify the available resources of an ATM network. There is one MCTD value assigned to each traffic class. *See also: MCDV.*

MIB Management Information Base: Used with SNMP management software to gather information from remote devices. The management station can poll the remote device for information, or the MIB running on the remote station can be programmed to send information on a regular basis.

MIP Multichannel Interface Processor: The resident interface processor on Cisco 7000 series routers, providing up to two channelized T1 or E1

connections by serial cables connected to a CSU. The two controllers are capable of providing 24 T1 or 30 E1 channel groups, with each group being introduced to the system as a serial interface that can be configured individually.

mips Millions of instructions per second: A measure of processor speed.

MLP Multilink PPP: A technique used to split, recombine, and sequence datagrams across numerous logical data links.

MLS Multi-Layer Switching: Switching typically takes place at layer 2. When layer 3 information is allowed to be cached, layer 2 devices have the capability of rewriting and forwarding frames based on the layer 3 information.

MLSP Multi-layer Switching Protocol: A protocol that runs on the router and enables it to communicate to the MLS-SE regarding topology or security changes.

MLS-RP Multi-layer Switching Route Processor: An MLS-capable router or an RSM (Route Switch Module) installed in the switch. *See also: RSM, MLS.*

MLS-SE Multi-layer Switching Switch Engine: An MLS-capable switch (a 5000 with an NFFC or a 6000 with an MSFC and PFC). *See also: MLS, NFFC, MSFC, PFC.*

MMP Multichassis Multilink PPP: A protocol that supplies MLP support across multiple routers and access servers. MMP enables several routers and access servers to work as a single, large dial-up pool with one network address and ISDN access number. MMP successfully supports packet fragmenting and reassembly when the user connection is split between two physical access devices.

modem Modulator-demodulator: A device that converts digital signals to analog and vice-versa so that digital information can be transmitted over analog communication facilities, such as voice-grade telephone lines. This is achieved by converting digital signals at the source to analog for transmission and reconverting the analog signals back into digital form at the destination. *See also: modulation* and *demodulation.*

modemcap database Stores modem initialization strings on the router for use in auto-detection and configuration.

modem eliminator A mechanism that makes possible a connection between two DTE devices without modems by simulating the commands and physical signaling required.

modulation The process of modifying some characteristic of an electrical signal, such as amplitude (AM) or frequency (FM), in order to represent digital or analog information. *See also: AM.*

MOSPF Multicast OSPF: An extension of the OSPF unicast protocol that enables IP multicast routing within the domain. *See also: OSPF.*

MP bonding MultiPoint bonding: A process of linking two or more physical connections into a single logical channel. This might use two or more analog lines and two or more modems, for example.

MPOA Multiprotocol over ATM: An effort by the ATM Forum to standardize how existing and future Network-layer protocols such as IP, Ipv6, AppleTalk, and IPX run over an ATM network with directly attached hosts, routers, and multi-layer LAN switches.

MSFC Multi-layer Switch Feature Card: A route processor (parallel to an RSM, or Route Switch Module) that is installed as a daughter card on Cisco Catalyst 6000 series switches. *See also: RSM.*

mtrace (multicast traceroute) Used to establish the SPT for a specified multicast group.

MTU Maximum transmission unit: The largest packet size, measured in bytes, that an interface can handle.

multicast Broadly, any communication between a single sender and multiple receivers. Unlike broadcast messages, which are sent to all addresses on a network, multicast messages are sent to a defined subset of the network addresses; this subset has a group multicast address, which is specified in the packet's destination address field. *See also: broadcast, directed broadcast.*

multicast address A single address that points to more than one device on the network by specifying a special nonexistent MAC address in that particular multicast protocol. Identical to group address. *See also: multicast.*

multicast group A group set up to receive messages from a source. These groups can be established based on Frame Relay or IP in the TCP/IP protocol suite, as well as other networks.

multicast send VCC A two-directional point-to-point virtual channel connection (VCC) arranged by an LEC to a BUS, it is one of the three types

of informational link specified by phase 1 LANE. *See also: control distribute VCC* and *control direct VCC.*

multi-layer switch A highly specialized, high-speed, hardware-based type of LAN router, the device filters and forwards packets based on their layer 2 MAC addresses and layer 3 network addresses. It's possible that even layer 4 can be read. Sometimes called a "layer 3 switch." *See also: LAN switch.*

Multi-Layer Switching Multi-Layer Switching combines layer 2, 3, and 4 switching technology and provides very high-speed scalability with low latency. This is provided by huge filter tables based on the criteria designed by the network administrator.

multiplexing The process of converting several logical signals into a single physical signal for transmission across one physical channel. *Contrast with: demultiplexing.*

NAK Negative acknowledgment: A response sent from a receiver, telling the sender that the information was not received or contained errors. *Contrast with: acknowledgment.*

NAT Network Address Translation: An algorithm instrumental in minimizing the requirement for globally unique IP addresses, permitting an organization whose addresses are not all globally unique to connect to the Internet, regardless, by translating those addresses into globally routable address space.

NBP Name Binding Protocol: In AppleTalk, the Transport-level protocol that interprets a socket client's name, entered as a character string, into the corresponding DDP address. NBP gives AppleTalk protocols the capacity to discern user-defined zones and names of mechanisms by showing and keeping translation tables that map names to their corresponding socket addresses.

NCP Network Control Protocol: A protocol at the Logical Link Control sublayer of the Data Link layer used in the PPP stack. It is used to enable multiple Network-layer protocols to run over a nonproprietary HDLC serial encapsulation.

neighboring routers Two routers in OSPF that have interfaces to a common network. On networks with multi-access, these neighboring routers are dynamically discovered by using the Hello protocol of OSPF.

NetBEUI NetBIOS Extended User Interface: An improved version of the NetBIOS protocol used in a number of network operating systems including LAN Manager, Windows NT, LAN Server, and Windows for Workgroups, implementing the OSI LLC2 protocol. NetBEUI formalizes the transport frame not standardized in NetBIOS and adds more functions. *See also: OSI.*

NetBIOS Network Basic Input/Output System: The API employed by applications residing on an IBM LAN to ask for services, such as session termination or information transfer, from lower-level network processes.

NetView A mainframe network product from IBM, used for monitoring SNA (Systems Network Architecture) networks. It runs as a VTAM (Virtual Telecommunications Access Method) application.

NetWare A widely used NOS created by Novell, providing a number of distributed network services and remote file access.

network address Used with the logical network addresses to identify the network segment in an internetwork. Logical addresses are hierarchical in nature and have at least two parts: network and host. An example of a hierarchical address is 172.16.10.5, where 172.16 is the network and 10.5 is the host address.

Network layer In the OSI reference model, it is layer 3—the layer in which routing is implemented, enabling connections and path selection between two end systems. *See also: Application layer, Data Link layer, Physical layer, Presentation layer, Session layer,* and *Transport layer.*

NFFC NetFlow Feature Card: A module installed on Cisco Catalyst 5000 series switches. It is capable of examining each frame's IP header as well as the Ethernet header. This in turn enables the NFFC to create flows.

NFS Network File System: One of the protocols in Sun Microsystems' widely used file system protocol suite, allowing remote file access across a network. The name is loosely used to refer to the entire Sun protocol suite, which also includes RPC, XDR (External Data Representation), and other protocols.

NHRP Next Hop Resolution Protocol: In a nonbroadcast multi-access (NBMA) network, the protocol employed by routers in order to dynamically locate MAC addresses of various hosts and routers. It enables systems to communicate directly without requiring an intermediate hop, thus facilitating increased performance in ATM, Frame Relay, X.25, and SMDS systems.

NHS Next Hop Server: Defined by the NHRP protocol, this server maintains the next-hop resolution cache tables, listing IP-to-ATM address maps of related nodes and nodes that can be reached through routers served by the NHS.

NIC Network interface card: An electronic circuit board placed in a computer. The NIC provides network communication to a LAN.

NLSP NetWare Link Services Protocol: Novell's link-state routing protocol, based on the IS-IS model.

NMP Network Management Processor: A Catalyst 5000 switch processor module used to control and monitor the switch.

node address Used to identify a specific device in an internetwork. Can be a hardware address, which is burned into the network interface card or a logical network address, which an administrator or server assigns to the node.

nondesignated ports The Spanning Tree Protocol tells a port on a layer 2 switch to stop transmitting, stopping a network loop. Only designated ports can send frames.

non-stub area In OSPF, a resource-consuming area carrying a default route, intra-area routes, interarea routes, static routes, and external routes. Non-stub areas are the only areas that can have virtual links configured across them and exclusively contain an autonomous system boundary router (ASBR). *Compare to: stub area. See also: ASBR* and *OSPF.*

NRZ Nonreturn to Zero: One of several encoding schemes for transmitting digital data. NRZ signals sustain constant levels of voltage with no signal shifting (no return to zero-voltage level) during a bit interval. If there is a series of bits with the same value (1 or 0), there will be no state change. The signal is not self-clocking. *See also: NRZI.*

NRZI Nonreturn to Zero Inverted: One of several encoding schemes for transmitting digital data. A transition in voltage level (either from high to low or vice-versa) at the beginning of a bit interval is interpreted as a value of 1; the absence of a transition is interpreted as a 0. Thus, the voltage assigned to each value is continually inverted. NRZI signals are not self-clocking. *See also: NRZ.*

NT1 Network termination 1: An ISDN designation to devices that understand ISDN standards.

NT2 Network termination 2: An ISDN designation to devices that do not understand ISDN standards. To use an NT2, you must use a terminal adapter (TA).

NVRAM Non-volatile RAM: Random-access memory that keeps its contents intact while power is turned off.

OC Optical Carrier: A series of physical protocols, designated as OC-1, OC-2, OC-3, and so on, for SONET optical signal transmissions. OC signal levels place STS frames on a multi-mode fiber-optic line at various speeds, of which 51.84Mbps is the lowest (OC-1). Each subsequent protocol runs at a speed divisible by 51.84. *See also: SONET.*

octet Base-8 numbering system used to identify a section of a dotted decimal IP address. Also referred to as a byte.

100BaseT Based on the IEEE 802.3u standard, 100BaseT is the Fast Ethernet specification of 100Mbps baseband that uses UTP wiring. 100BaseT sends link pulses (containing more information than those used in 10BaseT) over the network when no traffic is present. *See also: 10BaseT, FastEthernet,* and *IEEE 802.3.*

100BaseTX Based on the IEEE 802.3u standard, 100BaseTX is the 100Mbps baseband FastEthernet specification that uses two pairs of UTP or STP wiring. The first pair of wires receives data; the second pair sends data. To ensure correct signal timing, a 100BaseTX segment cannot be longer than 100 meters.

ones density Also known as "pulse density," this is a method of signal clocking. The CSU/DSU retrieves the clocking information from data that passes through it. For this scheme to work, the data needs to be encoded to contain at least one binary 1 for each eight bits transmitted. *See also: CSU* and *DSU.*

one-time challenge tokens Used to provide a single use password. This prevents replay attacks and snooping; however, it also requires the user to have a device that provides the token. This physical component of the security model works to prevent hackers from guessing or obtaining the user's password.

OSI Open Systems Interconnection: International standardization program designed by ISO and ITU-T for the development of data networking standards that make multivendor equipment interoperability a reality.

OSI reference model Open Systems Interconnection reference model: A conceptual model defined by the International Organization for Standardization (ISO), describing how any combination of devices can be connected for the purpose of communication. The OSI model divides the task into seven functional layers, forming a hierarchy with the applications at the top and the physical medium at the bottom, and it defines the functions each layer must provide. *See also: Application layer, Data Link layer, Network layer, Physical layer, Presentation layer, Session layer,* and *Transport layer.*

OSPF Open Shortest Path First: A link-state, hierarchical IGP routing algorithm derived from an earlier version of the IS-IS protocol, whose features include multipath routing, load balancing, and least-cost routing. OSPF is the suggested successor to RIP in the Internet environment. *See also: Enhanced IGRP, IGP,* and *IP.*

OUI Organizationally Unique Identifier: An identifier assigned by the IEEE to an organization that makes network interface cards. The organization then puts this OUI on each and every card they manufacture. The OUI is 3 bytes (24 bits) long. The manufacturer then adds a 3-byte identifier to uniquely identify the host on an internetwork. The total length of the address is 48 bits (6 bytes) and is called a hardware address or MAC address.

out-of-band management Management "outside" of the network's physical channels. For example, using a console connection not directly interfaced through the local LAN or WAN or a dial-in modem. *Compare to: in-band management.*

out-of-band signaling Within a network, any transmission that uses physical channels or frequencies separate from those ordinarily used for data transfer. For example, the initial configuration of a Cisco Catalyst switch requires an out-of-band connection via a console port.

packet In data communications, the basic logical unit of information transferred. A packet consists of a certain number of data bytes, wrapped or encapsulated in headers and/or trailers that contain information about where the packet came from, where it's going, and so on. The various protocols involved in sending a transmission add their own layers of header information, which the corresponding protocols in receiving devices then interpret.

packet mode connections Packet mode connections are typically passed through the router or remote access device. This includes Point-to-Point Protocol (PPP) sessions.

packet switch A physical device that makes it possible for a communication channel to share several connections; its functions include finding the most-efficient transmission path for packets.

packet switching A networking technology based on the transmission of data in packets. Dividing a continuous stream of data into small units—packets—enables data from multiple devices on a network to share the same communication channel simultaneously but also requires the use of precise routing information.

PAD Packet assembler and disassembler: Used to buffer incoming data that is coming in faster than the receiving device can handle it. Typically, only used in X.25 networks.

PAgP Port Aggregation Protocol: The communication process that switches use to determine if and how they will form an EtherChannel connection.

PAP Password Authentication Protocol: In Point-to-Point Protocol (PPP) networks, a method of validating connection requests. The requesting (remote) device must send an authentication request, containing a password and ID, to the local router when attempting to connect. Unlike the more secure CHAP (Challenge Handshake Authentication Protocol), PAP sends the password unencrypted and does not attempt to verify whether the user is authorized to access the requested resource; it merely identifies the remote end. *Compare to: CHAP.*

parity checking A method of error-checking in data transmissions. An extra bit (the parity bit) is added to each character or data word so that the sum of the bits will be either an odd number (in odd parity) or an even number (even parity).

partial mesh A type of network topology in which some network nodes form a full mesh (where every node has either a physical or a virtual circuit linking it to every other network node), but others are attached to only one or two nodes in the network. A typical use of partial-mesh topology is in peripheral networks linked to a fully meshed backbone. *See also: full mesh.*

PAT Port Address Translation: This process enables a single IP address to represent multiple resources by altering the source TCP or UDP port number.

payload compression Reduces the number of bytes required to accurately represent the original data stream. Header compression is also possible. *See also: compression.*

PCR Peak Cell Rate: As defined by the ATM Forum, the parameter specifying, in cells per second, the maximum rate at which a source can transmit.

PDN Public Data Network: Generally for a fee, a PDN offers the public access to a computer communication network operated by private concerns or government agencies. Small organizations can take advantage of PDNs, aiding them in creating WANs without investing in long-distance equipment and circuitry.

PDU Protocol Data Unit: The name of the processes at each layer of the OSI model. PDUs at the Transport layer are called "segments," PDUs at the Network layer are called "packets" or "datagrams," and PDUs at the Data Link layer are called "frames." The Physical layer uses "bits."

PFC Policy Feature Card: The PFC can be paralleled with the NFFC used in Catalyst 5000 switches. It is a device that is capable of examining IP and Ethernet headers in order to establish flow caches.

PGP Pretty Good Privacy: A popular public-key/private-key encryption application offering protected transfer of files and messages.

Physical layer The lowest layer—layer 1—in the OSI reference model, it is responsible for converting data packets from the Data Link layer (layer 2) into electrical signals. Physical-layer protocols and standards define, for example, the type of cable and connectors to be used, including their pin assignments and the encoding scheme for signaling 0 and 1 values. *See also: Application layer, Data Link layer, Network layer, Presentation layer, Session layer,* and *Transport layer.*

PIM Protocol Independent Multicast: A multicast protocol that handles the IGMP requests as well as requests for multicast data forwarding.

PIM DM Protocol Independent Multicast dense mode: PIM DM utilizes the unicast route table and relies on the source root distribution architecture for multicast data forwarding.

PIM SM Protocol Independent Multicast sparse mode: PIM SM utilizes the unicast route table and relies on the shared root distribution architecture for multicast data forwarding.

PIM sparse-dense mode An interface configuration that enables the interface to choose the method of PIM operation.

Ping Packet Internet groper: A Unix-based Internet diagnostic tool, consisting of a message sent to test the accessibility of a particular device on the IP network. The acronym (from which the "full name" was formed) reflects the underlying metaphor of submarine sonar. Just as the sonar operator sends out a signal and waits to hear it echo ("ping") back from a submerged object, the network user can ping another node on the network and wait to see whether it responds.

pleisochronous Nearly synchronous, except that clocking comes from an outside source instead of being embedded within the signal as in synchronous transmissions.

PLP Packet Level Protocol: Occasionally called "X.25 Level 3" or "X.25 Protocol," a Network-layer protocol that is part of the X.25 stack.

PNNI Private Network-Network Interface: An ATM Forum specification for offering topology data used for the calculation of paths through the network, among switches and groups of switches. It is based on well-known link-state routing procedures and allows for automatic configuration in networks whose addressing scheme is determined by the topology.

point-to-multipoint connection In ATM, a communication path going only one way, connecting a single system at the starting point, called the "root node," to systems at multiple points of destination, called "leaves." *See also: point-to-point connection.*

point-to-point connection In ATM, a channel of communication that can be directed either one way or two ways between two ATM end systems. *See also: point-to-multipoint connection.*

poison reverse updates These update messages are transmitted by a router back to the originator (thus ignoring the split-horizon rule) after route poisoning has occurred. Typically used with DV routing protocols in order to overcome large routing loops and offer explicit information when a subnet or network is not accessible (instead of merely suggesting that the network is unreachable by not including it in updates). *See also: route poisoning.*

polling The procedure of orderly inquiry, used by a primary network mechanism, to determine whether secondary devices have data to transmit. A message is sent to each secondary, granting the secondary the right to transmit.

POP 1) Point of Presence: The physical location where an interexchange carrier has placed equipment to interconnect with a local exchange carrier. 2) Post Office Protocol (currently at version 3): A protocol used by client e-mail applications for recovery of mail from a mail server.

port density Port density reflects the capacity of the remote access device regarding the termination of interfaces. For example, the port density of an access server that serves four T1 circuits is 96 analog lines (non-ISDN PRI).

PortFast The configuration option that tells the switch to move directly from blocking mode to forwarding mode. Only to be used when a single PC is connected to the port.

port security Used with layer 2 switches to provide some security. Not typically used in production because it is difficult to manage. Allows only certain frames to traverse administrator-assigned segments.

POTS Plain old telephone service: This refers to the traditional analog phone service that is found in most installations.

PPP Point-to-Point Protocol: The protocol most commonly used for dial-up Internet access, superseding the earlier SLIP. Its features include address notification, authentication via CHAP or PAP, support for multiple protocols, and link monitoring. PPP has two layers: the Link Control Protocol (LCP) establishes, configures, and tests a link; and then any of various Network Control Programs (NCPs) transport traffic for a specific protocol suite, such as IPX. *See also: CHAP, PAP,* and *SLIP.*

PPP callback The point-to-point protocol supports callback to a predetermined number to augment security.

Predictor A compression technique supported by Cisco. *See also: compression.*

Presentation layer Layer 6 of the OSI reference model, it defines how data is formatted, presented, encoded, and converted for use by software at the Application layer. *See also: Application layer, Data Link layer, Network layer, Physical layer, Session layer,* and *Transport layer.*

PRI Primary Rate Interface: A type of ISDN connection between a PBX and a long-distance carrier, which is made up of a single 64Kbps D channel in addition to 23 (T1) or 30 (E1) B channels. *Compare to: BRI. See also: ISDN.*

priority queuing A routing function in which frames temporarily placed in an interface output queue are assigned priorities based on traits such as packet size or type of interface.

process switching As a packet arrives on a router to be forwarded, it's copied to the router's process buffer, and the router performs a lookup on the layer 3 address. Using the route table, an exit interface is associated with the destination address. The processor forwards the packet with the added new information to the exit interface, while the router initializes the fast-switching cache. Subsequent packets bound for the same destination address follow the same path as the first packet. *Compare to: fast switching.*

PROM Programmable read-only memory: ROM that is programmable only once, using special equipment. *Compare to: EPROM* and *EEPROM.*

propagation delay The time it takes data to traverse a network from its source to its destination.

protocol In networking, the specification of a set of rules for a particular type of communication. The term is also used to refer to the software that implements a protocol.

protocol stack A collection of related protocols.

Proxy ARP Proxy Address Resolution Protocol: Used to allow redundancy in case of a failure with the configured default gateway on a host. Proxy ARP is a variation of the ARP protocol in which an intermediate device, such as a router, sends an ARP response on behalf of an end node to the requesting host.

pruning The act of trimming down the Shortest Path Tree. This deactivates interfaces that do not have group participants.

PSE Packet Switch Exchange: The X.25 term for a switch.

PSN Packet-switched network: Any network that uses packet-switching technology. Also known as "packet-switched data network (PSDN)." *See also: packet switching.*

PSTN Public Switched Telephone Network: Colloquially referred to as "plain old telephone service" (POTS). A term that describes the assortment of telephone networks and services available globally.

PTSP PNNI Topology State Packet, used in ATM.

PVC Permanent virtual circuit: In a Frame-Relay network, a logical connection, defined in software, that is maintained permanently. *Compare to: SVC. See also: virtual circuit.*

PVP Permanent virtual path: A virtual path made up of PVCs. *See also: PVC.*

PVP tunneling Permanent virtual path tunneling: A technique that links two private ATM networks across a public network by using a virtual path; the public network transparently trunks the complete collection of virtual channels in the virtual path between the two private networks.

PVST Per-VLAN Spanning Tree: A Cisco proprietary implementation of STP. PVST uses ISL and runs a separate instance of STP for each and every VLAN.

PVST+ Per-VLAN Spanning Tree+: Allows CST information to be passed into PVST.

QoS Quality of Service: A set of metrics used to measure the quality of transmission and service availability of any given transmission system.

queue Broadly, any list of elements arranged in an orderly fashion and ready for processing, such as a line of people waiting to enter a movie theater. In routing, it refers to a backlog of information packets waiting in line to be transmitted over a router interface.

queuing A quality of service process that enables packets to be forwarded from the router based on administratively defined parameters. This can be used for time-sensitive protocols, such as SNA.

R reference point Used with ISDN networks to identify the connection between an NT1 and an S/T device. The S/T device converts the four-wire network to the two-wire ISDN standard network.

RADIUS Remote Access Dial-in User Service: A protocol that is used to communicate between the remote access device and an authentication server. Sometimes an authentication server running RADIUS will be called a RADIUS server.

RAM Random access memory: Used by all computers to store information. Cisco routers use RAM to store packet buffers and routing tables, along with the hardware addresses cache.

RARP Reverse Address Resolution Protocol: The protocol within the TCP/IP stack that maps MAC addresses to IP addresses. *See also: ARP.*

rate queue A value, assigned to one or more virtual circuits, that specifies the speed at which an individual virtual circuit will transmit data to the remote end. Every rate queue identifies a segment of the total bandwidth available on an ATM link. The sum of all rate queues should not exceed the total available bandwidth.

RCP Remote Copy Protocol: A protocol for copying files to or from a file system that resides on a remote server on a network, using TCP to guarantee reliable data delivery.

redistribution Command used in Cisco routers to inject the paths found from one type of routing protocol into another type of routing protocol. For example, networks found by RIP can be inserted into an IGRP network.

redundancy In internetworking, the duplication of connections, devices, or services that can be used as a backup in the event that the primary connections, devices, or services fail.

reference point Used to define an area in an ISDN network. Providers used these reference points to find problems in the ISDN network.

reliability The measure of the quality of a connection. It is one of the metrics that can be used to make routing decisions.

reload An event or command that causes Cisco routers to reboot.

remote access A generic term that defines connectivity to distant resources using one of many technologies, as appropriate.

remote services Network services close to users but not on the same network or subnet as the users. The users would have to cross a layer 3 device to communicate with the network services, but they might not have to cross the backbone.

rendezvous point *See:* RP.

reverse Telnet Maps a Telnet port to a physical port on the router or access device. This enables the administrator to connect to a modem or other device attached to the port.

RFC Request for Comments: RFCs are used to present and define standards in the networking industry.

RIF Routing Information Field: In source-route bridging, a header field that defines the path direction of the frame or token. If the Route Information Indicator (RII) bit is not set, the RIF is read from source to destination (left to right). If the RII bit is set, the RIF is read from the destination back to the source, so the RIF is read from right to left. It is defined as part of the Token Ring frame header for source-routed frames, which contains path information.

ring Two or more stations connected in a logical circular topology. In this topology, which is the basis for Token Ring, FDDI, and CDDI, information is transferred from station to station in sequence.

ring topology A network logical topology comprising a series of repeaters that form one closed loop by connecting unidirectional transmission links. Individual stations on the network are connected to the network at a repeater. Physically, ring topologies are generally organized in a closed-loop star. *Contrast with: bus topology* and *star topology*.

RIP Routing Information Protocol: The most commonly used interior gateway protocol in the Internet. RIP employs hop count as a routing metric. *See also: Enhanced IGRP, IGP, OSPF,* and *hop count*.

RIP version 2 Newer, updated version of Routing Information Protocol (RIP). Allows VLSM. *See also: VLSM*.

RJ connector Registered jack connector: Used with twisted-pair wiring to connect the copper wire to network interface cards, switches, and hubs.

robbed bit signaling Used in Primary Rate Interface clocking mechanisms.

ROM Read-only memory: Chip used in computers to help boot the device. Cisco routers use a ROM chip to load the bootstrap, which runs a power-on self test, and then find and load the IOS in flash memory by default.

root bridge Used with the Spanning Tree Protocol to stop network loops from occurring. The root bridge is elected by having the lowest bridge ID. The bridge ID is determined by the priority (32768 by default on all bridges and switches) and the main hardware address of the device. The root bridge

determines which of the neighboring layer 2 devices' interfaces become the designated and nondesignated ports.

routed protocol Routed protocols (such as IP and IPX) are used to transmit user data through an internetwork. By contrast, routing protocols (such as RIP, IGRP, and OSPF) are used to update routing tables between routers.

route poisoning Used by various DV routing protocols in order to overcome large routing loops and offer explicit information about when a subnet or network is not accessible (instead of merely suggesting that the network is unreachable by not including it in updates). Typically, this is accomplished by setting the hop count to one more than maximum. *See also: poison reverse updates.*

route summarization In various routing protocols, such as OSPF, EIGRP, and IS-IS, the consolidation of publicized subnetwork addresses so that a single summary route is advertised to other areas by an area border router.

router A Network-layer mechanism, either software or hardware, using one or more metrics to decide on the best path to use for transmission of network traffic. Sending packets between networks by routers is based on the information provided on Network layers. Historically, this device has sometimes been called a "gateway."

router on a stick A term that identifies a single router interface connected to a single distribution layer switch port. The router is an external router that provides trunking protocol capabilities for routing between multiple VLANs. *See also: RSM, MSFC.*

routing The process of forwarding logically addressed packets from their local subnetwork toward their ultimate destination. In large networks, the numerous intermediary destinations that a packet might travel before reaching its destination can make routing very complex.

routing domain Any collection of end systems and intermediate systems that operate under an identical set of administrative rules. Every routing domain contains one or several areas, all individually given a certain area address.

routing metric Any value that is used by routing algorithms to determine whether one route is superior to another. Metrics include such information as bandwidth, delay, hop count, path cost, load, MTU, reliability, and

communication cost. Only the best possible routes are stored in the routing table, while all other information may be stored in link-state or topological databases. *See also: cost.*

routing protocol Any protocol that defines algorithms to be used for updating routing tables between routers. Examples include IGRP, RIP, and OSPF.

routing table A table kept in a router or other internetworking mechanism that maintains a record of only the best possible routes to certain network destinations and the metrics associated with those routes.

RP 1) Rendezvous point: A router that acts as the multicast source in a multicast network. Primarily in a shared tree distribution. 2) Route Processor: Also known as a "supervisory processor," a module on Cisco 7000 series routers that holds the CPU, system software, and most of the memory components used in the router.

RSFC Route Switch Feature Card: Used to provide routing between VLANs. The RSFC is a daughter card for the Supervisor engine II G and Supervisor III G cards. The RSFC is a fully functioning router running the Cisco IOS.

RSM Route Switch Module: A route processor that is inserted into the chassis of a Cisco Catalyst 5000 series switch. The RSM is configured exactly like an external router.

RSP Route/Switch Processor: A processor module combining the functions of RP and SP used in Cisco 7500 series routers. *See also: RP and SP.*

RTS Request to Send: An EIA/TIA-232 control signal requesting permission to transmit data on a communication line.

S reference point ISDN reference point that works with a T reference point to convert a four-wire ISDN network to the two-wire ISDN network needed to communicate with the ISDN switches at the network provider.

sampling rate The rate at which samples of a specific waveform amplitude are collected within a specified period of time.

SAP 1) Service Access Point: A field specified by IEEE 802.2 that is part of an address specification. *See also: DSAP* and *SSAP.* 2) Service Advertising Protocol: The Novell NetWare protocol that supplies a way to inform

network clients of resources and services availability on a network, using routers and servers. *See also: IPX.*

SCR Sustainable Cell Rate: An ATM Forum parameter used for traffic management, it is the long-term average cell rate for VBR connections that can be transmitted.

scripts A script predefines commands that should be issued in sequence, typically to complete a connection or accomplish a repetitive task.

SDLC Synchronous Data Link Control: A protocol used in SNA Data Link–layer communications. SDLC is a bit-oriented, full-duplex serial protocol that is the basis for several similar protocols, including HDLC and LAPB. *See also: HDLC* and *LAPB.*

security policy Document that defines the business requirements and processes that are to be used to protect corporate data. A security policy might be as generic as "no file transfers allowed" to very specific, such as "FTP puts allowed only to server X."

security server A centralized device that authenticates access requests, typically via a protocol such as TACACS+ or RADIUS. *See also: TACACS+, RADIUS.*

seed router In an AppleTalk network, the router that is equipped with the network number or cable range in its port descriptor. The seed router specifies the network number or cable range for other routers in that network section and answers to configuration requests from nonseed routers on its connected AppleTalk network, permitting those routers to affirm or modify their configurations accordingly. Every AppleTalk network needs at least one seed router physically connected to each network segment.

server Hardware and software that provide network services to clients.

set-based Set-based routers and switches use the `set` command to configure devices. Cisco is moving away from set-based commands and is using the command-line interface (CLI) on all new devices.

Session layer Layer 5 of the OSI reference model, responsible for creating, managing, and terminating sessions between applications and overseeing data exchange between Presentation layer entities. *See also: Application layer, Data Link layer, Network layer, Physical layer, Presentation layer,* and *Transport layer.*

setup mode Mode that a router will enter if no configuration is found in non-volatile RAM when the router boots. Enables the administrator to configure a router step-by-step. Not as robust or flexible as the command-line interface.

SF Super frame: A super frame (also called a "D4 frame") consists of 12 frames with 192 bits each, and the 193rd bit providing other functions including error checking. SF is frequently used on T1 circuits. A newer version of the technology is Extended Super Frame (ESF), which uses 24 frames. *See also: ESF.*

shared trees A method of multicast data forwarding. Shared trees use an architecture in which multiple sources share a common rendezvous point.

signaling packet An informational packet created by an ATM-connected mechanism that wants to establish a connection with another such mechanism. The packet contains the QoS parameters needed for connection and the ATM NSAP address of the endpoint. The endpoint responds with a message of acceptance if it is able to support the desired QoS, and the connection is established. *See also: QoS.*

silicon switching A type of high-speed switching used in Cisco 7000 series routers, based on the use of a separate processor (the Silicon Switch Processor, or SSP). *See also: SSE.*

simplex The mode at which data or a digital signal is transmitted. Simplex is a way of transmitting in only one direction. Half duplex transmits in two directions, but only one direction at a time. Full duplex transmits in both directions simultaneously.

sliding window The method of flow control used by TCP, as well as several Data Link–layer protocols. This method places a buffer between the receiving application and the network data flow. The "window" available for accepting data is the size of the buffer minus the amount of data already there. This window increases in size as the application reads data from it and decreases as new data is sent. The receiver sends the transmitter announcements of the current window size, and it may stop accepting data until the window increases above a certain threshold.

SLIP Serial Line Internet Protocol: An industry standard serial encapsulation for point-to-point connections that supports only a single routed protocol, TCP/IP. SLIP is the predecessor to PPP. *See also: PPP.*

SMDS Switched Multimegabit Data Service: A packet-switched, datagram-based WAN networking technology offered by telephone companies that provides high speed.

SMTP Simple Mail Transfer Protocol: A protocol used on the Internet to provide electronic mail services.

SNA System Network Architecture: A complex, feature-rich, network architecture similar to the OSI reference model but with several variations; created by IBM in the 1970s and essentially composed of seven layers.

SNAP Subnetwork Access Protocol: SNAP is a frame used in Ethernet, Token Ring, and FDDI LANs. Data transfer, connection management, and QoS selection are three primary functions executed by the SNAP frame.

snapshot routing Snapshot routing takes a point-in-time capture of a dynamic routing table and maintains it even when the remote connection goes down. This allows the use of a dynamic routing protocol without requiring the link to remain active, which might incur per-minute usage charges.

socket 1) A software structure that operates within a network device as a destination point for communications. 2) In AppleTalk networks, an entity at a specific location within a node; AppleTalk sockets are conceptually similar to TCP/IP ports.

SOHO Small office, home office: A contemporary term for remote users.

SONET Synchronous Optical Network: The ANSI standard for synchronous transmission on fiber-optic media, developed at Bell Labs. It specifies a base signal rate of 51.84Mbps and a set of multiples of that rate, known as Optical Carrier levels, up to 2.5Gbps.

source trees A method of multicast data forwarding. Source trees use the architecture of the source of the multicast traffic as the root of the tree.

SP Switch Processor: Also known as a "ciscoBus controller," it is a Cisco 7000 series processor module acting as governing agent for all CxBus activities.

span A full-duplex digital transmission line connecting two facilities.

SPAN Switch Port Analyzer: A feature of the Catalyst 5000 switch, offering freedom to manipulate within a switched Ethernet environment by extending the monitoring ability of the existing network analyzers into the

environment. At one switched segment, the SPAN mirrors traffic onto a predetermined SPAN port, while a network analyzer connected to the SPAN port is able to monitor traffic from any other Catalyst switched port.

spanning explorer packet Sometimes called "limited-route explorer packet" or "single-route explorer packet," it pursues a statically configured spanning tree when searching for paths in a source-route bridging network. *See also: all-routes explorer packet, explorer packet,* and *local explorer packet.*

spanning tree A subset of a network topology, within which no loops exist. When bridges are interconnected into a loop, the bridge, or switch, cannot identify a frame that has been forwarded previously, so there is no mechanism for removing a frame as it passes the interface numerous times. Without a method of removing these frames, the bridges continuously forward them—consuming bandwidth and adding overhead to the network. Spanning trees prune the network to provide only one path for any packet. *See also: Spanning Tree Protocol and spanning tree algorithm.*

spanning-tree algorithm (STA) An algorithm that creates a spanning tree using the Spanning Tree Protocol (STP). *See also: spanning tree* and *Spanning Tree Protocol.*

Spanning Tree Protocol (STP) The bridge protocol (IEEE 802.1d) that enables a learning bridge to dynamically avoid loops in the network topology by creating a spanning tree, using the spanning-tree algorithm. Spanning-tree frames called Bridge Protocol Data Units (BPDUs) are sent and received by all switches in the network at regular intervals. The switches participating in the spanning tree don't forward the frames; instead, they're processed to determine the spanning-tree topology itself. Cisco Catalyst series switches use STP 802.1d to perform this function. *See also: BPDU, learning bridge, MAC address, spanning tree,* and *spanning-tree algorithm.*

SPF Shortest Path First algorithm: A routing algorithm used to decide on the shortest-path spanning tree. Sometimes called "Dijkstra's algorithm" and frequently used in link-state routing algorithms. *See also: link-state routing algorithm.*

SPID Service Profile Identifier: A number assigned by service providers or local telephone companies and assigned by administrators to a BRI port. SPIDs are used to determine subscription services of a device connected via

ISDN. ISDN devices use SPID when accessing the telephone company switch that initializes the link to a service provider.

split horizon Useful for preventing routing loops, a type of distance-vector routing rule where information about routes is prevented from leaving the router interface through which that information was received.

spoofing 1) In dial-on-demand routing (DDR), where a circuit-switched link is taken down to save toll charges when there is no traffic to be sent, spoofing is a scheme used by routers that causes a host to treat an interface as if it were functioning and supporting a session. The router pretends to send "spoof" replies to keep-alive messages from the host in an effort to convince the host that the session is up and running. *See also: DDR.* 2) The illegal act of sending a packet labeled with a false address, in order to deceive network security mechanisms such as filters and access lists.

spooler A management application that processes requests submitted to it for execution in a sequential fashion from a queue. A good example is a print spooler.

SPX Sequenced Packet Exchange: A Novell NetWare transport protocol that augments the datagram service provided by Network-layer (layer 3) protocols, it was derived from the Switch-to-Switch Protocol of the XNS protocol suite.

SQE Signal Quality Error: In an Ethernet network, a message sent from a transceiver to an attached machine that the collision-detection circuitry is working.

SRB Source-route bridging: Created by IBM, the bridging method used in Token-Ring networks. The source determines the entire route to a destination before sending the data and includes that information in route information fields (RIF) within each packet. *Contrast with: transparent bridging.*

SRT Source-route transparent bridging: A bridging scheme developed by IBM, merging source-route and transparent bridging. SRT takes advantage of both technologies in one device, fulfilling the needs of all end nodes. Translation between bridging protocols is not necessary. *Compare to: SR/TLB.*

SR/TLB Source-route translational bridging: A bridging method that enables source-route stations to communicate with transparent bridge

stations aided by an intermediate bridge that translates between the two bridge protocols. Used for bridging between Token Ring and Ethernet. *Compare to: SRT.*

SSAP Source Service Access Point: The SAP of the network node identified in the Source field of the packet. *See also: DSAP* and *SAP.*

SSE Silicon Switching Engine: The software component of Cisco's silicon switching technology, hard-coded into the Silicon Switch Processor (SSP). Silicon switching is available only on the Cisco 7000 with an SSP. Silicon-switched packets are compared to the silicon-switching cache on the SSE. The SSP is a dedicated switch processor that offloads the switching process from the route processor, providing a fast-switching solution, but packets must still traverse the backplane of the router to get to the SSP and then back to the exit interface.

SS-7 signaling Signaling System 7: The current standard for telecommunications switching control signaling. This is an out-of-band signaling that establishes circuits and provides billing information.

Stac A compression method developed by Stacker Corporation for use over serial links.

standard IP access list IP access list that uses only the source IP addresses to filter a network.

standard IPX access list IPX access list that uses only the source and destination IPX address to filter a network.

star topology A LAN physical topology with endpoints on the network converging at a common central switch (known as a hub) using point-to-point links. A logical ring topology can be configured as a physical star topology using a unidirectional closed-loop star rather than point-to-point links. That is, connections within the hub are arranged in an internal ring. *Contrast with: bus topology* and *ring topology.*

startup range If an AppleTalk node does not have a number saved from the last time it was booted, then the node selects from the range of values from 65280 to 65534.

state transitions Digital signaling scheme that reads the "state" of the digital signal in the middle of the bit cell. If it is five volts, the cell is read as a one. If the state of the digital signal is zero volts, the bit cell is read as a zero.

static route A route whose information is purposefully entered into the routing table and takes priority over those chosen by dynamic routing protocols.

static VLAN VLAN that is manually configured port-by-port. This is the method typically used in production networks.

statistical multiplexing Multiplexing in general is a technique that enables data from multiple logical channels to be sent across a single physical channel. Statistical multiplexing dynamically assigns bandwidth only to input channels that are active, optimizing available bandwidth so that more devices can be connected than with other multiplexing techniques. Also known as "statistical time-division multiplexing" or "stat mux." *Contrast with ATDM, FDM,* and *TDM.*

STM-1 Synchronous Transport Module Level 1. In the European SDH standard, one of many formats identifying the frame structure for the 155.52Mbps lines that are used to carry ATM cells.

store-and-forward *See: store-and-forward packet switching*

store-and-forward packet switching A technique in which the switch first copies each packet into its buffer and performs a cyclical redundancy check (CRC). If the packet is error-free, the switch then looks up the destination address in its filter table, determines the appropriate exit port, and sends the packet.

STP 1) Shielded twisted-pair: A two-pair wiring scheme, used in many network implementations, that has a layer of shielded insulation to reduce EMI. 2) Spanning Tree Protocol.

stub area An OSPF area carrying a default route, intra-area routes, and interarea routes, but no external routes. Configuration of virtual links cannot be achieved across a stub area, and stub areas are not allowed to contain an ASBR. *See also: non-stub area, ASBR,* and *OSPF.*

stub network A network having only one connection to a router.

STUN Serial Tunnel: A technology used to connect an HDLC link to an SDLC link over a serial link.

subarea A portion of an SNA network made up of a subarea node and its attached links and peripheral nodes.

subarea node An SNA communications host or controller that handles entire network addresses.

subchannel A frequency-based subdivision that creates a separate broadband communications channel.

subinterface One of many virtual interfaces available on a single physical interface.

subnet *See: subnetwork*.

subnet address The portion of an IP address that is specifically identified by the subnet mask as the subnetwork. *See also: IP address, subnetwork,* and *subnet mask*.

subnet mask Also simply known as "mask," a 32-bit address mask used in IP to identify the bits of an IP address that are used for the subnet address. Using a mask, the router does not need to examine all 32 bits, only those selected by the mask. *See also: address mask* and *IP address*.

subnetwork 1) Any network that is part of a larger IP network and is identified by a subnet address. A network administrator segments a network into subnetworks in order to provide a hierarchical, multilevel routing structure, and at the same time protect the subnetwork from the addressing complexity of networks that are attached. Also known as a "subnet." *See also: IP address, subnet mask,* and *subnet address*. 2) In OSI networks, the term specifically refers to a collection of computing devices controlled by only one administrative domain, using a solitary network connection protocol.

SVC Switched virtual circuit: A dynamically established virtual circuit, created on demand and dissolved as soon as transmission is over and the circuit is no longer needed. In ATM terminology, it is referred to as a switched virtual connection. *Compare to: PVC.*

switch 1) In networking, a device responsible for multiple functions such as filtering, flooding, and sending frames. It works by using the destination address of individual frames. Switches operate at the Data Link layer of the OSI model. 2) Broadly, any electronic/mechanical device enabling connections to be established as needed and terminated if no longer necessary.

switch block A combination of layer 3 switches and layer 3 routers. The layer 2 switches connect users in the wiring closet into the access layer and provide 10Mbps or 100Mbps dedicated connections. 1900/2820 and 2900 Catalyst switches can be used in the switch block.

switched Ethernet A device that switches Ethernet frames between segments by filtering on hardware addresses.

switched LAN Any LAN implemented by using LAN switches. *See also: LAN switch*.

switch-fabric The central functional block of any switch design; responsible for buffering and routing the incoming data to the appropriate output ports.

synchronous transmission Signals transmitted digitally with precision clocking. These signals have identical frequencies and contain individual characters encapsulated in control bits (called start/stop bits) that designate the beginning and ending of each character. *Contrast with: asynchronous transmission* and *isochronous transmission.*

T reference point Used with an S reference point to change a four-wire ISDN network to a two-wire ISDN network.

T1 Digital WAN that uses 24 DS0s at 64KB each to create a bandwidth of 1.536Mbps, minus clocking overhead, providing 1.544Mbps of usable bandwidth.

T3 Digital WAN that can provide bandwidth of 44.763Mbps.

TACACS+ Terminal Access Control Access Control System: An enhanced version of TACACS, this protocol is similar to RADIUS. *See also: RADIUS.*

tag switching A high-performance technology used for forwarding packets. Based on the concept of label swapping, whereby packets or cells are designated to defined-length labels that control the manner in which data is to be sent. It incorporates Data Link–layer (layer 2) switching and Network-layer (layer 3) routing and supplies scalable, high-speed switching in the network core.

tagged traffic ATM cells with their cell loss priority (CLP) bit set to 1. Also referred to as "discard-eligible (DE) traffic." Tagged traffic can be eliminated in order to ensure trouble-free delivery of higher-priority traffic, if the network is congested. *See also: CLP.*

TCP Transmission Control Protocol: A connection-oriented protocol that is defined at the Transport layer of the OSI reference model. Provides reliable delivery of data.

TCP header compression A compression process that compresses only the TCP header information, which is typically repetitive. This would not compress the user data. *See also: compression.*

TCP/IP Transmission Control Protocol/Internet Protocol. The suite of protocols underlying the Internet. TCP and IP are the most widely known protocols in that suite. *See also: IP* and *TCP.*

TDM Time Division Multiplexing: A technique for assigning bandwidth on a single wire, based on preassigned time slots, to data from several channels. Bandwidth is allotted to each channel regardless of a station's ability to send data. *Contrast with: ATDM, FDM,* and *statistical multiplexing.*

TE Terminal equipment: Any peripheral device that is ISDN-compatible and attached to a network, such as a telephone or computer. TE1s are devices that are ISDN-ready and understand ISDN signaling techniques. TE2s are devices that are not ISDN-ready and do not understand ISDN signaling techniques. A terminal adapter must be used with a TE2.

TE1 A device with a four-wire, twisted-pair digital interface is referred to as terminal equipment type 1. Most modern ISDN devices are of this type.

TE2 Devices known as terminal equipment type 2 do not understand ISDN signaling techniques, and a terminal adapter must be used to convert the signaling.

telco A common abbreviation for the telephone company.

Telnet The standard terminal emulation protocol within the TCP/IP protocol stack. A method of remote terminal connection, enabling users to log in on remote networks and use those resources as if they were locally connected. Telnet is defined in RFC 854.

10BaseT Part of the original IEEE 802.3 standard, 10BaseT is the Ethernet specification of 10Mbps baseband that uses two pairs of twisted-pair, Category 3, 4, or 5 cabling—using one pair to send data and the other to receive. 10BaseT has a distance limit of about 100 meters per segment. *See also: Ethernet* and *IEEE 802.3.*

terminal adapter A hardware interface between a computer without a native ISDN interface and an ISDN line. In effect, a device to connect a standard async interface to a non-native ISDN device, emulating a modem.

terminal emulation The use of software, installed on a PC or LAN server, that enables the PC to function as if it were a "dumb" terminal directly attached to a particular type of mainframe.

TFTP Conceptually, a stripped-down version of FTP, it's the protocol of choice if you know exactly what you want and where it's to be found. TFTP doesn't provide the abundance of functions that FTP does. In particular, it has no directory-browsing abilities; it can do nothing but send and receive files. *See also: FTP*.

Thicknet Also called "10Base5." Bus network that uses a thick cable and runs Ethernet up to 500 meters.

Thinnet Also called "10Base2." Bus network that uses a thin coax cable and runs Ethernet media access up to 185 meters.

token A frame containing only control information. Possessing this control information gives a network device permission to transmit data onto the network. *See also: token passing*.

token bus LAN architecture that is the basis for the IEEE 802.4 LAN specification and employs token passing access over a bus topology. *See also: IEEE*.

token passing A method used by network devices to access the physical medium in a systematic way based on possession of a small frame called a token. *See also: token*.

Token Ring IBM's token-passing LAN technology. It runs at 4Mbps or 16Mbps over a ring topology. Defined formally by IEEE 802.5. *See also: ring topology* and *token passing*.

toll network WAN network that uses the Public Switched Telephone Network (PSTN) to send packets.

trace IP command used to trace the path a packet takes through an internetwork.

traffic shaping Used on Frame Relay networks to provide priorities of data.

transparent bridging The bridging scheme used in Ethernet and IEEE 802.3 networks, it passes frames along one hop at a time, using bridging information stored in tables that associate end-node MAC addresses within bridge ports. This type of bridging is considered transparent because the source node does not know it has been bridged, because the destination frames are sent directly to the end node. *Contrast with: SRB.*

Transport layer Layer 4 of the OSI reference model, used for reliable communication between end nodes over the network. The Transport layer provides mechanisms used for establishing, maintaining, and terminating virtual circuits, transport fault detection and recovery, and controlling the flow of information. *See also: Application layer, Data Link layer, Network layer, Physical layer, Presentation layer,* and *Session layer.*

TRIP Token Ring Interface Processor: A high-speed interface processor used on Cisco 7000 series routers. The TRIP provides two or four ports for interconnection with IEEE 802.5 and IBM media with ports set to speeds of either 4Mbps or 16Mbps set independently of each other.

trunk link Link used between switches and from some servers to the switches. Trunk links carry information about many VLANs. Access links are used to connect host devices to a switch and carry only VLAN information that the device is a member of.

TTL Time to Live: A field in an IP header, indicating the length of time that a packet is valid.

TUD Trunk Up-Down: A protocol used in ATM networks for the monitoring of trunks. If a trunk misses a given number of test messages being sent by ATM switches to ensure trunk line quality, TUD declares the trunk down. When a trunk reverses direction and comes back up, TUD recognizes that the trunk is up and returns the trunk to service.

tunneling A method of avoiding protocol restrictions by wrapping packets from one protocol in another protocol's packet and transmitting this encapsulated packet over a network that supports the wrapper protocol. *See also: encapsulation.*

20/80 rule A rule indicating that 20 percent of what the user performs on the network is local, whereas up to 80 percent crosses the network segmentation points to get to network services.

UART The Universal Asynchronous Receiver/Transmitter: A chip that governs asynchronous communications. Its primary function is to buffer incoming data, but it also buffers outbound bits.

U reference point Reference point between a TE1 and an ISDN network. The U reference point understands ISDN signaling techniques and uses a two-wire connection.

UDP User Datagram Protocol: A connectionless Transport-layer protocol in the TCP/IP protocol stack that simply enables datagrams to be exchanged without acknowledgements or delivery guarantees, requiring other protocols to handle error processing and retransmission. UDP is defined in RFC 768.

unicast Used for direct host-to-host communication. Communication is directed to only one destination and is originated from only one source.

unidirectional shared tree A method of shared tree multicast forwarding. This method allows only multicast data to be forwarded from the RP.

unnumbered frames HDLC frames used for control-management purposes, such as link startup and shutdown or mode specification.

UplinkFast Enables a switch to immediately begin forwarding frames on blocked ports when a failure is detected on the root port.

UTP Unshielded twisted-pair: Copper wiring used in small-to-large networks to connect host devices to hubs and switches. Also used to connect switch to switch or hub to hub.

VBR Variable Bit Rate: A QoS class, as defined by the ATM Forum, for use in ATM networks that is subdivided into real time (RT) class and non-real time (NRT) class. RT is employed when connections have a fixed-time relationship between samples. Conversely, NRT is employed when connections do not have a fixed-time relationship between samples, but still need an assured QoS. *Compare to: ABR* and *CBR*.

VCC Virtual Channel Connection: A logical circuit that is created by VCLs. VCCs carry data between two endpoints in an ATM network. Sometimes called a virtual circuit connection.

VIP 1) Versatile Interface Processor: An interface card for Cisco 7000 and 7500 series routers, providing multi-layer switching and running the Cisco IOS software. The most recent version of VIP is VIP2. 2) Virtual IP: A function making it possible for logically separated switched IP workgroups to run Virtual Networking Services across the switch ports of a Catalyst 5000.

virtual circuit Abbreviated VC, a logical circuit devised to ensure reliable communication between two devices on a network. Defined by a virtual path connection (VPC)/virtual path identifier (VCI) pair, a virtual circuit can be permanent (PVC) or switched (SVC). Virtual circuits are used in Frame Relay and X.25. Known as "virtual channel" in ATM. *See also: PVC* and *SVC.*

virtual ring In an SRB network, a logical connection between physical rings, either local or remote.

VLAN Virtual LAN: A group of devices on one or more logically segmented LANs (configured by use of management software), enabling devices to communicate as if attached to the same physical medium, when they are actually located on numerous different LAN segments. VLANs are based on logical instead of physical connections and thus are tremendously flexible.

VLAN database A special mode in 2900XL and 3500XL series switches where the administrator creates VLANs.

VLSM Variable-length subnet mask: Helps optimize available address space and specify a different subnet mask for the same network number on various subnets. Also commonly referred to as "subnetting a subnet."

VPN Virtual private network: A method of encrypting point-to-point logical connections across a public network, such as the Internet. This allows secure communications across a public network.

VTP VLAN Trunk Protocol: Used to update switches in a switch-fabric about VLANs configured on a VTP server. VTP devices can be a VTP server, client, or transparent device. Servers update clients. Transparent devices are only local devices and do not share information with VTP clients. VTPs send VLAN information down trunked links only.

VTP pruning VLAN Trunk Protocol is used to communicate VLAN information between switches in the same VTP domain. VTP pruning stops VLAN update information from being sent down trunked links if the updates are not needed.

WAN Wide area network: A designation used to connect LANs together across a DCE (data communications equipment) network. Typically, a WAN is a leased line or dial-up connection across a PSTN network. Examples of WAN protocols include Frame Relay, PPP, ISDN, and HDLC.

weighted fair queuing Default queuing method on serial links on all Cisco routers.

wildcard Used with access-list, supernetting, and OSPF configurations. Wildcards are designations used to identify a range of subnets.

windowing Flow-control method used with TCP at the Transport layer of the OSI model.

WinSock Windows Socket Interface: A software interface that makes it possible for an assortment of applications to use and share an Internet connection. The WinSock software consists of a Dynamic Link Library (DLL) with supporting programs such as a dialer program that initiates the connection.

workgroup switching A switching method that supplies high-speed (100Mbps) transparent bridging between Ethernet networks as well as high-speed translational bridging between Ethernet and CDDI or FDDI.

X.25 An ITU-T packet-relay standard that defines communication between DTE and DCE network devices. X.25 uses a reliable Data Link–layer protocol called LAPB. X.25 also uses PLP at the Network layer. X.25 has mostly been replaced by Frame Relay.

X.25 protocol First packet-switching network, but now mostly used in Europe. Replaced in U.S. by Frame Relay.

XTAG A locally significant numerical value assigned by the MLS-SE to each MLS-RP in the layer 2 network. *See also: MLS-SE, MLS-RP.*

ZIP Zone Information Protocol: A Session-layer protocol used by AppleTalk to map network numbers to zone names. NBP uses ZIP in the determination of networks containing nodes that belong to a zone. *See also: ZIP storm and zone.*

ZIP storm A broadcast storm occurring when a router running AppleTalk reproduces or transmits a route for which there is no corresponding zone name at the time of execution. The route is then forwarded by other routers downstream, thus causing a ZIP storm. *See also: broadcast storm* and *ZIP.*

zone A logical grouping of network devices in AppleTalk. *See also: ZIP.*