CCNA¡ªCisco Certified Network Associate Exam Notes, Third Edition

Todd Lammle
Sean Odom

Associate Publisher: Neil Edde

Acquisitions Editor: Maureen Adams

Developmental Editor: Heather O¡¯Connor

Editor: Emily K. Wolman

Production Editor: Mae Lum

Technical Editor: Andr¨¦ Paree-Huff

Graphic Illustrator: Tony Jonick

Electronic Publishing Specialist: Judy Fung

Proofreaders: Emily Hsuan, David Nash, Yariv Rabinovitch

Indexer: Ted Laux

Book Designer: Bill Gibson

Cover Designer: Archer Design

Cover Photographer: Tony Stone

Library of Congress Card Number: 2002106414ISBN: 0-7821-4168-4

Manufactured in the United States of America

10 9 8 7 6 5 4 3 2 1

To Erin, Mikayla, Hillary, Macky, and Trevor for allowing me to neglect them while I hid myself away and wrote this book.To Jeff Kellum, without whom there would not be a book number 1, much less a book number 12.And to Crystal Harwell, who will always be missed.

¡ªSean Odom

Acknowledgments

I would like to thank the wonderful staff at Sybex for all their support and help throughout this book process. I also want to personally thank Sean Odom for being so dependable.

¡ª*Todd Lammle*

There are many people I need to thank for the production of this book: English teacher Susan Pruna, Marni Ericksen, Todd Lammle for the opportunities he provides me to further my career, and Emily Wolman for fixing my typos and editing the book. Thanks also to Heather O¡¯Connor and Mae Lum for keeping the book on schedule, and to the many others at Sybex working behind the scenes to make this book a success.

The many friends and coworkers that I need to mention include Ken Gregg, Craig Martin, Laurie Stark, John Gilfillan, Aaron Jones, John Alcorcha, and, of course, those people who give me a real job¡ªall the Sweigarts at JTS Communities: Jack, John, Jeff, and Randy.

¡ª*Sean Odom*

Sybex would like to thank electronic publishing specialist Judy Fung; proofreaders Emily Hsuan, David Nash, and Yariv Rabinovitch; and indexer Ted Laux for their valuable contributions to this book.

Introduction

This book is intended to start you out on an exciting new path toward obtaining your CCNA certification. It reaches beyond popular certifications like the MCSE and CNE to provide you with an indispensable factor in understanding today¡¯s network¡ªinsight into the Cisco world of internetworking and network design.

If you¡¯ve purchased this book, you are probably chasing one of the Cisco professional certifications: CCNA/CCNP, CCDA/CCDP, CCIP, or CCIE. All of these are great goals, and they are also great career builders. Glance through any newspaper and you¡¯ll find employment opportunities for people with these certifications¡ªthese ads are there because finding qualified network administrators is a challenge in today¡¯s market. The certification means you know something about the product, but more important, it means you have the ability, determination, and focus to learn¡ªthe greatest skills any employee can have!

You¡¯ve probably also heard all the rumors about how hard the Cisco tests are¡ªbelieve us, the rumors are true! Cisco has designed a series of exams that truly challenge your knowledge of their products. Each test covers not only the materials presented in a particular class, but it also covers the prerequisite knowledge for that course.

Is This Book for You?

This book focuses on the exam objectives for the Cisco Certified Network Associate (CCNA). It will teach you how to install LAN, WAN, and dial-in networks using Cisco products. Each chapter begins with a list of the CCNA test objectives; be sure to read over them before working through the chapter.

The Sybex Exam Notes books were designed to be succinct, portable exam review guides. They can be used either in conjunction with a more complete study program¡ªsupplemented by books, CBT courseware, or practice in a classroom/lab environment¡ªor as an exam review for those who don¡¯t feel the need for more extensive test preparation. It isn¡¯t our goal to ¡°give the answers away,¡± but rather to identify those topics on which you can expect to be tested and to provide sufficient coverage of these topics.

Perhaps you¡¯ve been working with Cisco internetworking technologies for years now. The thought of paying lots of money for a specialized Cisco exam preparation course probably doesn¡¯t sound too appealing. What can they teach you that you don¡¯t already know, right? Be careful, though. Many experienced network administrators, even CCIEs, have walked confidently into test centers only to walk sheepishly out of them after failing a Cisco exam. As they discovered, there¡¯s the Cisco of the real world and the Cisco of the Cisco certification exams. It¡¯s our goal with the Exam Notes books to show you where the two converge and where they diverge. After you¡¯ve finished reading through this book, you should have a clear idea of how your understanding of the technologies involved matches up with the expectations of the Cisco test makers.

Or perhaps you¡¯re relatively new to the world of Cisco internetworking, drawn to it by the promise of challenging work and higher salaries. You¡¯ve just waded through an 1800-page Cisco CCNA study guide or taken a class at a local training center. Lots of information to keep track of, isn¡¯t it? Well, by organizing the Exam Notes books according to the Cisco exam objectives and by breaking up the information into concise, manageable pieces, we¡¯ve created what we think is the handiest exam review guide available. Throw the book in your briefcase and carry it to work with you. As you read through it, you¡¯ll be able to quickly identify those areas you know best and those that require more in-depth review.

Note The goal of the Exam Notes series is to help Cisco certification candidates familiarize themselves with the subjects on which they can expect to be tested in the certification exams. The CCNA exam objectives can be found at `www.cisco.com/warp/public/10/wwtraining/certprog/testing/pdf/ccna_607.pdf`. You¡¯ll notice that the objectives are vague. For complete, in-depth coverage of the technologies and topics involved in Cisco networking, we recommend the *CCNA: Cisco Certified Network Associate Study Guide,* 3rd ed. (Sybex, 2002).

How Is This Book Organized?

As mentioned previously, this book is organized according to the official exam objectives list prepared by Cisco for the CCNA exam. Within each chapter, the individual exam objectives are addressed in turn. Each objective section is further divided according to the type of information presented. Those sections are titled:

- Critical Information
- Necessary Procedures
- Exam Essentials

- Key Terms and Concepts

Critical Information

This section presents the greatest level of detail on information that is relevant to the objective. This is the place to start if you¡¯re unfamiliar with or uncertain about the technical issues related to the objective.

Necessary Procedures

Here you¡¯ll find instructions for procedures that require a lab computer to be completed. From configuring IP addressing to establishing serial point-to-point connections, the information in these sections addresses the hands-on requirements for the CCNA exam.

Note Not every objective has a hands-on procedure associated with it. For such objectives, the Necessary Procedures section has been left out.

Exam Essentials

In this section, we¡¯ve put together a concise list of the most crucial topics of subject areas that you¡¯ll need to comprehend fully prior to taking the Cisco exam. This section can help you identify those topics that might require more study on your part.

Key Terms and Concepts

Here we¡¯ve compiled a mini-glossary of the most important terms and concepts related to the specific objective. You¡¯ll understand what all those technical words mean within the context of the related subject matter.

How Do You Become a CCNA?

With their certification program, Cisco has created a stepping-stone approach to CCIE (Cisco Certified Internetwork Expert) certification. You can become a CCNA by passing one written exam.

Why Become a CCNA?

Cisco has created a certification process, not unlike that of Microsoft or Novell, to give administrators a set of skills and prospective employers an authenticated way to measure those skills. Becoming a CCNA can be the initial step of a successful journey toward a new or refreshed, highly rewarding, and sustainable career.

As you study for the CCNA exam, we can¡¯t stress this enough: It¡¯s critical that you have some hands-on experience with Cisco routers. If you can get your hands on some 2500 series routers, you¡¯re set!

Note One way to get the hands-on router experience you¡¯ll need in the real world is to attend one of the seminars offered by Globalnet Training Solutions, Inc. (`http://www.globalnettraining.com/`), taught by this book¡¯s authors, Todd Lammle and Sean Odom. Each student has three routers and a switch to configure throughout the six-day seminar. Each seminar teaches the students what they need to know to pass the CCNA and CCDA exams!

Note You can also purchase the *CCNA Virtual Lab e-Trainer*, which is a simulated lab environment complete with three routers and one switch. (A more robust version can be downloaded from `http://www.routersim.com/`.)

Where Do You Take the Exams?

You may take the exams at any one of the more than 800 Sylvan Prometric Authorized Testing Centers around the world. For the location of a testing center near you, call 800-204-3926. Outside the United States and Canada, contact your local Sylvan Prometric Registration Center. To register for a Cisco exam:

1. Determine the number of the exam you want to take. (The CCNA exam number is 640-607.)

2. Register with the Sylvan Prometric Registration Center nearest you. You will need to pay in advance for the exam. At the time of this writing, registration costs $125 per exam, and the test must be taken within one year of payment. You can sign up for an exam up to six weeks in advance or as late as the day you wish to take it. If something comes up and you need to cancel or reschedule your exam appointment, contact Sylvan Prometric at least 24 hours in advance.

3. When you schedule the exam, you¡¯ll be provided with instructions regarding all appointment and cancellation procedures, the ID requirements, and information about the testing center location.

Note Cisco exams are also administered at Virtual University Enterprises. Visit http://www.vue.com/ or http://www.cisco.com/warp/public/10/ww.training/certprog/testing/register.htm for more information.

What the Cisco CCNA Certification Exam Measures

The CCNA program was created not only to provide a solid introduction to the Cisco internetworking operating system (IOS) and to Cisco hardware, but also to internetworking in general, making it helpful to you in areas not exclusively Cisco¡¯s. It¡¯s hard to say at this point in the certification process, but it¡¯s not unrealistic to imagine that future network managers¡ªeven those without Cisco equipment¡ªcould easily require Cisco certifications of their job applicants.

To meet the CCNA certification skill level, you must be able to understand or perform the following:

- Install and support simple routed LAN, routed WAN, and switched LAN networks. The exam assumes basic networking understanding.
- Determine whether a hub, Ethernet switch, or router would be more appropriately used.
- Use Cisco software to identify addresses, protocols, and connectivity status in a network that contains multiple interconnected Cisco devices.
- Interconnect Cisco switches and routers using specified network design requirements.
- Configure Cisco switches and routers to support a specified list of protocols and technologies.
- Configure access lists to control access to network devices or segments and general network traffic.
- Verify that Cisco switches and routers, and their configured network services and protocols, operate correctly in a given network specification.

Tips for Taking Your Cisco CCNA Exam

The CCNA test contains around 65 questions, which are to be answered in 90 minutes. Cisco allows you to schedule and take your exam on the same day, as well as to take more than one exam per day.

Many questions on the exam will have potential answers that at first glance look identical¡ªespecially the syntax questions! Remember to read through the choices carefully, because a ¡°close¡± answer won¡¯t cut it. If you choose an answer in which the commands are in the wrong order or there is even one measly character missing, you¡¯ll get the question wrong.

Also, never forget that the right answer is the Cisco answer. In many cases, more than one answer will appear to be the answer, but the *correct* answer is the one Cisco recommends.

Here are some general tips for exam success:

- Arrive early at the exam center so you can relax and review your study materials¡ªparticularly IP tables and lists of exam-related information.
- Read the questions *carefully*. Don¡¯t jump to conclusions. Make sure you¡¯re clear on *exactly* what the question is asking.
- Don¡¯t leave any unanswered questions. These will be counted against you.
- When answering multiple-choice questions you¡¯re not sure about, use a process of elimination to get rid of the obviously incorrect answers first. Doing this will greatly improve your odds should you need to make an ¡°educated guess.¡±

Once you have completed an exam, you¡¯ll be given immediate online notification of your pass or fail status, plus a printed Examination Score Report indicating whether you passed or failed, along with 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 Authors

Todd Lammle can be reached at todd@lammle.com.

Sean Odom can be reached at sodom@surewest.net.

How to Contact the Publisher

Sybex welcomes reader feedback on all of their titles. Visit the Sybex website, http://www.sybex.com/, for book updates and additional certification information. You¡¯ll also find online forms to submit comments or suggestions regarding this or any other Sybex book.

Chapter 1: Bridging/Switching

Cisco Certified Network Associate Exam Objectives Covered in This Chapter:

- Name and describe two switching methods.*(pages 3¡ª6)*
- Distinguish between cut-through and store-and- forward LAN switching.*(pages 6¡ª8)*
- Describe the operation of the Spanning Tree Protocol and its benefits.*(pages 8¡ª15)*
- Describe the benefits of virtual LANs.*(pages 15¡ª22)*

This first chapter introduces you to the terms bridging and switching. Additionally, it covers the three switching methods (store-and-forward, cut-through, and FragmentFree), Spanning Tree Protocol (STP) and how to use STP in a Layer 2 switched internetwork, and the benefits of VLANs and how to configure VLANs on Cisco switches using static VLAN number assignments. Understanding frame tagging within a VLAN is discussed as well.

When there is more than one path through the network, data can come back to the original source, causing what is called a data loop. In this situation, STP is used in Layer 2 switched networks to prevent network loops and to block ports that can allow data to return.

Switches were placed in networks to replace bridges and hubs in flat- topology networks (where there is no segmentation of broadcast or collision domains). As networks grow, so does the amount of broadcast traffic. Not all broadcasts are bad; they are a necessity in today¡¯s networking protocols, to allow the location of certain devices to be known throughout the network segment. But when devices on the same network segment number in the hundreds, the result of all these devices sending broadcasts as well as data traffic can slow the network and the devices to a crawl.

Excessive broadcasts reduce the bandwidth available to end-users and require every node on the network to process every frame, regardless of whether it is the intended recipient of the data. The processor in each machine is responsible for doing this task, taking away from the processing power needed for the end-user applications.

As more and more broadcasts enter your network, the network can actually grind to a halt. This situation is known as a *broadcast storm*. Broadcast storms occur when broadcasts throughout the LAN use up all available bandwidth, bringing it to a complete stop. Switches use VLANs to segment the network into smaller broadcast domains. This chapter looks at the two different types of VLANs, both static and dynamic.

Note Token Ring, Fast Ethernet, Gigabit Ethernet, and Fiber Distri- buted Data Interface (FDDI) interfaces can be found on Cisco switches as well.

Name and describe two switching methods.

Cisco LAN switches primarily use three different switching methods: store-and-forward, cut-through, and FragmentFree. This section discusses all three methods. LAN switch methods are used to determine how a frame is handled when it is received on a switch port. You should know all three LAN switch types for the CCNA exam.

Throughout this book you will hear the term *latency*. Device latency is a term that describes the amount of time it takes for a frame or packet to enter a network device, for the device to make a decision as to which port or ports the data should exit, and then for the data to completely exit the device port. Network latency is the time it takes for data to get from the sending host or device to the destination host or device.

Critical Information

The device latency for packet switching through the switch depends on the chosen switching mode. Let¡¯s take a look at the three types of switching methods:

- Store-and-forward
- Cut-through
- FragmentFree, or modified cut-through

Store-and-Forward

Store-and-forward switching is one of two primary types of LAN switching. In this method, the LAN switch copies the entire frame into its onboard buffers and computes the cyclic redundancy check (CRC), which is a value, contained in the frame. The CRC is derived from taking every bit contained in the frame, computing a mathemati- cal value, and placing it at the end of a frame. A switch operating in store-and-forward mode will calculate the number of bits received in the frame and match that value with the value located in the CRC portion of the frame. If the values do not match, the switch assumes that an error occurred during transport of the frame, and the frame is discarded.

Note If the frame is fewer than 64 bytes including the CRC, the frame is considered a runt. If the frame is more than 1518 bytes including the CRC, it is considered a giant.

If the frame doesn¡¯t contain any errors, the LAN switch looks up the destination address in its forwarding or switching table and determines the outgoing interface. The switch uses the forwarding or switching table to forward packets based on manually configured information or information the switch has learned from the devices connected to the ports. The switch then forwards the frame toward its destination. Because this type of switching copies the entire frame and runs a CRC, latency can vary depending on frame length. This is the mode used by Cisco Catalyst 5000 Series switches.

Cut-Through

In this method, the LAN switch copies only the destination address (the first six bytes following the preamble) into its onboard buffers. It then looks up the destination address in its switching table, determines the outgoing interface, and forwards the frame toward its destination. A cut-through switch reduces 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. When the error rate falls below the threshold, the port automatically changes back to cut- through mode.

FragmentFree (Modified Cut-Through)

This is a modified form of cut-through switching in which the switch waits for the collision windows, which are 64 bytes long, 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 almost no increase in latency. The FragmentFree LAN switch type looks into the data field of the frame.

Figure 1.1 shows where the different switching modes take place in the frame.

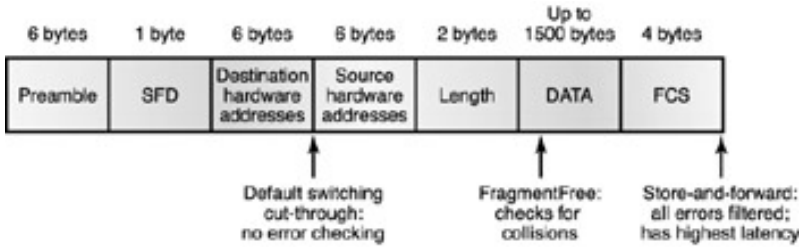

Figure 1.1: Different switching modes within a frame

Exam Essentials

Remember that FragmentFree is also referred to as ¡°modified cut- through.¡± FragmentFree switching looks into the data field of the frame.

Key Terms and Concepts

broadcast storm This occurs when network broadcasts use up all the available bandwidth in the network, bringing the network to a complete stop.

cyclic redundancy check (CRC) Mathematical algorithm used to check for errors when a frame, packet, or segment has been transmitted through a network.

latency Time lapse between when a port receives a frame and when it is forwarded to another port.

Distinguish between cut-through and store-and-forward LAN switching.

There are crucial differences between the cut-through and store-and-forward switching methods. You might think that since cut-through switching is much faster, it would be the default on Cisco¡¯s higher-end switches. However, it is just the opposite. Store- and-forward switching is turned on by default on many of the high- end Layer 2 switching modules.

Critical Information

The last section looked at both store-and-forward and cut-through switching. This section takes a closer look at them and examines their crucial differences.

Store-and-Forward

Cisco¡¯s higher-end LAN switches are called multilayer switches because they operate at Layer 3 and sometimes even higher layers. These switches all use store-and-forward by default. With store-and-forward switching, the switch waits for the entire frame to be buffered. The CRC at the end of the frame is computed, then checked (as is the size of the frame for runts, fragmented packets, and giants). As mentioned earlier, a runt is a frame that is smaller than 64 bytes; a giant is a frame that contains more than 1518 bytes.

When the switch determines that the frame is error free, the switch looks up the destination address in its switching or forwarding table and determines the outgoing port or ports. Only frames that are error free are forwarded out of the destination port or ports; frames containing errors are dropped.

Cut-Through

Using the cut-through switching method, the LAN switch copies only the destination address that is contained in the first 14 bytes of the frame received by the switch. The destination address is only eight bytes long, but there is a six-byte preamble in the front of the frame. After copying the destination address into its onboard buffers, the switch looks up the destination address in its switching or forwarding table to determine the port or ports that the frame will exit. Since only the first 14 bytes are read, the cut-through switch reduces the device latency and will begin to forward the frame as soon as it reads the destination address and makes a decision as to which port or ports the data will exit. The switch can actually be forwarding the frame before the entire frame is received.

Many Cisco switches can be configured to use cut-through switching until a pre-defined error threshold is reached. It then switches automatically to the slower store-and-forward mode. After the error rate returns to numbers below the threshold, the switch port or ports automatically return to cut-through mode.

Exam Essentials

Know the difference between cut-through and store-and-forward. The cut-through method of LAN switching has a consistent latency because the switch reads only the first eight bytes of the frame after the preamble. Store-and-forward reads the entire frame; therefore, latency varies with frame length.

Key Terms and Concepts

cut-through LAN switching method that looks only at the destination hardware address in a frame before making forwarding decisions.

FragmentFree LAN switching method that checks for errors by looking at the first 64 bytes of a frame after it has been received at a switch port.

store-and-forward LAN switching method that copies the entire frame to onboard buffers and runs a CRC before making forwarding decisions.

Describe the operation of the Spanning Tree Protocol and its benefits.

If the data you sent came right back to you through a secondary connection, would this help your network? In some ways it would, I suppose. It would eat up your bandwidth, it would be a security nightmare, and every interface on your network would have to keep reading it over and over continuously. It would be great to send out an e-mail and pick it up a week later with a sniffer continuing to loop around your network, wouldn¡¯t it? Imagine how many times your friend would get that e-mail. I guess it wouldn¡¯t be that much of good thing. So what do we do in an Ethernet network when we need to make sure we have secondary paths to a destination? Well, that is where a good understanding of Spanning Tree Protocol (STP) becomes important.

Critical Information

This section talks about the main purpose of STP, which is to stop network loops from occurring on your Layer 2 network (bridges or switches). STP is used to constantly monitor the switch ports and to make sure the protocol knows of all the links in your network. If more than one link exists, STP disables the secondary link until it is needed. This way the switch shuts down redundant links, putting a stop to any data loops in the network.

The STP process elects a root bridge in the network 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 these operate in what is called a forwarding state. Forwarding state ports send and receive traffic.

If you have other switches in your network, as shown in Figure 1.2, then these are non-root bridges. The switch uses a special algorithm called the *spanning-tree algorithm (STA)* to determine a cost to assign to each link based on the bandwidth of each hop from one switch in the network to another switch. A cost can also be assigned manually to each port. The port that has the lowest cost to the root bridge is called a root port, which sends and receives traffic.

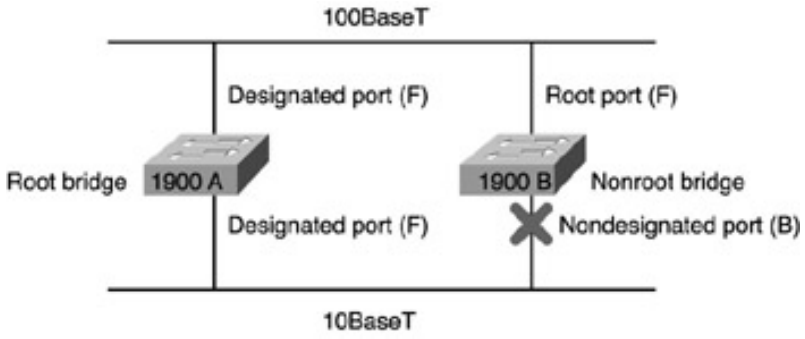

Figure 1.2: Spanning-tree operations

Ports that are determined to have the lowest-cost path to the root bridge are also called designated ports and, like root bridge ports, they operate in forwarding state (noted as *F* in the illustration). Other ports on the bridge are considered nondesignated, and will not send or receive traffic. This is called blocking mode (noted as *B* in the illustration). STP is enabled by default on most Cisco switches with Ethernet or FastEthernet ports.

Selecting the Root Bridge

Switches or bridges running STP exchange information with bridge protocol data units (BPDUs). BPDUs are used to send configuration messages using multicast frames, carrying the bridge ID of each device to other devices.

The bridge ID is used to determine the root bridge in the network and to determine the root port. The bridge ID is eight bytes long and includes the device¡¯s priority value and its MAC address. The default priority on all devices running the IEEE STP version is 32768.

To determine the root bridge, the bridge¡¯s priority and the MAC address are combined. If two switches

or bridges have the same priority value, then the lower MAC address is used to determine who has the lowest ID.

For example, if two switches use the default priority of 32768, then the MAC addresses are compared. If switch A¡¯s MAC address is 0000.0c00.1111.1111 and switch B¡¯s MAC address is 0000.0c00.2222.2222, then switch A becomes the root bridge.

Selecting the Designated Port

To determine the port or ports that will be used to communicate with the root bridge, the path cost is determined. The STP cost is an accumulated total path cost based on the bandwidth of the links. Table 1.1 shows the typical costs associated with the different Ethernet networks. The IEEE 802.1D specification has recently been revised to handle the new higher-speed links; the 1900 switches use the *original* IEEE 802.1D specifications.

Table 1.1: Typical Costs of Various Ethernet Networks:

Speed	New IEEE Cost	Original IEEE Cost
10Gbps	2	1
1Gbps	4	1
100Mbps	19	10
10Mbps	100	100

Spanning-Tree Port States

The ports on a bridge or switch running STP can transition through four different states:

Blocking Won¡¯t forward frames, listens to BPDUs. All ports are in blocking state by default when the switch is powered up.

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 Sends and receives data on the bridge port.

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 even if 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. Once a switch determines the best path to the root bridge, then all other ports will be in blocking state. Blocked ports still receive BPDUs.

If a switch determines that a blocked port should now be the designated port, it will go into listening state. The port will check all incoming BPDUs heard to make sure that the switch wouldn¡¯t create a data loop if the port goes into forwarding state.

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 to make 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 state to forwarding state is 50 seconds. It is not recommended to change the default STP timers, but these can be adjusted if need be. The time it takes to transition a port from listening to learning state or from learning to forwarding state is called the forward delay.

Spanning-Tree Example

In Figure 1.3, the three switches all have the same priority of 32768. However, notice the MAC address of each switch. By looking at the priority value and MAC address of each switch, you should be able to determine the root bridge.

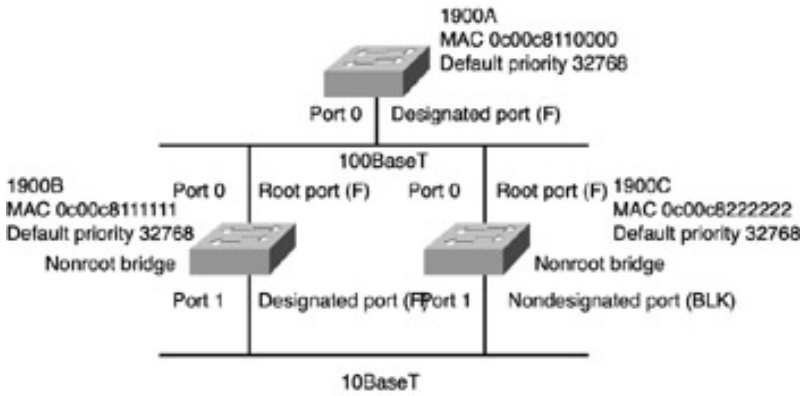

Figure 1.3: Spanning-tree example

Since 1900A has the lowest MAC address and all three switches use the default priority, then 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. Since the connection from both switches to the root switch is from port 0 using a 100Mbps link, that port has the best cost and will be the root port for both switches.

To determine the designated ports on the switches, the bridge ID is used. The root bridge always has all ports as designated. However, since both 1900B and 1900C have the same cost to the root bridge, the designated port will be on switch 1900B because it has the lowest bridge ID. 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. The next section looks at an example of the procedures needed to configure the Cisco Catalyst 1900 Series switch.

Necessary Procedures

This section takes a step-by-step look at verifying the STP configuration, which can be essential to troubleshooting.

Verifying STP Information

To verify if STP is configured and running on a switch, you can use the `show spantree` (`sh span` for short) command. This will show you information for VLAN 1 only. To see information about other VLANs running STP, use `show spantree` *`[vlan #]`*, as seen here:

```
1900A#sh span
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 occured 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]
```

The `show spantree` command displays the STP information for VLAN 1. Notice that the bridge ID, MAC address, and timers are displayed. The output "VLAN 1 is executing the IEEE compatible Spanning Tree Protocol" is telling you that STP is running on this VLAN.

Exam Essentials

Understand how a designated port is determined. To determine the designated ports on switches, the bridge ID is used. All ports of the root bridge are always designated ports.

Understand how root ports are determined. To determine the root ports on switches, you need to look at the cost of the link connecting the switches.

Understand how the root bridge is elected. The root bridge is determined by the bridge¡¯s priority and MAC address.

Key Terms and Concepts

802.1D IEEE specification for STP.

root bridge Switch that includes the designated port with the highest priority or the lowest MAC address.

spanning-tree algorithm (STA) System used to calculate a loop-free network topology for STP.

Spanning Tree Protocol (STP) A protocol that uses the spanning- tree algorithm to map the best path through the network and block ports that can create a redundant path for data in the network.

Describe the benefits of virtual LANs.

When you use a hub, all the ports on it are part of the same network. If you have multiple hubs daisy-chained together, you may have a rather large network or broadcast domain. Switches won¡¯t segment your broadcast domains by default because all ports are initially configured to VLAN1. You can use virtual local area networks (VLANs) to break up your large broadcast domains into much smaller ones. You can set up ports connecting switches called *trunks* to transport traffic from all the VLANs assigned to ports in your network. This allows you to assign individual ports on one switch to a VLAN and assign ports on another switch to use the same VLAN. VLANs can be created by location, function, department¡ªeven by the application or protocol used¡ªregardless of where the resources or users are located.

Critical Information

You can assign VLANs manually (static VLAN) or let the switch assign the VLAN (dynamic VLAN). With a *static VLAN*, you assign the VLAN number to a port, and then the switch maintains that VLAN assignment until it is manually changed. This type of VLAN configuration is easy to set up and monitor. This also controls the movement of users within the network. Using network management software to configure the ports can be helpful but is not mandatory.

A *dynamic VLAN* determines a node¡¯s VLAN assignment automatically. Using intelligent management software, you can enable hardware (MAC) addresses, protocols, or even applications to create dynamic VLANs. 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. If a user moves, the switch will automatically assign him or her to the correct VLAN. However, more administration is needed initially to set up the database.

Cisco administrators can use the VLAN Management 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¨Cto- VLAN mapping database.

Note VLAN Membership Policy Server (VMPS) is implemented in order to maintain a database of MAC addresses associated with an identified VLAN for use with dynamic VLAN assignments.

Necessary Procedures

To configure VLANs on a switched internetwork, you need to follow the steps listed below:

1. Configure the VLANs.
2. Assign switch ports to VLANs.
3. Identify the VLANs.
4. Verify the configuration.

Configuring VLANs

Configuring VLANs is the easy part of the job. Actually, it¡¯s understanding which users you want in each VLAN that is time consuming. Once you have decided the number of VLANs you want to create and the users who will be members of each, you can create your VLAN.

To configure VLANs on the 1900 Series switch, choose K from the initial user interface menu to get into IOS configuration. Even though you can create VLANs with the menu system available with the 1900 switch, we show only how to configure VLANs with the 1900 switch CLI. This is because it is the Cisco IOS, and also because the CCNA exam objectives cover only the CLI method of configuration on the 1900 switch.

The following switch output is the console display when connecting to a 1900 switch. Press **K** to enter the CLI mode:

```
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].
```

Enter global configuration mode using the `enable` command and then `config t` (short for `configure terminal`). To configure VLANs on an IOS-based switch, use the `vlan` *`[vlan#]`* `name` *`[vlan_name]`* command. The following example demonstrates how to configure VLANs on the switch by creating three VLANs for three different departments:

```
>en
#config t
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
```

After you create the VLANs that you want, you can use the `show vlan` command to see the configured VLANs. However, notice that all ports on the switch are in VLAN 1 by default. To change the VLAN associated with a port, you need to go to each interface and tell it what VLAN to be a part of. 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. Once the VLANs are created, verify your configuration with the `show vlan` command (`sh vlan` for short). For instance:

```
1900EN#sh 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
-------------------------------------
[output cut]
```

Now that you can see the three VLANs created, you can assign switch ports to a VLAN. Normally, each port can be part of only one VLAN. Trunking is used to overcome the one-VLAN rule and make a port available to one or more VLANs at a time.

Assigning Switch Ports to VLANs

You can configure each port to be in a VLAN by using the `vlan- membership` command. You can configure VLANs only one port at a time. There is no command to assign more than one port at a time to a VLAN with the 1900 switch.

Remember that you can configure either static memberships or dynamic memberships on a port. This book and the Cisco CCNA exam objectives cover static VLAN memberships only.

In the following example, we configure interface 2 to VLAN 2, interface 4 to VLAN 3, and interface 5 to VLAN 4:

```
1900EN#config t
Enter configuration commands, one per line.
End with CNTL/Z
1900EN(config)#int e0/2
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)#int e0/4
1900EN(config-if)#vlan-membership static 3
1900EN(config-if)#int e0/5
1900EN(config-if)#vlan-membership static 4
1900EN(config-if)#exit
1900EN(config)#exit
```

Now, type **sh vlan** again to see the ports assigned to each VLAN:

```
1900EN#sh 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
-------------------------------------
[output cut]
```

Note You could also use `show vlan <#>` to gather information about only one VLAN at a time. Another command you can use to see the ports assigned to a VLAN is `show vlan-membership`.

Identifying VLANs

VLANs can span multiple connected switches. Switches in this switch fabric must keep track of frames and of which VLAN they belong to. Frame tagging, discussed in the next section, performs this function. Switches can then direct frames to the appropriate port.

There are two different types of links in a switched environment:

Access Link A link that is part of only one VLAN and 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 the frame is sent to an access link device. Access link devices cannot communicate with devices outside their VLAN unless the packet is routed through a router.

Trunk Link A link that can carry multiple VLANs. Originally named after the trunks of the telephone system, which carry multiple telephone conversations, trunk links are used to connect switches to other switches, to routers, or even to servers. Trunked links are supported on Fast Ethernet or Gigabit Ethernet only. To identify the VLAN that a frame belongs to with Ethernet technology, Cisco switches support two different 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.

Note For more information on identifying VLANs, see Chapter 6 of *CCNA: Cisco Certified Network Associate Study Guide,* 3rd ed. (Sybex, 2002).

Verifying the Configuration

An internetwork switch needs a way to keep track of users and frames as they travel the switch block. A *switch block* is a group of switches sharing the same VLAN information. As the frame traverses through each switch from the port of entry to the port of exit, the highway of wires, processors, and ASICs between the ports is referred to as the *switch fabric*.

VLAN frame identification, or *frame tagging*, is a relatively new approach that was specifically developed for switched communications. In this approach, a unique user-defined identifier is placed in the header of each frame as it¡¯s forwarded throughout the switch fabric. (This identifier is sometimes referred to as a VLAN ID or VLAN color.) The identifier is understood and examined by each switch prior to any broadcasts or transmissions to switch ports of other switches, routers, or end-station devices. When the

frame exits the switch fabric, the switch removes the identifier before the frame is transmitted to the target end-station.

All this means is that the switch tags a frame with a VLAN identifier that is used only within the switch fabric itself. Before that frame leaves the switch, it removes the VLAN ID, because nothing outside the switch would be able to understand that ID. There is one exception: When you run ISL, the VLAN ID is preserved as it passes over the ISL link.

The following points summarize frame tagging:

- Specifically developed for multi-VLAN, inter-switch communication.
- Places a unique identifier in the header of each frame.
- Removes identifier before frame exits switch on non-trunk links.
- Functions at the Data Link layer.
- Requires little processing or administrative overhead.
- Inter-Switch Link (ISL) frame tagging is a Cisco proprietary frame- tagging method that encapsulates an existing frame with the VLAN information.

Exam Essentials

Understand what a VLAN is. Virtual LANs are used to break up broadcast domains in a Layer 2 switched internetwork.

Understand how to configure static VLAN assignments. Static VLAN assignments are created by an administrator manually configuring each switch port to a VLAN.

Understand frame tagging. Frame tagging is used to keep track of frames as they traverse a trunked link. Cisco uses the proprietary ISL method of frame tagging on Fast Ethernet and Gigabit Ethernet links.

Key Terms and Concepts

frame tagging Method used to identify frame membership in a VLAN as the frame traverses a trunked link.

Inter-Switch Link (ISL) Cisco proprietary method of frame tagging for Fast Ethernet and Gigabit Ethernet links.

static VLAN Assignment of a switch port to a VLAN by an administrator.

virtual local area network (VLAN) A logical grouping of network users and resources connected to defined ports on the switch. A VLAN looks like, and is treated like, its own subnet.

Chapter 2: OSI Reference Model and Layered Communication

Cisco Certified Network Associate Exam Objectives Covered in This Chapter:

- Describe data link and network addresses and identify key differences between them.*(pages 24¡ª27)*
- Define and describe the function of the MAC address.*(pages 27¡ª29)*
- List the key internetworking functions for the OSI Network layer.*(pages 30¡ª33)*
- Identify at least three reasons why the industry uses a layered model.*(pages 33¡ª42)*
- Describe the two parts of network addressing; then identify the parts in specific protocol address examples.*(pages 42¡ª46)*
- Define and explain the five conversion steps of data encapsulation.*(pages 46¡ª49)*
- Describe connection-oriented network service and connectionless network service, and identify their key differences.*(pages 50¡ª53)*
- Identify the parts in specific protocol address examples.*(pages 53¡ª53)*
- Describe the advantages of LAN segmentation.*(pages 53¡ª55)*
- Describe LAN segmentation using bridges and switches.*(pages 56¡ª58)*
- Describe the benefits of network segmentation using routers.*(pages 58¡ª59)*

This chapter has many functions. It will familiarize you with the OSI Reference Model, IP addressing, IPX addressing, the reasons for a layered model, the steps of data encapsulation, connection-oriented networks, and reasons for segmenting your LAN. We cover a lot of information in this chapter, which is why it¡¯s the biggest one in the book. Knowing the items in this chapter is critical for passing the exam.

Describe data link and network addresses and identify key differences between them.

The Data Link and Network layers of the OSI model are responsible for addressing local and network data. One layer uses logical addresses; the other layer uses physical addresses. This section briefly covers Media Access Control (MAC) addresses used at the Data Link layer and protocol addresses used at the Network layer. Although there are other Network-layer protocols, this section focuses on the implementation of Internet Protocol (IP) at this layer. Chapter 3 looks at Network-layer protocols including routing with IPX.

Critical Information

Let¡¯s first concentrate on the Data Link layer, since this is the layer at which physical addresses that are assigned to network interface cards (NICs) are installed on the local hosts. Many people do not realize that there is actually a 48-bit address individually assigned to every NIC. Although you may buy a case of NICs from many different manufacturers, they all are coded with a unique *MAC address*.

Discussed later in this chapter, frames are data units at the Data Link layer (layer 2 of the OSI model). Each frame is composed of a Data Link¨Clayer header, data from the upper OSI layers, and a trailer. Cisco¡¯s definition of what the Data Link layer provides is reliable transit of data across a physical network link. The OSI defines many specifications for this layer regarding different network and protocol characteristics. This includes the physical addressing, network topology, error notification, sequencing of frames, and flow control. Let¡¯s take a look at each one:

- Physical addresses are defined as the MAC addresses assigned to the NIC card at the Data Link layer.
- The network topology is how devices are connected to the network.
- The error notification process alerts the OSI model¡¯s upper layers of a transmission error.
- Sequencing is important. If data frames arrive out of sequence, a real problem might occur if the receiving device had no way of knowing the correct sequence.
- *Flow control* is used to manage how many frames are sent to a receiving device to keep the receiver from being overwhelmed with more frames than it can process or buffer.

MAC addresses are divided into two parts: a 24-bit manufacturer¡¯s identifier called the organizationally unique identifier (OUI), and a 24-bit vendor-supplied number or serial number that is unique to any other address the manufacturer has assigned to their cards. This makes MAC addresses 48 bits in length. These 48 bits are expressed with 12 hexadecimal digits, as in this example: 00D0.5966.A8AD or 00-D0-59-66-A8-AD (depending on the operating system or software used to display it). The vendor code would be the 00-D0-59, and the serial number would be 66-A8-AD.

MAC addresses are called *burned-in addresses (BIAs)*, or hardware addresses, because they are burned into read-only memory (ROM) on the installed host interface. The MAC address is copied into random access memory (RAM) when the interface initializes. The Network layer needs to map a logical address such as an IP address to the hardware address. Mappings can be statically created; however, mappings can be made dynamically using the Address Resolution Protocol (ARP), which is discussed in the next section.

The Network layer, also known as layer 3 of the OSI model, defines an address that differs significantly from the MAC address. Network- layer protocol addresses allow systematical comparison of the source network address and the destination network address. Routers use learned IP address information and routing protocols to make the best determination of how to route Network-layer data packets through the network. (Packets are the data unit used at the Network layer. They are composed of the Network-layer header, encapsulated upper-layer data, and a trailer.)

The CCNA exam focuses on two different types of logical addresses: IP addresses and IPX addresses. We will discuss these in more detail later in this chapter, but let¡¯s look quickly at how IP and IPX addresses differ from the layer 2 MAC addresses.

An IP address is made up of 32 bits of information. These bits are divided into four sections, referred to

as *octets* or bytes, each containing one byte (eight bits). Most often, IP addresses are shown in dotted-decimal form. An example would be 198.1.1.1.

An IPX address uses 80 bits, or 10 bytes, of data. The first four bytes show the network address, and the last six bytes always represent the node address, which is the MAC address. An example is 00007C80.0000.8609.33E9. The first eight hex digits (00007C80) represent the network portion of the address.

Exam Essential

Remember the differences between MAC and Network-layer addresses. You should know that MAC addresses are assigned to a physical device¡¯s interface. Network addresses are assigned by a protocol running on the device.

Key Terms and Concepts

burned-in address (BIA) The address burned into the ROM on a NIC.

flow control A way of controlling the speed of data from a sending device to a receiving device.

MAC address This is the address that is assigned to the local NIC. It is burned into the ROM on the NIC, and the address is unique to any other NIC.

Define and describe the function of the MAC address.

The Institute of Electrical and Electronics Engineers (IEEE) has subdivided the Data Link layer into two sublayers called the Logical Link Control (LLC) and Media Access Control (MAC). This section details the functions of MAC addresses and how they are used at layer 2 of the OSI Reference Model.

Critical Information

The MAC sublayer is used to create unique addresses used by Network- layer protocols to map the network address to the interface address so data can be routed to the interface. As mentioned earlier, MAC addresses are 48 bits in length and displayed as 12 hexadecimal digits. The first six hexadecimal digits are used to identify the manufacturer or vendor who produced the network interface. The second part of the MAC address is six hexadecimal digits composing a serial number assigned by the interface¡¯s manufacturer or vendor.

Also explained above, MAC addresses are called burned-in addresses (BIAs), or hardware addresses, because they are burned into read-only memory (ROM). Different Network-layer protocol suites use unique methods to perform mappings from their addresses to the MAC address. For example, IP uses *Address Resolution Protocol (ARP)*.

A device on the network that needs to send data to another network device must know where the device resides in order to send data to it. When the destination device resides on a remote network, the sending host sends an ARP request for the MAC address of its default gateway. The host receives a reply with the MAC address of the default gateway and then sends the data, including the IP address of the destination host, to the router. The router then forwards the data to the next hop based on information learned or manually inserted into the router¡¯s routing table. This occurs for each hop the data takes through the networks needed to deliver the data packets to the network on which the destination host resides.

Once the destination router receives the data, it checks an ARP table to see if it knows the MAC address assigned to the host it received data for. If the router does not find an entry in its table for the IP address, it sends an ARP broadcast on the network to learn the MAC address for the receiving host. The device using the IP address listed in the ARP broadcast returns the message with a reply containing the MAC address the host is using.

Another way of mapping MAC addresses to the Network-layer addresses is the *Hello Protocol*. This Network-layer protocol allows hosts to identify themselves and indicate that they are still functioning on the network. When a new host joins the network, it sends a hello message advertising itself. The other hosts on the network each send hello replies containing their MAC addresses to indicate their existence on the network. At specific intervals, hello messages are also sent to all the devices on the network to notify other hosts on the network they are still on the network.

A third way of mapping ARP addresses is called *predictable MAC addressing*. There are three protocols that use predictable MAC addresses: Xerox Network Service (XNS), Novell Internetwork Packet Exchange (IPX), and DECnet Phase IV. These protocols embed the MAC address into the Network-layer addresses they use on the network.

Exam Essentials

Know how IP uses ARP. It is important to remember how ARP is used with IP. When a host needs to know the MAC address of a local host, the device will send an ARP request and wait for a reply with the MAC address of the device to which it needs to send data.

Remember the Network-layer protocols that use predictable MAC address mappings. The three protocols that use predictable MAC addresses are XNS, IPX, and DECnet.

Key Terms and Concepts

Address Resolution Protocol (ARP) Used to find hardware addresses and map them to IP addresses.

Hello Protocol Uses broadcasts on the network to advertise MAC addresses on the network.

predictable MAC addressing A method of using MAC addresses in the Network-layer addresses used by XNS, IPX, and DECnet.

List the key internetworking functions for the OSI Network layer.

The OSI model was created in the late 1970s to help facilitate data transfer between network nodes. One of the greatest functions of the OSI specifications is help in data transfer between disparate hosts. This means that you could transfer data between a Unix host and a PC, for example.

You must have a fundamental understanding of the different layers of the OSI model, and this objective lays the groundwork you need.

Critical Information

The *OSI (Open Standards Interconnect) Reference Model* is not physical; rather, it is a set of guidelines that application developers can use when creating and implementing applications to run on a network. It also provides a framework for creating and implementing networking standards and devices, and internetworking schemes. There are many reasons why you must understand the model, and Cisco thinks this knowledge is especially important for troubleshooting and understanding data conversion in internetworks.

The OSI model is the primary architectural model for networks. It describes how user data and network information are communicated from an application on one computer to an application on another computer through the network media. The OSI Reference Model breaks this approach into seven layers, which are divided into two groups. The top three layers define how the applications within the end stations will communicate with each other and with users. The lower four layers define how data is transmitted, end to end. Figure 2.1 illustrates the three upper layers and their functions.

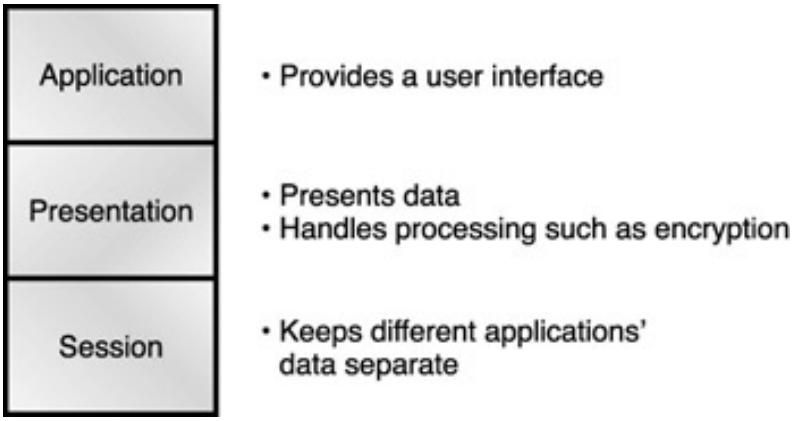

Figure 2.1: The upper layers of the OSI model

In Figure 2.1, you can see that the user interfaces with the computer at the Application layer, and also that the upper layers are responsible for applications communicating between hosts. Remember that none of the upper layers knows anything about networking or network addresses. That is the responsibility of the four bottom layers, which are shown in Figure 2.2.

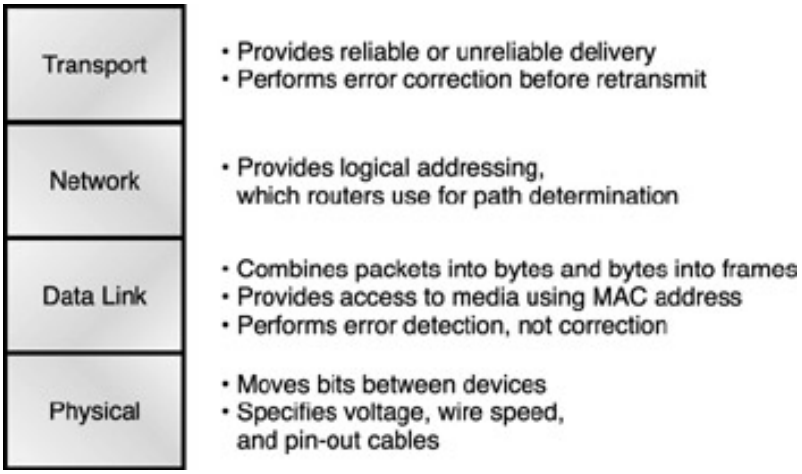

Figure 2.2: The lower, or data flow, layers

The four bottom layers define how data is transferred through a phy- sical wire, how it moves through switches and routers, and how to rebuild a data stream from a transmitting host to a destination host¡¯s application.

The following objective describes the seven layers in detail.

The primary responsibility of the OSI model¡¯s layer 3 is to route data from one network to another, to route updates from one router to another, and network addressing. Routers are considered Network-layer devices. Routing updates allow routers to know of other networks and where to send data that needs to traverse through other routers in the network. This means that there are two packet types: data and route update.

Data Packets Used to transport user data through the internetwork; protocols used to support data traffic are called routed protocols. Examples of routed protocols are IP and IPX.

Route Update Packets Used to update neighboring routers about networks connected to routers in the internetwork. Protocols that send route update packets are called routing protocols; examples include RIP, EIGRP, and OSPF. Route update packets are used to help build and maintain routing tables on each router.

Routers are used to break up broadcast domains. This means, by default, that broadcasts are not forwarded through a router. This is good. Routers also break up collision domains, but this can also be accomplished through layer 2 switches. Each interface in a router is a separate network and must be assigned unique network identification numbers. Each host on the network connected to that router must use that same network number.

Some points about routers that you must remember:

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

Exam Essential

To pass the exam, OSI knowledge is essential. You will not be able to pass the CCNA exam without a complete understanding of the OSI model and how the protocols function within it.

Key Term and Concept

OSI (Open Standards Interconnect) Reference Model Network architectural model developed by the International Organization for Standardization (ISO) and ITU-T in 1977. Their basic purpose was to develop a data communication standard for multivendor interoper- ability. The OSI model consists of seven layers, each with different specifications.

Identify at least three reasons why the industry uses a layered model.

One of the first things to understand is that Cisco presents many different reasons why the industry uses a layered model. Here we will define the reasons that we think are the most important for you to remember for the exam. You should have a fundamental understanding of the OSI model, including knowing why the industry uses a model and what the benefits are. Knowing this can help you fulfill business requirements in the real world as well as prepare for the CCNA exam.

Critical Information

There are many advantages to using a layered model. Because developers know that another layer will handle functions they¡¯re not currently working on, they can confidently focus on just one layer¡¯s functions. This promotes specialization. Another benefit is that if changes to protocols are made to one layer, it doesn¡¯t necessarily change protocols within the other layers. A third big advantage of using layered models is *compatibility*. If software developers adhere to the specifications outlined in the reference model, all the protocols written to conform to that model will work together. This is a very good thing. Compatibility creates the foundation for a large number of protocols to be written and used.

Cisco¡¯s official reasons for why the industry uses a layered model include the following:

- It clarifies general functions rather than specifics.
- It divides the complexity of networking into more manageable sublayers.
- It uses standard interfaces to enable ease of interoperability.
- It allows developers to change the features of one layer without changing all the code.
- It permits specialization, which helps the industry progress.
- It eases troubleshooting.

The OSI Reference Model Layers

The International Organization for Standardization (ISO) is the Emily Post of the network protocol world. Just like Ms. Post, who wrote the book setting the standards¡ªor protocols¡ªfor human social interaction, the ISO developed the OSI Reference Model as the guide and precedent for an open network protocol set. Defining the etiquette of communication models, it remains today the most popular means of comparison for protocol suites. The OSI model¡¯s seven layers are illustrated in Figure 2.3. The diagram also shows the functions defined at each layer.

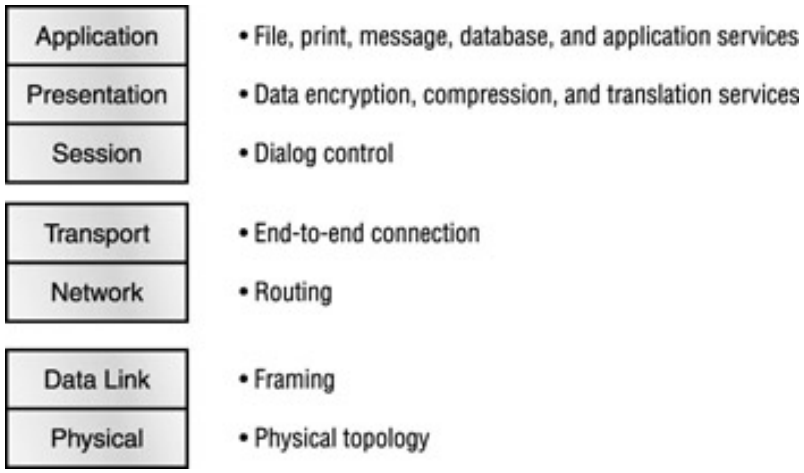

Figure 2.3: The OSI layers and their functions

Since the focus on the CCNA test is the OSI Reference Model¡¯s seven layers, let¡¯s take a close look at these layers in the order of layer 7 through layer 1:

- Application
- Presentation
- Session
- Transport
- Network
- Data Link
- Physical

Application Layer

The Application layer of the OSI model supports the communication components of an application and provides network services to application processes that span beyond the OSI model specifications.

The Application layer is also responsible for the following:

- Understanding the resources needed to communicate between two devices and establishing their availability
- Synchronizing applications on the server and client
- Agreeing on error control and data integrity of communicating applications
- Providing system-independent processes or program services to end-users

Presentation Layer

The Presentation layer is so named because it presents data to the Application layer. It¡¯s essentially a translator, making sure that the data sent from one system is readable by the Application layer of the receiving station. The Presentation layer is responsible for code formatting, conversion, and negotiating the data transfer syntax for the Application layer.

A successful data-transfer technique is to convert the data into a standard format before transmission. Computers are configured to receive this generically formatted data and then convert the data back into its native format for actual reading (for example, EBCDIC to ASCII). It is important to remember that the Presentation layer is the only layer that can actually change data.

The OSI has protocol standards that define how standard data should be formatted. Tasks such as data compression, decompression, encryption, and decryption are associated with this layer.

Session Layer

The Session layer is responsible for setting up, managing, and then tearing down sessions between Presentation-layer entities. The Session layer also provides dialog control between devices, or nodes. It coordinates communication between systems, and serves to organize their communication by offering three different modes¡ªsimplex, half-duplex, and full-duplex. Basically, the Session layer keeps different applications¡¯ data separate from other applications¡¯ data.

Transport Layer

Services located in the Transport layer both segment and reassemble data from upper-layer applications and unite it onto the same data stream. They provide end-to-end data transport services and can establish a logical connection between the sending host and destination host on an internetwork.

Some of you might already be familiar with TCP and UDP (which you will learn about in Chapter 3) and how TCP is a reliable service but UDP is not. Application developers have their choice of the two protocols when working with TCP/IP protocols.

The Transport layer is responsible for providing mechanisms for multiplexing upper-layer application, session establishment, and teardown of virtual circuits. It also hides details of any network- dependent

information from the higher layers by providing transparent data transfer. The use of the term *virtual circuits* here should not confuse you. Cisco uses the phrase as a way of identifying the process here at the Transport layer. This may be confusing to some, because virtual circuits are also used to establish connections over serial links.

Flow Control

Data integrity is ensured at this layer by maintaining flow control and by allowing users the option of requesting reliable data transport between systems. Flow control prevents a sending host on one side of the connection from overflowing the buffers in the receiving host¡ªan event that can result in lost data. Reliable data transport employs a connection-oriented communication session between systems, and the protocols involved ensure that the following will be achieved:

- The segments delivered are acknowledged back to the sender upon their reception.
- Any segments not acknowledged are retransmitted.
- Segments are sequenced back into their proper order upon arrival at their destination.
- A manageable data flow is maintained in order to avoid congestion, overloading, and the loss of any data.

Network Layer

The Network layer is responsible for routing through an internetwork and for network addressing using *logical addressing*. Logical addressing is the term used for protocol addressing to define the network address and uniquely define hosts in a network. This means that the Network layer is responsible for transporting traffic between devices that are not locally attached. *Routers*, or layer 3 devices, are specified at the Network layer and provide the routing services in an internetwork.

When a packet is received on a router interface, the destination IP address is checked. If the packet is not destined for the router, then the router will look up the destination network address in the routing table. Once an exit interface is chosen, the packet will be sent to the interface to be framed and sent out on the local network. If the entry for the destination network is not found in the routing table, the router drops the packet.

Data Link Layer

The Data Link layer ensures that messages are delivered to the proper device and translates messages from the Network layer into bits for the Physical layer to transmit. It formats the message into data frames and adds a customized header containing the hardware destination and source addresses. This added information forms a sort of capsule that surrounds the original message in much the same way that engines, navi- gational devices, and other tools were attached to the lunar modules of the Apollo project. These various pieces of equipment were useful only during certain stages of space flight and were stripped off the module and discarded when their designated stage was complete. Data traveling through networks is much the same. Figure 2.4 shows the Data Link layer with the Ethernet and IEEE specifications.

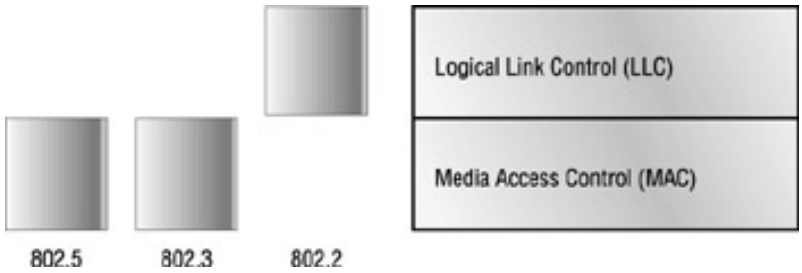

Figure 2.4: The Data Link layer

You need to understand that routers, which work at the Network layer, do not care about where a host is located, but only where networks are located. They also keep track of the best way to get to a remote network. The Data Link layer is responsible for uniquely identifying each device on a local network.

Note Bridges and switches are typically used at the Data Link layer for segmenting the network. Hubs, devices also used at this layer, are merely repeaters, so the same signal sent to one device in the network is propagated to all the devices attached to the hub.

For a host to send packets to individual hosts and between routers, the Data Link layer uses *hardware*

addressing. Each time a packet is sent between routers, it is framed with control information at the Data Link layer, but that information is stripped off at the receiving router, and only the original packet is left completely intact. This framing of the packet continues for each hop until the packet is finally delivered to the receiving host. It is important to understand that the packet was never altered along the route, only encapsulated with the type of control information to be passed upon the different media types.

The IEEE Ethernet Data Link layer has two sublayers:

Media Access Control (MAC) 802.3 This sublayer defines how packets are placed on the media. Contention media access is first- come, first-serve media access, where everyone shares the same bandwidth. Physical addressing is defined here as are logical topologies. Logical topology is the signal path through a physical topology. Line discipline, error notification (not correction), ordered delivery of frames, and optional flow control can also be used at this sublayer.

Logical Link Control (LLC) 802.2 This sublayer is responsible for identifying Network-layer protocols and then encapsulating them. An LLC header is used to tell the Data Link layer what to do with a packet once a frame is received. For example, a host will receive a frame and then look in the LLC header to understand that the packet is destined for the IP protocol at the Network layer. The LLC can also provide flow control and sequencing of control bits.

Physical Layer

The Physical layer has two responsibilities: it sends bits and receives bits. Bits come only in values of 1 or 0¡ªa Morse code with numeric value. The Physical layer communicates directly with the various types of actual communication media. Different kinds of media represent these bit values in different ways. Some use audio tones, while others employ state transitions¡ªchanges in voltage from high to low and low to high. Specific protocols are needed for each type of media to describe the proper bit patterns to be used, how data is encoded into media signals, and the various qualities of the physical media¡¯s attachment interface.

The Physical layer specifications specify the electrical, mechanical, procedural, and functional requirements for activating, maintaining, and deactivating a physical link between end-systems.

At the Physical layer, the interface between the data terminal equipment (DTE) and the data communication equipment (DCE) is identified. The DCE is usually located at the service provider, while the DTE is the attached device. The services available to the DTE are most often accessed via a modem or channel service unit/data service unit (CSU/DSU).

The connectors and different physical topologies are defined by the OSI as standards, which allow disparate systems to communicate because of these standard interfaces. The CCNA course and exam are interested only in the Ethernet standards.

Hubs at the Physical Layer

Hubs are really multiple-port repeaters. A repeater receives a digital signal, reamplifies or regenerates it, then forwards it out all active ports without looking at any data. An active hub does the same thing. Any digital signal received from a segment on a hub port is regenerated or reamplified and transmitted out all ports on the hub. This means that all devices plugged into a hub are in the same collision domain as well as in the same broadcast domain. A broadcast domain is defined as all devices on a network segment that hear all broadcasts sent on that segment.

Hubs, like repeaters, do not look at any traffic as it enters and is transmitted out to the other parts of the physical media. Hubs create a physical star network where the hub is a central device and cables extend in all directions, creating the physical star effect. However, Ethernet networks use a logical bus topology. This means that the signal has to run from end to end of the network. Every device connected to the hub, or hubs, must listen if a device transmits.

Exam Essentials

Know the different layers and their functions. Just knowing the order of the layers won¡¯t suffice. You must have a good understanding of what function each layer provides, including its protocols and specifications. Study this information hard.

Understand the different devices used at the various layers. Routers are defined at the Network layer, bridges and switches at the Data Link layer, and hubs at the Physical layer.

Remember why developers use layered models. Ease of troubleshooting, a standard interface, and industry specialization are three good reasons Cisco gives for using a layered model in the networking industry.

Key Terms and Concepts

compatibility This is a key reason for reference models. Application developers can ensure compatibility between disparate systems if they use the specifications of a layered model, such as the OSI Reference Model.

hardware addressing Defined at the Data Link layer, hardware addressing is used to uniquely define hosts on a LAN. Hardware addresses are 48 bits long (six bytes).

logical addressing Defined at the Network layer, logical addressing is used to define the network address and uniquely define hosts in an internetwork.

routers Defined at the Network layer, routers break up broadcast domains by default and provide logical addressing of a network.

switches Defined at the Data Link layer, switches break up collision domains. Switches allow you to segment broadcast domains by port by assigning them to different virtual LANs, making each VLAN its own broadcast domain.

Describe the two parts of network addressing; then identify the parts in specific protocol address examples.

For this objective, you need to be able to identify the network identifier in an IP and IPX address as well as the node address portion that identifies the individual host. The host address is a unique address not assigned to any other device on the same network. You may also need to know what networks are valid on the inside and which are not.

Note This section does not discuss subnetting, which is covered in Chapter 3.

Critical Information

Let¡¯s take a look at the components of IP and IPX addresses and how to identify the network identifier from the node¡¯s unique address.

IP Addresses

An *IP address* is a numeric identifier assigned to each machine on an IP network. It designates the location of a device on the network. An IP address is made up of 32 bits of information. These bits are divided into four sections, referred to as octets or bytes, each containing one byte (eight bits). The network address uniquely identifies each network. Every machine on the same network shares that network address as part of its IP address. In the IP address 172.16.30.100, for example, 172.16 is the network address.

The node address is assigned to, and uniquely identifies, each machine on a network. This part of the address must be unique because it identifies a particular machine¡ªan individual¡ªas opposed to a network, which is a group. This number can also be referred to as a host address. In the sample IP address 172.16.30.100, 30.100 is the node address. The network address of an IP address can differ based on the subnet mask used. In the example here, we used a 24-bit subnet mask, which equals 255.255.255.0. See Chapter 3 to learn about the different subnet masks and how to subnet.

In a *Class A IP address*, only the first octet identifies the network. This means that the address would be viewed as *network.node.node.node*. How do you know if it is a Class A address? The network address will always be from 1 to 126. Technically, the 127 network is also a Class A network, but the network is reserved for diagnostics and the address of 127.0.0.1 is reserved for loopbacking on the local interface. The 10 network (along with the 127 network) is not valid on the Internet¡ªit is used for internal addressing.

Class B IP addresses are a little trickier. If the first octet has a value between 128 and 191, the address is a Class B network. The second octet is still part of the network address but can be any value under 255. So the IP address would be viewed as *network.network.node.node*. The 172.16 network is a Class B network that is not valid on the Internet¡ªit is used for internal addressing.

Class C IP addresses are just about as tricky as the Class B. The first three octets identify the network, leaving only 254 available hosts in each network. Class C networks always start with a value of 192 to 223 and would be viewed as *network.network.network.node*. The 192.168.10 network is reserved for internal network addressing¡ªyet another network not valid for use on the Internet.

Note Remember that values in an octet can never be lower than 0 or higher than 255. A 255 in the node address portion of the last octet always indicates that the address is a broadcast address.

IPX Addresses

An *internetwork Packet Exchange (IPX) address* is 80 bits, or 10 bytes, long, which is significantly longer than an IP address. As with TCP/IP addresses, IPX addresses are hierarchical and divided into network and node portions. The first four bytes always represent the network address, and the last six bytes always represent the node address. There¡¯s none of that Class A, Class B, or Class C TCP/IP stuff in IPX addressing¡ªthe network and node portions of the address are always the same length. After subnet masking, this is sweet indeed!

IPX addresses are also shown in hex digits. This means that every value in the address must be

between 0 and 9 or between the letters A through F. It can never be any other letter, which is good to remember since exams try to confuse you by placing other letters in the IPX addresses.

The actual node address is always the MAC address assigned to the NIC on the machine using the IPX protocol. A MAC address is always 12 hex digits; for example, AB23.45FF.3428. The network portion of the address can be up to eight hex digits long; for example, A6B32398. Put the network address and the node address together, and it looks like this: A6B32398. AB23.45FF.3428. They can be deceiving too. If you have a small network address such as the network 00002374, then the IPX address can look like this: 2374. AB23.45FF.3428.

Exam Essentials

Remember the parts of an IP address for each class. You need to remember that a Class A IP address is viewed as *network.node.node.node,* a Class B IP address is shown as *network.network.node.node*, and a Class C is shown as *network.network.network.node*.

Remember the parts of an IPX address. An IPX address is made up of up to 8 hex digits for the network address and the remainder of the address are the 12 hex digits taken from the MAC address assigned to the NIC card of the machine using IPX.

Key Terms and Concepts

Class A IP address An IP address where only the first octet identifies the network. The network address will always be between 1 and 126, and shown in only the first octet. The address would be viewed as *network.node.node.node*.

Class B IP address An IP address where the first octet has a value between 128 and 191. The second octet is still part of the network. The address is viewed as *network.network.node.node*.

Class C IP address An IP address where the first three octets identify the network. Addresses always start with a value of 192 to 223. The address is viewed as *network.network.network.node*.

IP address Network address assigned to a node on a network. Used to send and receive packets or datagrams on an internetwork. The address is 32-bits long and consists of three individual octets.

Internetwork Packet Exchange (IPX) address Novell copied a protocol stack developed by Xerox (which they called XNS) and called it IPX. It is used for routing packets through an internetwork and for network addressing.

Define and explain the five conversion steps of data encapsulation.

Data encapsulation is 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. Cisco considers the five conversion steps to be from data, then to segment, then to packet, then to frame, and then to bits. Let¡¯s take a close look at the data encapsulation process.

Critical Information

When a host transmits data across a network to another device, the data is encapsulated with protocol information at each layer of the OSI model. Each layer communicates only with its peer layer on the receiving device.

To communicate and exchange information, each layer uses protocol data units (PDUs). These hold the control information attached to the data at each layer of the model, typically attached to the header of the data field but in some instances in the trailer, or end, of the data field.

Each PDU is attached to the data by encapsulating the data at each layer of the OSI model. A specific name is given to each PDU depending on the information each header has. Only the peer layer on the receiving device reads this PDU information; it is then stripped off, and the data is handed to the next upper layer.

Figure 2.5 shows the PDUs and how they attach control information to each layer.

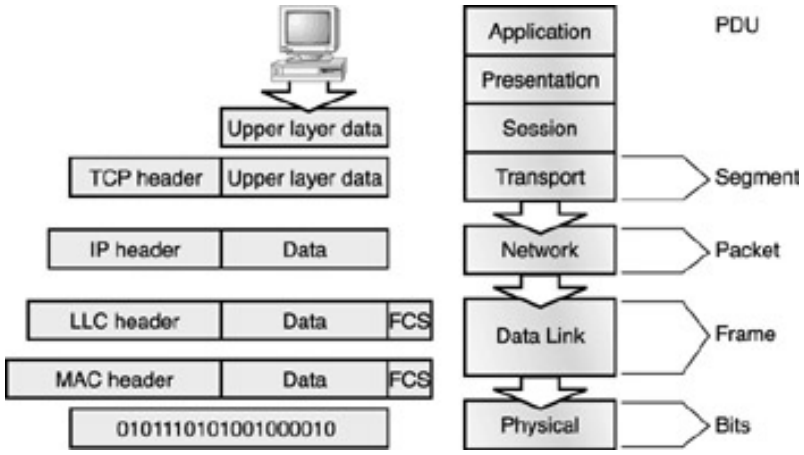

Figure 2.5: Data encapsulation

Figure 2.5 shows how the upper-layer user data is converted for transmission on the network. This data stream is handed down to the Transport layer, which sets up a virtual circuit to the receiving device by sending a sync packet. The data stream is then broken up into smaller pieces, a Transport-layer header (PDU) is created, and the header control information is attached to the header of the data field. The result is a *segment*. Each segment is sequenced so the data stream can be put back together on the receiving side exactly as transmitted.

Each segment is then handed to the Network layer for network addressing and routing through an internetwork. Logical addressing is used¡ªfor example, IP¡ªto get each segment to the correct network. The Network-layer protocol adds a control header to the segment handed down from the Transport layer, and the entire block is now called a *packet,* or datagram. Remember that the Transport and Network layers work together to rebuild a data stream on a receiving host. However, they have no responsibility for placing their PDUs on a local network segment, which is the only way to get the information to a router or host.

The Data Link layer is responsible for taking packets from the Network layer and placing them on the network medium (cable or wireless). The Data Link layer encapsulates each packet in a *frame*, and the frame¡¯s header carries the hardware address of the source and destination local hosts. If the device is on a remote network, then the frame is sent to a router, to be routed through an internetwork. Once it

gets to the destination network, a new frame is used to get the packet to the destination host.

To put this frame on the network, it must first be put into a digital signal. Since a frame is really a logical group of *bits*, the Physical layer is responsible for taking these digits and encapsulating them into a digital signal, which is read by devices on the same local network. The receiving devices will synchronize on the digital signal and extract the 0s and 1s from the digital signal. At this point, the devices build the frame, run a cyclic redundancy check (CRC), and check their answer with the answer in the Frame Check Sequence (FCS) field of the frame. If it matches, the packet is pulled from the frame, and the frame is discarded. This process is called de-encapsulation.

When the packet is handed to the Network layer, the address is checked. If the address matches the address of the local device, the segment is pulled from the packet, and the packet is discarded. The segment is processed at the Transport layer, which rebuilds the data stream and acknowledges that it received each piece to the transmitting station. It then happily hands the data stream to the upper-layer application.

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. If you are using a connection- oriented protocol, a reliable connection is established between the transmitting and receiving hosts. If you are using a protocol such as UDP, the segment is sent unreliable.

3. Segments are converted to packets or datagrams, and the logical address is placed in the header so each packet can be routed through an internetwork.

4. Packets or datagrams are converted to frames for transmission on the local network. Hardware (Ethernet) addresses are used to uniquely identify hosts on a local network segment.

5. Frames are converted to bits, and a digital encoding and clocking scheme is used.

Exam Essential

Memorize the encapsulation method of each layer. Remember, from the upper layers down, this is the encapsulation method: user data at the Application, Presentation, and Session layers; segments at the Transport layer; packets, or datagrams, at the Network layer; frames at the Data Link layer; and bits at the Physical layer.

Key Terms and Concepts

bits The Physical layer takes the binary data handed down from the Data Link layer and converts 0s and 1s to a digital signal to be sent out over the physical topology.

frames Frames house the packets, or datagrams, handed down from the Network layer to be delivered to a device on a LAN.

packets Sometimes called datagrams, packets house the segments handed down from the Transport layer to be routed through an internetwork.

segments Defined at the Transport layer, these are parts of a data stream that are handed down from the upper layers to be transmitted to a destination device.

Describe connection-oriented network service and connectionless network service, and identify their key differences.

Connectionless and connection-oriented services can be used at almost all layers of the OSI model, and the decision to use them at any given layer is completely up to the application developer. Understanding the differences will help you troubleshoot an internetwork, configure Cisco routers correctly, and find the correct answers on the CCNA exam. This objective describes the connection-oriented network service.

Critical Information

When talking about the difference between connection-oriented and connectionless network service, people usually refer to an actual protocol as an example. For instance, IP is connectionless, and TCP is connection-oriented. This is true; however, these are just protocols that use the specifications of the Network and Transport layers to set up and deliver data to network devices. They do not actually define the network service.

This objective discusses the actual connection-oriented service used at the Transport layer. However, remember that connection-oriented services can be used at almost any layer of the OSI model, but that the CCNA exam is concerned with only the connection-oriented service at the Transport layer.

Connection-Oriented Communication

In reliable transport operation, one user first establishes a *connection- oriented* session with its peer system. Figure 2.6 portrays a typical reliable session taking place between sending and receiving systems. In it, both hosts¡¯ application programs begin by notifying their individual operating systems that a connection is about to be initiated. The two operating systems communicate by sending messages over the network, confirming that the transfer is approved and that both sides are ready for it to take place. Once the required synchronization is complete, a connection is fully established, and data transfer begins.

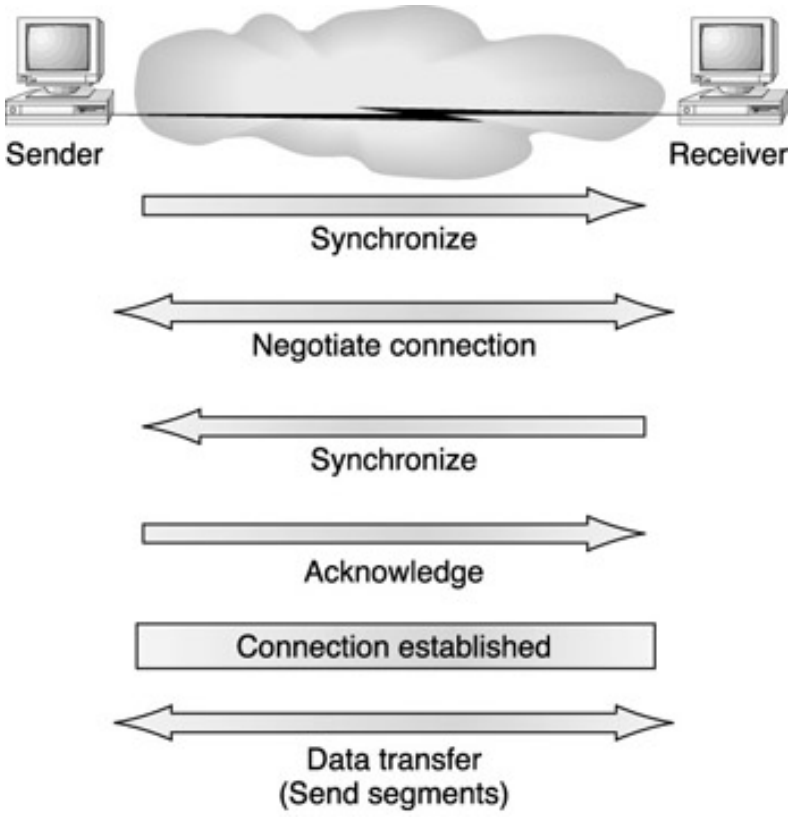

Figure 2.6: Establishing a connection-oriented session

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

The following summarizes the steps in a connection-oriented session pictured in Figure 2.6:

1. The first ¡°connection agreement¡± segment is a request for synchronization.

2. The second and third segments acknowledge the request and establish connection parameters between hosts.

3. The final segment is also an acknowledgment. It notifies the destin- ation host that the connection agreement is accepted and that the actual connection has been established. Now data transfer can begin.

The steps of a connection-oriented session are sometimes summarized into the following steps:

1. Call setup, which consists of each segment in Figure 2.6 down to ¡°Connection established¡±

2. Data transfer, the last segment in Figure 2.6 and step 3 in the previous list

3. Call termination (not shown in the figure)

Connectionless Protocols

Connectionless protocols can be used in applications that do not want the overhead associated with setting up a virtual circuit. As mentioned previously, the application developers decided on what type of connection service to use. This objective gives you the basic information regarding connectionless models.

Connectionless protocols can be used to save a tremendous overhead over connection-oriented protocols. Perhaps the best and most often used analogy displaying the difference between connectionless and connection-oriented communication is the difference between sending a postcard and a registered letter. A connectionless network service is similar to sending a postcard. You put the correct source and destination host addresses on the postcard and then drop it in the mailbox. Does it get to its destination? You hope so. Since the message on the postcard is probably not a matter of life or death, you don¡¯t need an acknowledgment of its receipt. Using this type of delivery saves time and overhead, but at the cost of reliability.

Data sent using a connection-oriented protocol is like sending a registered letter. The sending device receives a confirmation that the destination host received the data. This adds a lot of overhead in terms of speed, bandwidth, and processor usage. Because of the overhead and the reliability of today¡¯s networks, many application developers prefer to use connectionless over connection-oriented service.

Exam Essential

Understand what makes a reliable session. It is important to understand how to create a reliable connection with a virtual circuit.

Key Terms and Concepts

connection-oriented Data transfer that requires the establishment of a virtual circuit. The sending device receives a reply from the receiving device that no data was lost in transit. This creates a reliable session. Typically called a reliable connection.

connectionless Data transfer that does not use a virtual circuit. Typically described as best-effort delivery of datagrams.

Identify the parts in specific protocol address examples.

For information pertaining to this objective, see the objective ¡°Describe the two parts of network addressing; then identify the parts in specific protocol address examples,¡± earlier in this chapter.

Describe the advantages of LAN segmentation.

This section gives a general understanding of the benefits of LAN segmentation.

Critical Information

One of the biggest advantages of LAN *segmentation* is the ability to increase the bandwidth available to the users on the network. Each user can be confined to different LAN segments that confine broadcasts and other traffic to individual segments.

In addition, by segmenting a LAN, you can overcome the distance limitations of the LAN cabling, decrease collisions, decrease broadcast traffic, decrease multicast traffic, improve throughput in the network, and decrease latency.

Let¡¯s take a look at the following topics, which Cisco believes are advantages of network segmenting:

- Security
- Broadcast Control
- Performance
- Scalability

Security

By segmenting, you improve your network¡¯s security by isolating groups by task, location, or department. Those users who need more security can be segmented into their own network. Data shared between these users can be seen only by those users who are on the same network, and users who are not part of their network cannot communicate with them.

Broadcast Control

This is one of the main reasons for segmenting your network with switches and VLANs. Too many broadcasts on the network can really slow things down. Whether you use a hub or a switch, every PC on the network that is part of the same VLAN has to attempt to process the broadcast. Switches can isolate collision domains for attached hosts and forward only appropriate traffic to particular ports. Layer 3 VLANs can provide complete isolation of data between different user groups, even if they are connected to the same switch.

Performance

By segmenting your network, you eliminate broadcasts and limit the number of users who are sending traffic down your cabling. Since cabling does not have an unlimited capacity, anything you do to segment users away from your cabling eliminates data traffic and increases the amount of bandwidth available.

If you contain data traffic originating on a particular network, you avoid wasting bandwidth. VLANs are one of the best solutions for eliminating broadcasts and segmenting the network.

Scalability

Segmenting adds to your network¡¯s scalability, particularly in LANs that have heavy broadcast or multicast network environments.

Exam Essential

Know the benefits of segmenting the LAN. Segmenting the LAN allows you to overcome cabling distance limitations, and to decrease broadcasts, multicasts, and collisions. This lets you to improve throughput, latency, and the amount of total bandwidth for each user.

Key Term and Concept

segmentation The use of LAN devices such as routers, bridges, and switches to decrease the size of a LAN and the number of users, increase distance limitations, improve network throughput, and decrease the amount of traffic on the local LAN.

Describe LAN segmentation using bridges and switches.

This section does not deal with how to segment the LAN, and it barely touches on the reasons to use switches, bridges, or VLANs to segment your network. These items were covered in the last chapter. This section is here to verify your knowledge of the advantages of segmenting your LAN and the differences between switches and bridges.

Note The Cisco objectives list for this objective actually lists it as three separate objectives. However, for simplicity¡¯s sake, we¡¯ve combined these into two objectives, this one and the following.

Critical Information

As mentioned earlier, there are many reasons to segment your network, including excessive broadcasts on the network and heavy data traffic. You can use a router, you can use a switch, you can use VLANs, you can hook up two PCs and use Microsoft Windows Multihoming, you can use a bridge, you can use a multiplayer switch. All these are devices or methods for segmenting your network.

Switches and bridges both work at the Data Link layer and filter the network by hardware addresses. Layer 2 switching is considered hardware-based bridging because it uses specialized hardware called an application-specific integrated circuit (ASIC). ASICs can run up to gigabit speeds with very low latency.

Bridges and switches read each frame as it passes through the network. The layer 2 device then puts the source hardware address in a filter table and keeps track of which port it was received on. This tells the switch where that device is located.

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

When a frame is received on a layer 2 device interface and the destination hardware address is unknown to the device, it will forward the frame to all connected segments. If the unknown device answers this forwarding of the frame, then the switch updates the filter table on the location of that device. However, the source address of the transmitting frame may be a broadcast address. The switch will forward all broadcasts or unknown unicasts out every interface, with the exception of the interface of arrival, by default. All devices that the broadcast is forwarded to are considered to be in the same broadcast domain. Layer 2 devices propagate layer 2 broadcast storms. The only way to stop a broadcast storm from propagating through an internetwork is with a layer 3 device (router).

The biggest difference between (and benefit of) using switches instead of hubs in your internetwork is that each switch port is its own collision domain, while a hub creates one large collision domain. Switches and bridges do not break up broadcast domains, and instead forward all broadcasts.

Another benefit of LAN switching over hub implementations is that one device on every segment plugged into a switch can transmit at the same time, because each segment is its own collision domain. Hubs allow only one device per network to communicate at a time.

Tip Switches cannot translate between different media types on the same segment.

Exam Essential

Know the differences between switches and bridges. Bridges create only one network, and all the devices attached to a bridge are in that network. Switches, which use VLANs, can assign each port to an individual network or VLAN.

Key Term and Concept

transparent bridging The bridging scheme used in Ethernet networks to pass frames one hop at a

time. This type of bridging uses MAC addresses and is considered transparent because the source node does not know it has been bridged. The destination frames are sent directly to the end node.

Describe the benefits of network segmentation with routers.

Now that we have discussed the benefits of segmenting the LAN and using switches or bridges to do so, let¡¯s look at a layer 3 solution using routers to segment the network into smaller LANs.

Critical Information

Routers are a very expensive way of segmenting your LAN into smaller networks. When you look at larger networks that need segmenting, you need to look at the per-port costs, and routers cost the most. However, they are a great way of segmenting your network because every port is not only its own broadcast domain and its own collision domain, but it is also its own network.

Multilayer switches using *virtual local area networks (VLANs)* provide the best and most manageable solution, as we learned in the last chapter. A logical grouping of users allows easier network management. Not only that, but to move users or create new networks, it is not necessary to run new cables or add new hardware. It is merely a configuration change on the switch. And the per-port costs in large networks are the lowest compared to all the other methods. Communication between each VLAN (network) needs a router, which is usually built in or comes as a module on Cisco multilayer switches.

There are several benefits to segmenting the LAN with a router. One of the biggest is that routers do not forward broadcasts and multicasts by default. Another reason is that distance limitations can be overcome because each segment can be created using the maximum distance allowable by the cable type being used. Additionally, routers can translate between multiple media types, while switches cannot. Finally, routers provide better manageability of the routing process, which allows you to configure the data paths used when there are redundant links.

Exam Essential

Know the main benefits of using routers to segment the network. The main benefits of using routers to segment the network are their ability to control the chosen path of data, their ability to translate between multiple media types, their control of forwarding broadcasts and multicasts, and better manageability.

Key Terms and Concepts

router A layer 3 device used to segment networks, route data traffic exiting its current network, and make routing solutions for VLANs.

virtual local area network (VLAN) A logical grouping of network users and resources connected to defined ports on the switch. A VLAN looks like, and is treated like, its own subnet.

Chapter 3: Network Protocols

Cisco Certified Network Associate Exam Objectives Covered in This Chapter:

- Describe the different classes of IP addresses (and subnetting).*(pages 62¡ª81)*
- Identify the functions of the TCP/IP network-layer protocol.*(pages 81¡ª88)*
- Identify the functions performed by ICMP.*(pages 88¡ª91)*
- Configure IP addresses.*(pages 92¡ª93)*
- Verify IP addresses.*(pages 93¡ª99)*
- List the required IPX address and encapsulation type.*(pages 100¡ª112)*

This chapter covers some very important information, but it provides only what you need to know for the CCNA exam. This book cannot cover TCP/IP and IPX in great detail. You should already have some understanding of IP addresses, IPX addresses, and IP subnetting. This chapter should act only as a refresher.

Describe the different classes of IP addresses (and subnetting).

An IP address is made up of 32 bits of information. These bits are divided into four sections, referred to as octets or bytes, each containing 1 byte (8 bits). You can depict an IP address using one of three methods:

- Dotted-decimal, as in 172.16.30.56
- Binary, as in 10101100.00010000.00011110.00111000
- Hexadecimal, as in AC 39 1E 38

The 32-bit IP address is a structured, or hierarchical, address, as opposed to a flat, or nonhierarchical, address. Although either type of addressing scheme could have been used, the hierarchical variety was chosen for a good reason.

The advantage of this scheme is that it can handle a large number of addresses, namely, almost 4.3 billion (a 32-bit address space with two possible values for each position¡ªeither 0 or 1¡ªgives you 2^{32}, or approximately 4.3 billion). The disadvantage of the flat addressing scheme, and the reason it¡¯s not used for IP addressing, relates to routing. If every address were unique, all routers on the Internet would need to store the address of each and every machine on the Internet. This would make efficient routing impossible, even if only a fraction of the possible addresses were used.

The solution to this dilemma is to use a two- or three-level, hierarchical addressing scheme that is structured by network and host, or by network, subnet, and host.

Critical Information

The network address uniquely identifies each network. Every machine on the same network shares that network address as part of its IP address. For example, in the IP address 172.16.30.56, 172.16 is the network address.

The node address is assigned to, and uniquely identifies, each machine on a network. This part of the address must be unique because it identifies a particular machine¡ªan individual¡ªas opposed to a network, which is a group. This number can also be referred to as a host address. In the sample IP address 172.16.30.56, 30.56 is the node address.

The designers of the Internet decided to create classes of networks based on network size. For the small number of networks possessing a very large number of nodes, they created the rank of Class A network. At the other extreme is the Class C network, which is reserved for the numerous networks with a small number of nodes. The class distinction for networks between very large and very small is predictably called the Class B network.

Subdividing an IP address into a network and node address is determined by the class designation of one¡¯s network. Figure 3.1 provides a summary of the three classes of networks, plus the D and E class addresses not used in production networks.

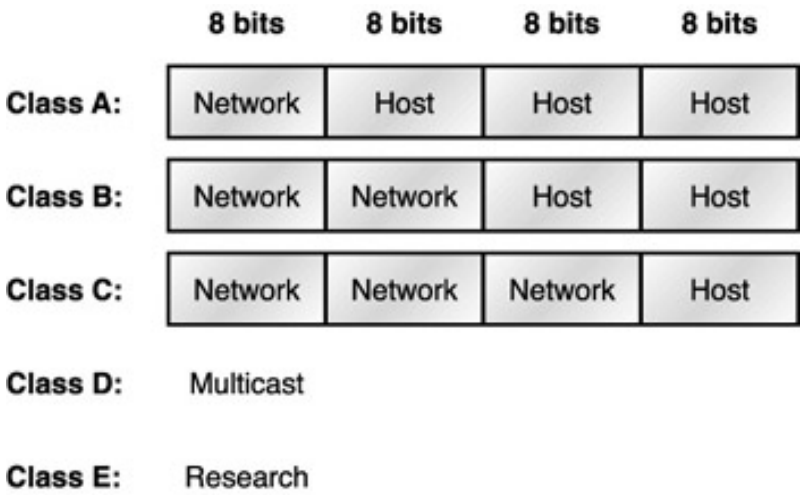

Figure 3.1: Summary of the five classes of network addresses

Some IP addresses are reserved for special purposes, and network administrators shouldn¡¯t assign these addresses to nodes. Table 3.1 lists the members of this exclusive little club and why they¡¯re included in it.

Table 3.1: Reserved IP Addresses:

Address	Function
Network address of all 0s	Interpreted to mean ¡°this network or segment.¡±
Network address of all 1s	Interpreted to mean ¡°all networks.¡±
Network address 127.0.0.1	Reserved for loopback tests. Designates the local node and allows that node to send a test packet to itself without generating network traffic.
Node address of all 0s	Interpreted to mean ¡°this node.¡±
Node address of all 1s	Interpreted to mean ¡°all nodes¡± on the specified network. For example, 128.2.255.255 means ¡°all nodes¡± on Class B network 128.2.
Entire IP address set to all 0s	Used by Cisco routers to designate the default route.
Entire IP address set to all 1s (same as 255.255.255.255)	Broadcast to all nodes on the current network; sometimes called an ¡°all 1s broadcast.¡±

Class A Network Addresses

In a Class A network address, the first byte is assigned to the network address, and the three remaining bytes are used for the node addresses. The Class A format is *net.node.node.node*. For example, in the IP address 49.22.102.70, the network address is 49, and 22.102.70 is the node address. Every machine on this particular network would have the distinctive network address of 49.

Class A network addresses are one byte long, with the first bit of that byte set to 0 and the seven remaining bits available for manipulation. As a result, the maximum number of Class A networks that can be created is 128. Why? Because each of the seven bit positions can be either a 0 or a 1, thus 2^7, or 128.

To complicate matters further, the network address of all 0s (00000000) is reserved to designate the default route (see Table 3.1, earlier). Additionally, the address 127, which is reserved for diagnostics, can¡¯t be used either, which means that you can use only the numbers one to 126 to designate Class A network addresses. This means the actual number of usable Class A network addresses is 128 minus two, or 126. Got it?

Each Class A network address has three bytes (24 bit positions) for the node address of a machine. Thus, there are 2^{24}¡ªthat¡¯s 16,777,216¡ª unique combinations and, therefore, precisely that many possible unique node addresses for each Class A network. Because the two address patterns of all 0s and all 1s are reserved, the actual maximum usable number of nodes for a Class A network is 2^{24} minus two, which equals 16,777,214.

Class A Valid Host IDs

Here is an example of how to figure out the valid host IDs in a Class A network address:

10.0.0.0	All host bits turned off is the network address.
10.255.255.255	All host bits turned on is the broadcast address.

The valid hosts are the numbers between the network address and the broadcast address: 10.0.0.1 through 10.255.255.254. Notice that 0s and 255s are valid host IDs. All you need to remember when trying to find valid host addresses is that the host bits cannot all be turned off or on at the same time.

Class B Network Addresses

In a Class B network address, the first two bytes are assigned to the network address, and the remaining two bytes are used for node addresses. The format is *net.net.node.node*. For example, in the IP address 172.16.30.56, the network address is 172.16, and the node address is 30.56.

With a network address being two bytes of eight bits each, there would be 2^{16} unique combinations. But the Internet designers decided that all Class B network addresses should start with the binary digit 1, then 0. This leaves 14 bit positions to manipulate and therefore 16,384 (that is, 2^{14}) unique Class B network addresses.

A Class B network address uses two bytes for node addresses. This is 2^{16} minus the two reserved patterns (all 0s and all 1s), for a total of 65,534 possible node addresses for each Class B network.

Class B Valid Host IDs

Here is an example of how to find the valid hosts in a class B network:

172.16.0.0	All host bits turned off is the network address.
172.16.255.255	All host bits turned on is the broadcast address.

The valid hosts would be the numbers between the network address and the broadcast address: 172.16.0.1 through 172.16.255.254.

Class C Network Addresses

The first three bytes of a Class C network address are dedicated to the network portion of the address, with only one measly byte remaining for the node address. The format is *net.net.net.node*. Using the example IP address 192.168.100.102, the network address is 192.168.100, and the node address is 102.

In a Class C network address, the first three bit positions are always the binary 110. The calculation is such: three bytes, or 24 bits, minus three reserved positions, which leaves 21 positions. Therefore, there are $2^{21,}$ or 2,097,152, possible Class C networks.

Each unique Class C network has one byte to use for node addresses. This leads to 2^8, or 256, minus the two reserved patterns of all 0s and all 1s, for a total of 254 node addresses for each Class C network.

Class C Valid Host IDs

Here is an example of how to find a valid host ID in a class C network:

192.168.100.0	All host bits turned off is the network address.
192.168.100.1	The first host.
192.168.100.254	The last host.
192.168.100.255	All host bits turned on is the broadcast address.

The valid hosts would be the numbers between the network address and the broadcast address: 192.168.100.1 through 192.168.100.254.

Subnetting

In the previous sections, you learned how to define and find the valid host ranges used in a Class A, a

Class B, and a Class C network address by turning the host bits all off and then all on. However, you were defining one network. What happens if you wanted to take one network address and create six networks from it? You would have to perform what is called *subnetting*, which allows you to take one larger network and break it up into many smaller networks.

Note Although it¡¯s possible to subnet Class A, we don¡¯t cover it here, as it¡¯s not relevant to the CCNA exam. You would need to know that for the CCNP test, though.

Subnet Masks

For the subnet address scheme to work, every machine on the network must know which part of the host address will be used as the subnet address. This is accomplished by assigning to each machine a subnet mask, a 32-bit value that allows the recipient of IP packets to distinguish the network ID portion of the IP address from the host ID portion.

The network administrator creates a 32-bit subnet mask composed of 1s and 0s; the 1s represent the positions that refer to the network or subnet addresses. Table 3.2 shows the default subnet masks for Classes A, B, and C.

Table 3.2: Default Subnet Mask

Class	Format	Default Subnet Mask
A	*net.node.node.node*	255.0.0.0
B	*net.net.node.node*	255.255.0.0
C	*net.net.net.node*	255.255.255.0

Subnetting Class C Network Addresses

In a Class C network address, only eight bits are available for defining the hosts. Remember that subnet bits start at the left and go to the right, without skipping bits. This means the subnet masks can be:

```
10000000 = 128
11000000 = 192
11100000 = 224
11110000 = 240
11111000 = 248
11111100 = 252
11111110 = 254
```

Now, the RFCs state that you cannot have only one bit for subnetting, since that would mean that the bit would always be either off or on, which would be illegal. So the first subnet mask that you can legally use is 192, and the last one is 252, since you need at least two bits for defining hosts.

When you have a subnet mask and need to determine the number of subnets, valid hosts, and broadcast addresses, all you need to do is answer five simple questions:

1. How many subnets does the subnet mask produce?
2. How many valid hosts per subnet?
3. What are the valid subnets?
4. What are the valid hosts in each subnet?
5. What is the broadcast address of each subnet?

Here is how you determine the answers to these questions:

1. 2^x ¡ª 2 = number of subnets. *x* is the number of masked bits, or the 1s. For example, 11000000 would give 2^2 ¡ª 2. In this example, there are two subnets.
2. 2^x ¡ª 2 = number of hosts per subnet. *x* is the number of unmasked bits, or the 0s. For example, 11000000 produces 2^6 ¡ª 2. In this example, there are 62 hosts per subnet.
3. 256 ¡ª subnet mask = base number. For example, 256 ¡ª 192 = 64.
4. Valid hosts are the numbers between the subnets, minus all 0s and all 1s.

5. Broadcast address is all host bits turned on, which is the number immediately preceding the next subnet.

Now, though this can seem confusing, it is easier than it looks. Just try a few practice examples and see for yourself. These following examples give you an opportunity to practice subnetting Class C network addresses using the method just described. You¡¯ll start with the first Class C subnet mask and work through a few subnets, and when you¡¯re done, you¡¯ll see just how easy this is with Class B networks, as well.

Practice Example 1: 255.255.255.192

In this example, you will subnet the following:

192.168.10.0	The network address
255.255.255.192	The subnet mask

Now, answer the five questions:

1. How many subnets? Since 192 is two bits on (11000000), the answer would be 2^2¡ª2 = 2 subnets. (The ¡°minus 2¡± is the subnet bits all on or all off, which are not valid by default.)

2. How many hosts per subnet? We have six hosts bits off (11000000), so the equation would be 2^6¡ª2 = 62 hosts.

3. What are the valid subnets? 256¡ª192 = 64, which is the first subnet and our base number or variable. Keep adding the variable to itself until you reach the subnet mask. 64 + 64 = 128. 128 + 64 = 192, which is invalid because it is the subnet mask (all subnet bits turned on). Our two valid subnets are then 64 and 128.

4. What are the valid hosts?

5. What is the broadcast address for each subnet? These are the numbers between the subnets; however, the number right before the next subnet is all hosts bits turned on and is the broadcast address. The easiest way to find the hosts is to write out the subnet address and the broadcast address. This way, the valid hosts are obvious. Table 3.3 shows the 64 and 128 subnets, the valid host ranges of each, and the broadcast address of both subnets.

Table 3.3: The 64 and 128 Subnet Ranges

Feature	Subnet One	Subnet Two
Subnet address (do this first)	64	128
First host (perform host addressing last)	65	129
Last host	126	190
Broadcast address (do this second)	127	191

Practice Example 2: 255.255.255.224

In this example, you will subnet the following:

192.168.10.0	The network address
255.255.255.224	The subnet mask

Ask the five questions:

1. How many subnets? 224 is 11100000, so the answer would be 2^3¡ª2 = 6.

2. How many hosts? 2^5¡ª2 = 30.

3. What are the valid subnets? 256¡ª224 = 32. 32 + 32 = 64. 64 + 32 = 96. 96 + 32 = 128. 128 + 32 = 160. 160 + 32 = 192. 192 + 32 = 224, which is invalid as it is our subnet mask (all subnet bits on). Our subnets are 32, 64, 96, 128, 160, and 192.

4. What are the valid hosts? For each valid subnet, the subnet number (such as 32, 64, and so on) is not a valid host and represents the network address. The last number in the subnet (33, 65,

and so on) represents the broadcast address. All the numbers in between the network address and the broadcast address are valid hosts.

5. What is the broadcast address for each subnet? First, just write out the subnets. Then write out the broadcast addresses, which is the number right before the next subnet. Finally, fill in the host addresses. The following chart shows all the subnets for the 255.255.255.224 Class C subnet mask.

Subnet Address	32	64	96	128	160	192
First Valid Host	33	65	97	129	161	193
Last Valid Host	62	94	126	158	190	222
Broadcast Address	63	95	127	159	191	223

Practice Example 3: 255.255.255.240

Let¡¯s practice on another one:

192.168.10.0	The network number
255.255.255.240	The subnet mask

Answer the five questions:

1. 240 is 11110000 in binary. 2^4¡ª2 = 14 subnets.

2. Four host bits, or 2^4¡ª2 = 14 hosts per subnet.

3. 256¡ª240 = 16. 16 + 16 = 32. 32 + 16 = 48. 48 + 16 = 64. 64 + 16 = 80. 80 + 16 = 96. 96 + 16 = 112. 112 + 16 = 128. 128 + 16 = 144. 144 + 16 = 160. 160 + 16 = 176. 176 + 16 = 192. 192 + 16 = 208. 208 + 16 = 224. 224 + 16 = 240, which is our subnet mask. So, our valid subnets are 16, 32, 48, 64, 80, 96, 112, 128, 144, 160, 176, 192, 208, and 224.

For questions 4 and 5, the following chart shows the pattern of the subnets, the valid hosts, and the broadcast addresses for each subnet.

Subnet Address	16	32	48	64	80	96	224
First Valid Host	17	33	49	65	81	97	225
Last Valid Host	30	46	62	78	94	110	238
Broadcast Address	31	47	63	79	95	111	239

Subnetting in Your Head: Class C Network Addresses

It is possible to perform subnetting in your head. Do you believe us? It¡¯s relatively easy. Take the following example:

192.168.10.33	The network address
255.255.255.224	The subnet mask

First, determine what subnet and broadcast address the above IP address is a member of. You can do this by performing step three in the five-step process: 256¡ª224 = 32. 32 + 32 = 64. Bingo. The address falls between the two subnets and must be part of the 192.168.10.32 subnet. The next subnet is 64, so the broadcast address is 63. Remember that the broadcast address of a subnet is always the number right before the next subnet. The valid host range is 33¨C62. This is getting too easy.

Let¡¯s try another one. Here, you will subnet another Class C network address. What subnet and broadcast address is this IP address a member of?

192.168.10.33	The network address
255.255.255.240	The subnet mask

256¡ª240 = 16. 16 + 16 = 32. 32 + 16 = 48. Yup, the host address is between the 32 and 48 subnet. The subnet is 192.168.10.32, and the broadcast address is 47. The valid host range is 33¨C46.

Subnetting Class B Network Addresses

Since we went through some of the possible Class C subnets, let¡¯s take a look at subnetting a Class B network. First, let¡¯s look at all the possible Class B subnet masks. Notice that we have far more possible subnets than with a Class C network address:

```
255.255.128.0
255.255.192.0
255.255.224.0
255.255.240.0
255.255.248.0
255.255.252.0
255.255.254.0
255.255.255.0
255.255.255.128
255.255.255.192
255.255.255.224
255.255.255.240
255.255.255.248
255.255.255.252
```

The Class B network address has 16 bits available for host addressing. This means we can use up to 14 bits for subnetting, since we must leave at least two bits for host addressing.

The process of subnetting a Class B network is the same as with Class C, except you just have more host bits. Use the same subnet numbers you used with Class C, but add a 0 to the network portion and a 255 to the broadcast section in the fourth octet. For example, this chart shows you a host range of two subnets used in a Class B network:

16.0	32.0
16.255	32.255

Just add the valid hosts between the numbers, and you¡¯re set.

Practice Example 1: 255.255.192.0

Here is a Class B example:

172.16.0.0	The network address
255.255.192.0	The subnet mask

1. 2^2 ¡ª 2 = 2 subnets.
2. 2^{14} ¡ª 2 = 16,382 hosts per subnet.
3. 256 ¡ª 192 = 64. 64 + 64 = 128.

For questions 4 and 5, the following chart shows the two subnets available, the valid host ranges, and broadcast address of each subnet.

Subnet Address	64.0	128.0
First Valid Host	64.1	128.1
Last Valid Host	127.254	191.254
Broadcast Address	127.255	191.255

Notice that we just added the fourth octet¡¯s lowest and highest values and came up with the answers. Again, these produce the same answers as a Class C subnet, but we added the fourth octet.

Practice Example 2: 255.255.240.0

Here is another example:

172.16.0.0	The network address
255.255.240.0	The subnet address

1. 2^4 ¡ª 2 = 14 subnets.
2. 2^{12} ¡ª 2 = 4094 hosts per subnet.

3. 256¡ª240 = 16, 32, 48, etc., up to 224. Notice that these are the same numbers as a Class C 240 mask.

For questions 4 and 5, the following chart shows the first three subnets, their valid hosts, and broadcast addresses:

Subnet Address	16.0	32.0	48.0
First Valid Host	16.1	32.1	48.1
Last Valid Host	31.254	47.254	63.254
Broadcast Address	31.255	47.255	63.255

Practice Example 3: 255.255.255.0

Contrary to popular belief, 255.255.255.0 is not a Class C subnet mask. It is amazing how many people see this mask used in a Class B network and say it is a Class C subnet mask. This is a Class B subnet mask with eight bits of subnetting; it is considerably different from a Class C mask. Subnetting this address is fairly simple:

1. 2^8¡ª2 = 254 subnets.
2. 2^8¡ª2 = 254 hosts per subnet.
3. 256¡ª255 = 1, 2, 3, etc., all the way to 254.

For questions 4 and 5, the following chart shows the first three and the last subnet, the valid hosts, and the broadcast addresses.

Subnet Address	1.0	2.0	3.0	254.0
First Valid Host	1.1	2.1	3.1	254.1
Last Valid Host	1.254	2.254	3.254	254.254
Broadcast Address	1.255	2.255	3.255	254.255

Practice Example 4: 255.255.255.128

This must be illegal! What type of mask is this? Don¡¯t you wish it were illegal? This is one of the hardest subnet masks you can play with. Actually, it is a good subnet to use in production, as it creates more than 500 subnets with 126 hosts per subnet. That¡¯s a nice mixture.

1. 2^9¡ª2 = 510 subnets.
2. 2^7¡ª2 = 126 hosts per subnet.
3. This is the tricky part. 256¡ª255 = 1, 2, 3, etc., for the third octet. However, you need to remember the one subnet bit used in the fourth octet. Remember when we showed you how to figure one subnet bit with a Class C mask? You figure this the same way. Now you know why we showed you the one-bit subnet mask in the Class C section: to make this part easier. You actually get two subnets for each third octet value, hence the 510 subnets. For example, if the third octet were showing subnet 3, the two subnets would actually be 3.0 and 3.128.

For questions 4 and 5, the following chart shows how you can create subnets, valid hosts, and broadcast addresses using the 255.255.255.128 subnet mask:

Subnet Address	0.128	1.0	1.128	2.0	2.128	3.0	3.128
First Valid Host	0.129	1.1	1.129	2.1	2.129	3.1	3.129
Last Valid Host	0.254	1.126	1.254	2.126	2.254	3.126	3.254
Broadcast Address	0.255	1.127	1.255	2.127	2.255	3.127	3.255

Practice Example 5: 255.255.255.192

This one gets just a little tricky. Both the 0 subnet and the 192 subnet could be valid in the fourth octet. It just depends on what the third octet is doing.

1. 2^{10}¡ª2 = 1022 subnets.

2. 2^6 ¡ª2 = 62 hosts per subnet.

3. 256¡ª192 = 64 and 128. However, as long as all the subnet bits in the third octet are not all off, then subnet 0 in the fourth octet is valid. Also, as long as all the subnet bits in the third octet are not all on, then 192 is valid in the fourth octet as a subnet.

For questions 4 and 5, the following chart shows the first seven subnet ranges, valid hosts, and broadcast addresses:

Subnet Address	0.64	0.128	0.192	1.0	1.64	1.128	1.192
First Valid Host	0.65	0.129	0.192	1.1	1.65	1.129	1.193
Last Valid Host	0.126	0.190	0.254	1.62	1.126	1.190	1.254
Broadcast Address	0.127	0.192	0.255	1.63	1.127	1.191	1.255

Notice that for each subnet value in the third octet, you get subnets 0, 64, 128, and 192 in the fourth octet. This is true for every subnet in the third octet except 0 and 255. The 0 subnet value in the third octet is demonstrated above. Notice, however, for the 1 subnet in the third octet, that the fourth octet has four subnets: 0, 64, 128, and 192.

Practice Example 6: 255.255.255.224

This is done the same way as the subnet mask above; we just get more subnets and fewer hosts per subnet available.

1. 2^{11} ¡ª2 = 2046 subnets.

2. 2^5 ¡ª2 = 30 hosts per subnet.

3. 256¡ª224 = 32, 64, 96, 128, 160, 192. However, as demonstrated above, both the 0 and 224 subnets can be used as long as the third octet does not show a value of 0 or 255. Here is a demonstration of having no subnet bits on in the third octet.

For steps 4 and 5, the following chart shows the first range of subnets:

Subnet Address	0.32	0.64	0.96	0.128	0.160	0.192	0.224
First Valid Host	0.33	0.65	0.96	0.129	0.161	0.193	0.225
Last Valid Host	0.62	0.94	0.126	0.158	0.190	0.222	0.254
Broadcast Address	0.63	0.95	0.127	0.159	0.191	0.223	0.255

Let¡¯s take a look at when a subnet bit is turned on in the third octet. The next chart shows the range of subnets available in the fourth octet:

Subnet Address	1.0	1.32	1.64	1.224
First Valid Host	1.1	1.33	1.65	1.225
Last Valid Host	1.30	1.62	1.94	1.254
Broadcast Address	1.31	1.63	1.95	1.255

And this chart shows the last subnet range:

Subnet Address	255.0	255.32	255.64	255.192
First Valid Host	255.1	255.33	255.65	255.193
Last Valid Host	255.30	255.62	255.94	255.222
Broadcast Address	255.31	255.63	255.95	255.223

Subnetting in Your Head: Class B Network Addresses

We know what you are thinking: ¡°Are you nuts?¡± Honest, it¡¯s actually easier than writing it out. We¡¯ll show you how with the next few quick examples. For each IP address, what subnet and broadcast address is it a member of?

IP Address	Subnet and Broadcast Address Calculation
172.16.10.33, mask 255.255.255.224	256¡ª224 = 32. 32 + 32 = 64. Bingo, 33 is between 32 and 64. However, remember that the third octet is considered part of the subnet, so the answer would be the 10.32 subnet. The broadcast is 10.63, since 10.64 is the next subnet.
172.16.90.66, mask 255.255.255.192	256¡ª192 = 64. 64 + 64 = 128. The subnet is 172.16.90.64. The broadcast must be 172.16.90.127, since 90.128 is the next subnet.
172.16.50.97, mask 255.255.255.224	256¡ª224 = 32, 64, 96, 128. The subnet is 172.16.50.96, and the broadcast must be 172.16.50.127, since 50.128 is the next subnet.
172.16.10.10, mask 255.255.255.192	256¡ª192 = 64. This address must be in the 172.16.10.0 subnet, and the broadcast must be 172.16.10.63.
172.16.10.10, mask 255.255.255.224	256¡ª224 = 32. The subnet is 172.16.10.0 with a broadcast of 172.16.10.31.

Network Access¨CLayer Protocols

The Network Access layer combines both the Physical and Data Link layers of the OSI model. The LAN media access protocols and phy- sical cabling topologies found here at this layer of the DoD (Department of Defense) model are listed below:

802.2 SNAP	FDDI
802.3 CSMA/CD	Category 1¨C5
802.5 Token Ring	PPP/SLIP
MAC Addressing	ATM
Ethernet II	Coaxial Cables

Exam Essentials

Understand how to find the valid hosts in a subnet. The best way to do this is to use the equation 256 minus the subnet mask. For example, if you have a 240 mask, you would use 256¡ª240. The result, 16, is your first subnet and your base number, or interval. Keep adding the base number to itself until you reach the value of the subnet mask. The valid hosts are the numbers between the subnets.

Understand how to find a broadcast address in a subnet. Once you find the valid subnets, you can find the valid hosts, which are the numbers between the subnets minus the broadcast address, which is the last number in the host range. For example, in a 240 mask, the first subnet is 16, and the second subnet is 32. That means the valid hosts are 17 through 30, with 31 being the broadcast address for that subnet.

Key Terms and Concepts

Class A Address class used to differentiate between a network and node within an IP address, creating very few large networks. The syntax is *net.node.node.node*.

Class B Address class used to differentiate between a network and node within an IP address. The syntax is *net.net.node.node*.

Class C Address class used to differentiate between a network and node within an IP address, creating many small networks. The syntax is *net.net.net.node*.

IP address Network address assigned to a node on a network. Used to send and receive packets or datagrams on an internetwork.

subnetting The breaking up of an IP network address into smaller networks.

Transmission Control Protocol (TCP) A connection-oriented protocol specified at the Host-to-Host layer of the DoD model.

Identify the functions of the TCP/IP Network-layer protocol.

This section starts off by taking a look at the Department of Defense¡¯s version of TCP/IP, and then compares it and its protocols with the OSI Reference Model discussed in Chapter 2. The last section looked at IP addressing. This section reviews the functions of TCP/IP at the Network layer.

Critical Information

IP uses the Department of Defense (DoD) model, which is a condensed version of the OSI model, composed of four¡ainstead of seven¡alayers. These layers are:

- The Process/Application layer
- The Host-to-Host layer
- The Internet layer
- The Network Access layer

Figure 3.2 shows a comparison of the four-layer DoD model and the seven-layer OSI model. As you can see, the two are similar in concept, but each has a different number of layers with different names.

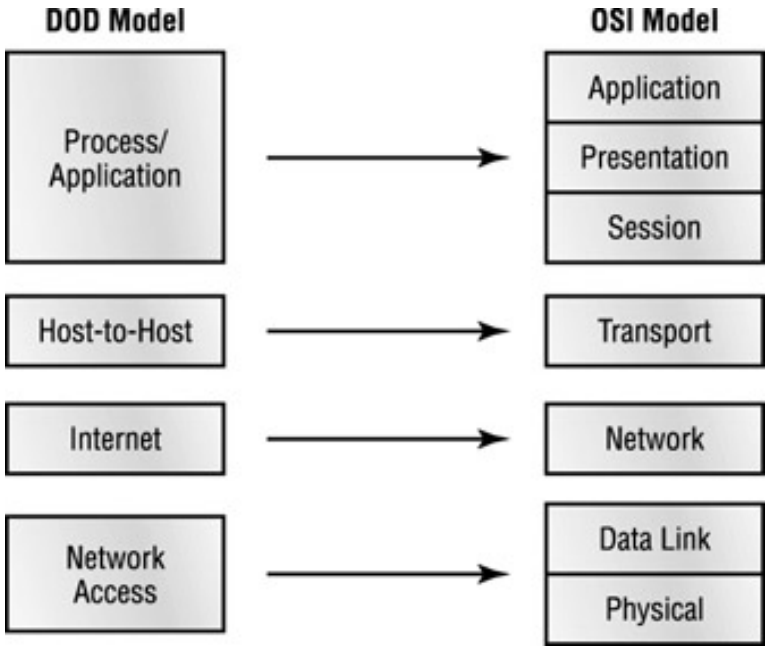

Figure 3.2: The DoD and OSI models

A vast array of protocols combine at the DoD model¡¯s Process/ Application layer to integrate the various activities and duties spanning the focus of the OSI¡¯s corresponding top three (Application, Presentation, and Session) layers. The Process/Application layer defines protocols for node-to-node application communication and also controls user interface specifications.

The DoD¡¯s Host-to-Host layer parallels the functions of OSI¡¯s Transport layer, defining protocols for setting up the level of transmission service for applications. It tackles issues like creating reliable end-to-end communication and ensuring the error-free delivery of data. It handles packet sequencing and maintains data integrity.

The Internet layer corresponds to the OSI¡¯s Network layer, designa- ting the protocols relating to the logical transmission of packets over the entire network. It takes care of host addressing by giving each host an Internet Protocol (IP) address, and it handles the routing of packets among multiple networks. The Internet layer also controls the communication flow between two hosts.

At the bottom of the model, the Network Access layer monitors the data exchange between the host and the network. The equivalent of the Data Link and Physical layers of the OSI model, the Network Access layer oversees hardware addressing and defines protocols for the physical transmission of data.

While the DoD and OSI models are alike in design and concept, and have similar functions in similar places, *how* those functions occur are different. Figure 3.3 shows the TCP/IP protocol suite and how its protocols relate to the DoD model layers.

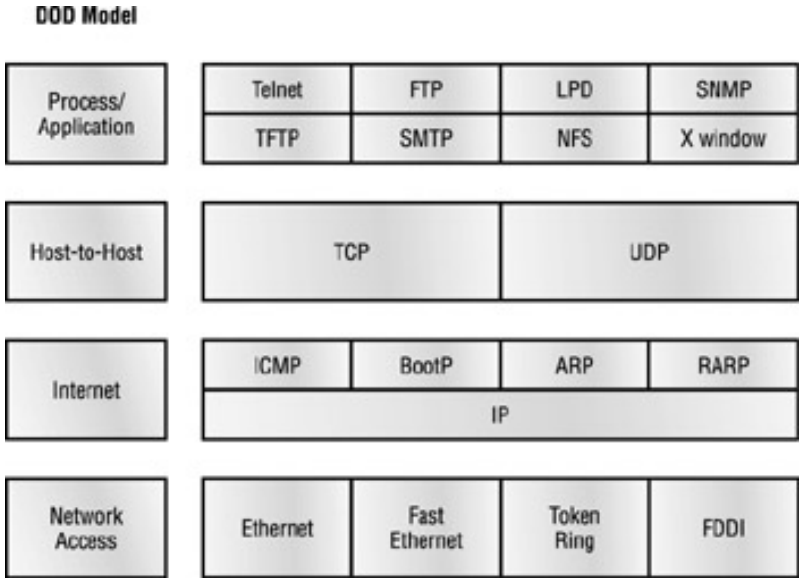

Figure 3.3: The TCP/IP protocol suite

Process/Application-Layer Protocols

This section covers the various protocols, applications, and services typically used in IP networks:

Telnet This protocol¡¯s specialty is terminal emulation. It allows a user on a remote client machine, called the Telnet client, to access the resources of another machine, the Telnet server**.**

File Transfer Protocol (FTP) The protocol that actually lets us transfer files. FTP is a connection-oriented service that uses TCP and can provide login and authentication.

Trivial File Transfer Protocol (TFTP) The stripped-down, stock version of FTP. It uses UDP at the Transport layer and is connectionless.

Network File System (NFS) Designed by Sun Microsystems to provide a filesystem that can be shared by disparate systems.

Simple Mail Transfer Protocol (SMTP) Answering our ubiquitous call to e-mail, SMTP uses a spooled, or queued, method of mail delivery.

Line Printer Daemon (LPD) Designed for printer sharing.

X Window Designed for client-server operations, X Window (or just X) defines a protocol for the writing of graphical user interface (GUI)¨Cbased client/server applications.

Simple Network Management Protocol (SNMP) The protocol that provides for the collection and manipulation of valuable network information. It gathers data by polling the devices on the network from a management station at fixed or random intervals, requiring them to disclose certain information.

Domain Name System (DNS) Used to resolve hostnames and specifically used to resolve Internet names. DNS is used to resolve fully qualified domain names (FQDNs)¡ªfor example, `http://www.thequestforcertification.com/` or `server1.thequestforcertification.com`. An FQDN is a hierarchy that can logically locate a system based on its domain identifier.

Bootstrap Protocol (BootP) When a diskless workstation is powered on, it broadcasts a BootP request on the network. A BootP server hears the request and looks up the client¡¯s MAC address in its

BootP file. If it finds an appropriate entry, it responds by telling the machine its IP address and the file from which it should boot.

Dynamic Host Configuration Protocol (DHCP) Used to give IP addresses and other network configuration dynamically to hosts.

Host-to-Host¨CLayer Protocols

The Host-to-Host layer¡¯s main purpose is to shield the upper-layer applications from the complexities of the network. The two protocols at this layer are Transmission Control Protocol (TCP) and User Datagram Protocol (UDP).

Transmission Control Protocol (TCP)

TCP takes large blocks of information from an application and breaks them into segments. It numbers and sequences each segment so that the destination¡¯s TCP can put the segments back into the order that the application intended. After these segments are sent, TCP (on the transmitting host) waits for an acknowledgment of the receiving end¡¯s TCP virtual circuit session, retransmitting those that aren¡¯t acknowledged.

Before a transmitting host starts to send segments down the model, the sender¡¯s TCP contacts the destination¡¯s TCP in order to establish a connection. What is created is known as a virtual circuit. This type of communication is called connection-oriented. During this initial handshake, the two TCP layers also agree on the amount of information that¡¯s going to be sent before the recipient¡¯s TCP sends back an acknowledgment. With everything agreed upon in advance, the path is paved for reliable communication to take place.

TCP is a full-duplex, connection-oriented, reliable, accurate protocol, and establishing all these terms and conditions, in addition to checking for errors, is no small task. TCP is very complicated and, not surprisingly, very costly in terms of network overhead.

User Datagram Protocol (UDP)

Application developers can use UDP in place of TCP. UDP is the scaled-down economy model and is considered a thin protocol.

It doesn¡¯t offer all the bells and whistles of TCP, but UDP does do a fabulous job of transporting information that doesn¡¯t require reliable delivery¡ªand does it using far fewer network resources.

Note UDP is covered thoroughly in RFC 768.

A circumstance calling for UDP instead of TCP is when the matter of reliability is already accomplished at the Process/Application layer. For example, NFS handles its own reliability issues, making the use of TCP both impractical and redundant. However, it¡¯s the application developer, not the user who wants to transfer data faster, who decides whether to use UDP or TCP.

UDP receives upper-layer blocks of information and breaks them into segments. Like TCP, each UDP segment is given a number for reassembly into the intended block at the destination. However, UDP does *not* sequence the segments, nor does it care in which order the segments arrive at the destination; it leaves sequencing and ordering the segments up to the application. At least UDP numbers them. But after that, it sends the segments off and forgets about them. It doesn¡¯t follow through, check up on them, or even allow for an acknowledgment of safe arrival¡ªcomplete abandonment. Because of this, it¡¯s referred to as an unreliable protocol. This does not mean that UDP is ineffective, only that it doesn¡¯t handle issues of reliability. A UDP header contains only the Source Port, Destination Port, Length, and Checksum fields.

Further, UDP doesn¡¯t create a virtual circuit, nor does it contact the destination before delivering information to it. Therefore, it is also considered a connectionless protocol. Since UDP assumes that the application will use its own reliability method, it doesn¡¯t use any. This gives an application developer a choice when running the Internet Protocol stack: TCP for reliability or UDP for faster transfers.

Internet-Layer Protocols

There are two main reasons for the Internet layer¡¯s existence. First, none of the protocols on layers above or below has any functions relating to routing; this complex and important task is the job of the Internet layer. The second reason for the Internet layer is to provide a single network interface to the upper-layer protocols. Without this layer, application programmers would need to write ¡°hooks¡± into every one of their applications for each different Network Access protocol. Not only would this be a pain in the neck, but it would lead to different versions of each application¡ªone for Ethernet, another one for

Token Ring, and so on. To prevent this, IP provides one single network interface for the upper-layer protocols. That accomplished, it¡¯s then the job of IP and the various Network Access protocols to get along and work together.

All network roads don¡¯t lead to Rome¡ªthey lead to IP. And all the other protocols at this layer, as well as all those at the upper layers, use it. Never forget that. *All* paths through the model go through IP. Following are the protocols that work at the Internet layer:

Internet Protocol (IP) Responsible for logical network addressing and routing through an internetwork.

Internet Control Message Protocol (ICMP) Used to provide a messaging service for IP.

Address Resolution Protocol (ARP) Used to resolve a known IP address to an Ethernet address.

Reverse Address Resolution Protocol (RARP) Used to resolve a known Ethernet address to an IP address.

Exam Essentials

Know the differences in how UDP sequences packets. You need to remember that UDP does not sequence packets and is connection-oriented.

Know how the DoD model matches to the OSI Reference Model. The DoD model contains four layers, which match up to the OSI Reference Model¡¯s seven layers.

Remember the specifications of each protocol. For example, you should know that TCP is a connection-oriented protocol, and UDP is a connectionless protocol.

Key Terms and Concepts

Address Resolution Protocol (ARP) Described at the Internet layer of the DoD model, ARP is used to find a hardware address, given the IP address.

Bootstrap Protocol (BootP) Described at the Internet layer of the DoD model, BootP is used to give diskless workstations an IP address.

IP address Network address assigned to a node on a network. Used to send and receive packets or datagrams on an internetwork.

Internet Protocol (IP) A connectionless protocol described at the Internet layer of the DoD model.

Reverse Address Resolution Protocol (RARP) Described at the Internet layer of the DoD model, RARP is used to find an IP address, given the hardware address.

Subnetting The breaking up of an IP network address into smaller networks.

Telnet Terminal emulation program used to create a virtual window to a remote device.

Transmission Control Protocol (TCP) A connection-oriented protocol specified at the Host-to-Host layer of the DoD model.

User Datagram Protocol (UDP) A connectionless protocol defined at the Host-to-Host layer of the DoD model.

Identify the functions performed by ICMP.

I*nternet Control Message Protocol (ICMP)* is one of the protocols used at the Internet layer of the DoD model. ICMP is important to Cisco because it is used for many different things, mainly to send updates to routers about problems with network routes or packets that are undeliverable in the internetwork.

Note When studying for the CCNA exam, be sure to remember what ICMP does when IP is configured with Cisco routers.

Critical Information

ICMP works at the Network layer of the OSI Reference Model. It is used by IP in many different services, such as network management and as a messaging service provider. RFC 1256 is an annex to ICMP, which affords hosts extended capability in discovering routes to gateways.

Periodically, router advertisements are announced over the network, reporting IP addresses for its network interfaces. Hosts listen for these ¡°network infomercials¡± to acquire route information. A router solicitation is a request for immediate advertisements and may be sent by a host when it starts up. The following are some common events and messages that ICMP relates to:

Destination Unreachable If a router can¡¯t send an IP datagram any farther, it uses ICMP to send a message back to the sender advising it of the situation. For example, if a router receives a packet destined for a network that the router doesn¡¯t know about, it will send an ICMP ¡°destination unreachable¡± message back to the sending station.

Buffer Full If a router¡¯s memory buffer for receiving incoming data- grams is full, it will use ICMP to send out a ¡°buffer full¡± message.

Hop Limits Each IP datagram is allotted a certain number of routers that it may go through, called a *hop*. If it reaches its limit of hops before arriving at its destination, the last router to receive that datagram deletes it. The executioner router then uses ICMP to send an obituary message, informing the sending machine of the demise of its datagram.

ping *ping (Packet Internet Groper)* uses ICMP echo messages to check the physical connectivity of machines on an internetwork.

The following data is from a network analyzer catching an ICMP echo request:

```
Flags:    0x00
 Status:    0x00
 Packet Length:78
 Timestamp:  14:04:25.967000 05/06/1998
Ethernet Header
 Destination: 00:a0:24:6e:0f:a8
 Source:    00:80:c7:a8:f0:3d
 Ether-Type:08-00 IP
IP Header - Internet Protocol Datagram
 Version:             4
 Header Length:       5
 Precedence:          0
 Type of Service:     %000
 Unused:              %00
 Total Length:        60
 Identifier:          56325
 Fragmentation Flags: %000
 Fragment Offset:     0
 Time To Live:        32
 IP Type:             0x01 ICMP
 Header Checksum:     0x2df0
 Source IP Address:   100.100.100.2
 Dest. IP Address:    100.100.100.1
 No Internet Datagram Options
ICMP - Internet Control Messages Protocol
 ICMP Type:           8 Echo Request
```

```
 Code:                0
 Checksum:            0x395c
 Identifier:          0x0300
 Sequence Number:     4352
 ICMP Data Area:
 abcdefghijklmnop  61 62 63 64 65 66 67 68 69 6a  ƒ6b 6c 6d
 qrstuvwabcdefghi  71 72 73 74 75 76 77 61 62 63  ƒ64 65 66
Frame Check Sequence: 0x00000000
```

Notice that even though ICMP works at the Network layer, it still uses IP to do the `ping` request. The Type field in the IP header is 0x01h, which specifies the ICMP protocol.

If you remember reading about the Data Link layer and the different frame types in Chapter 1, you should be able to look at the above trace and know what type of Ethernet frame this is. The only fields are Destination hardware address, Source hardware address, and Ethernet Type. The only frame that uses an Ethernet Type field is an Ethernet_II frame. (SNAP uses an Ethernet Type field but only within an 802.2 LLC field, which is not present in the frame.)

Exam Essentials

Remember what ICMP can do. ICMP sends ¡°destination unreachable¡± and ¡°buffer full¡± messages. It can find the number of hops to a destination host.

Remember which programs use ICMP. Packet Internet Groper (ping) uses ICMP echo messages to check the physical connectivity of machines on an internetwork. Traceroute (trace) uses ICMP and TTL (time to live) time-outs to find a packet¡¯s destination through an internetwork.

Key Terms and Concepts

Hop A unit of measurement used to describe the next device in a data path that data travels to. Each device a datagram passes through is considered a hop.

Internet Control Message Protocol (ICMP) Described at the Internet layer of the DoD model, ICMP is used for testing, verification, and notification services.

ping (Packet Internet Groper) Used to test IP connectivity between two IP hosts on an internetwork.

Configure IP addresses.

Let¡¯s take a step-by-step walk through configuring the IP address on a Cisco 2514 router. Doing so will aid you in understanding how to configure the IP address on a router.

Critical Information

First off, you need to connect to an unconfigured router through the router¡¯s console port using a console cable. The cables I have been receiving lately have been prefabricated, all-in-one cables. However, previous cables that you are tested for on this exam use a nine- or 25-pin serial adapter connected to a rollover cable. Many people believe that a crossover cable and a rollover cable are the same. They are not. A rollover cable has the exact opposite pin-out on the opposite side of the cable. This means that pin 8 matches to pin 1 on the opposite end, pin 7 to pin 2, and so on.

After connecting the cable, configuring a terminal emulator, and turning the power on, you are ready to configure the router. You will get a prompt asking you to do a global configuration. This is a configuration that configures only the router¡¯s basics; it is not tested on the Cisco exam. You can press Ctrl+C to exit this configuration.

If you are configuring the router for the first time, press Enter when the password prompt comes up. At the right-pointing carrot sign (>), type **enable** and press Enter.

The Privileged Mode Password prompt appears. Press Enter again. You will then see a pound sign (#). Type **config terminal** for the global configuration mode, and press Enter. Now you see the Global Configuration prompt. Type **interface e0** to select the first Ethernet interface configuration mode. At the interface prompt, follow these instructions:

1. Type **ip address 10.1.2.1 255.255.255.0** to set the IP address, and press Enter.
2. Type **no shutdown** to activate the interface, and press Enter.
3. Type **exit** to return to global configuration mode.
4. Type **exit** again to return to the privileged mode, and press Enter.

Follow these instructions to save the configuration:

1. Type **copy running-config starting-config** and press Enter.
2. Wait for the [OK] surrounded by brackets ([OK]).

To view the configuration, type **show running-config** to view the configuration. To exit the router, type **exit** twice.

Exam Essentials

Know the command to enter Ethernet interfaces from the global configuration mode. The command is the `interface` command**,** followed by the interface designation. For Ethernet interface 2, it would be `interface ethernet 2`. The first Ethernet port is always 0.

Know the command to configure an IP address from the Interface Configuration Mode prompt. To set the IP address, use the following command followed by the subnet (this example uses a Class C subnet):

```
ip address 207.12.81.254 255.255.255.0
```

Key Term and Concept

Interface This command allows you to enter an interface. Use the `interface` command followed by the interface¡¯s name and number.

Verify IP addresses.

This section looks at the tools provided to verify the configuration and connectivity on a Cisco IOS router. You¡¯ll examine a router¡¯s configuration and learn how to view the configuration, status, and statistics on a router¡¯s interface.

Critical Information

There are several tools that can be used to verify that IP addresses are configured correctly. As you learned in the earlier section on ICMP, both ping and trace can be used to verify connectivity on the network. One of the best things to do first is to look at the configuration and make sure that it has been entered correctly. To view the configuration on a Cisco IOS¨Cbased router, type **show running-config** at the Privileged Mode prompt. Let¡¯s take a look at the output from the `show running-config` command and view the configuration of a Cisco 1605 router already in production:

```
hostname Media Inc.
!
logging rate-limit console 10 except errors
no logging console
enable password MyPassword
!
ip subnet-zero
!
no ip dhcp-client network-discovery
!
!
!
interface Ethernet0
 ip address 166.15.108.110 255.255.255.248
 ip nat outside
 no ip route-cache
 no ip mroute-cache
no shut
!
interface Fa0
 ip address 10.1.1.2 255.255.0.0
 ip nat inside
 no ip route-cache
 no ip mroute-cache
no shut
!
router rip
 network 10.0.0.0
 network 166.15.108.0
!
ip nat inside source list 1 interface Ethernet0 ƒoverload
ip nat inside source static tcp 10.1.2.2 53 ƒ166.15.108.106 53 extendable
ip nat inside source static udp 10.1.2.2 53 ƒ166.15.108.106 53 extendable
ip nat inside source static 10.1.2.2 166.15.108.106
ip nat inside source static tcp 10.1.4.27 5631 ƒ166.15.108.110 5631 extendable
ip nat inside source static tcp 10.1.2.1 110 ƒ166.15.108.107 110 extendable
ip nat inside source static tcp 10.1.2.1 25 ƒ166.15.108.107 25 extendable
ip nat inside source static udp 10.1.2.2 50 ƒ166.15.108.106 50 extendable
ip nat inside source static udp 10.1.2.2 47 ƒ166.15.108.106 47 extendable
ip nat inside source static udp 10.1.2.2 6 ƒ166.15.108.106 6 extendable
ip nat inside source static udp 10.1.2.2 1723 ƒ166.15.108.106 1723 extendable
ip nat inside source static udp 10.1.2.2 1023 ƒ166.15.108.106 1023 extendable
ip nat inside source static tcp 10.1.2.2 50 ƒ166.15.108.106 50 extendable
ip nat inside source static tcp 10.1.2.2 47 ƒ166.15.108.106 47 extendable
ip nat inside source static tcp 10.1.2.2 6 ƒ166.15.108.106 6 extendable
ip nat inside source static tcp 10.1.2.2 1723 ƒ166.15.108.106 1723 extendable
ip nat inside source static tcp 10.1.2.2 1023 ƒ166.15.108.106 1023 extendable
ip nat inside source static 10.1.2.1 166.15.108.107
ip classless
ip route 0.0.0.0 0.0.0.0 166.15.108.105
ip route 10.1.2.2 255.255.255.255 Ethernet1
ip route 166.15.108.106 255.255.255.255 10.1.2.2
ip route 166.15.108.107 255.255.255.255 10.1.2.1
no ip http server
!
access-list 1 deny  10.1.2.2
access-list 1 permit 10.0.0.0 0.255.255.255
access-list 101 permit ip 10.3.0.0 0.0.255.255 any
access-list 101 permit ip 10.1.2.0 0.0.0.255 any
access-list 101 permit ip 10.2.2.0 0.0.0.255 any
access-list 101 permit ip 10.4.2.0 0.0.0.255 any
access-list 101 permit tcp any any eq telnet
access-list 101 permit tcp any any eq ftp
access-list 101 permit tcp any host 10.1.2.1 eq pop3
```

```
access-list 101 permit tcp any host 10.1.2.1 eq smtp
access-list 101 deny   tcp any any eq pop3
access-list 101 deny   tcp any any eq smtp
access-list 101 permit tcp any any eq domain
access-list 101 permit udp any any eq domain
access-list 101 permit udp any host 10.1.2.2 eq 1723
access-list 101 permit tcp any host 10.1.2.2 eq 1023
access-list 101 permit udp any host 10.1.2.2 eq 6
access-list 101 permit tcp any host 10.1.2.2 eq 6
access-list 101 permit udp any host 10.1.2.2 eq 47
access-list 101 permit tcp any host 10.1.2.2 eq 47
access-list 101 permit udp any host 10.1.2.2 eq 50
access-list 101 permit tcp any host 10.1.2.2 eq 50
access-list 101 permit ip host 10.1.4.200 any
access-list 101 permit ip host 10.1.4.201 any
access-list 101 permit ip host 10.1.4.202 any
access-list 101 permit ip host 10.1.4.203 any
access-list 101 permit ip host 10.1.4.204 any
access-list 101 permit ip host 10.1.4.205 any
access-list 101 permit ip host 10.1.4.206 any
access-list 101 permit ip host 10.1.4.207 any
access-list 101 permit ip host 10.1.4.208 any
access-list 101 permit ip host 10.1.4.209 any
access-list 101 permit ip host 10.1.4.210 any
access-list 101 permit ip host 10.1.4.211 any
access-list 101 permit ip host 10.1.4.212 any
access-list 101 deny  tcp 10.0.0.0 0.255.255.255 ƒany eq www
access-list 101 permit ip any any
!
!
!
line con 0
 exec-timeout 0 0
 password MyPassword
 login
line vty 0 4
 password MyPassword
 login
!
end
```

This is a very complex configuration, since the company uses Network Address Translation (NAT). They also control the IP addresses that can have access to the Internet.

Sometimes looking at the interface¡¯s configuration, statistics, and status to see if the interface is up and running correctly can help to verify connectivity as well. To do this, you need to look at the interface. Use the `show interface` command. Let¡¯s take a look at the output:

```
Media Inc.# show interface
Ethernet0 is up, line protocol is up
 Hardware is PQUICC Ethernet, address is 0007.eb32
ƒ.d6a3 (bia 0007.eb32.d6a3)
 Internet address is 207.212.78.110/29
 MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,
   reliability 255/255, txload 1/255, rxload 2/255
 Encapsulation ARPA, loopback not set
 Keepalive set (10 sec)
 Half-duplex, 10BaseT
 ARP type: ARPA, ARP Timeout 04:00:00
 Last input 00:00:00, output 00:00:00, output hang ƒnever
 Last clearing of "show interface" counters never
 Queueing strategy: fifo
 Output queue 0/40, 0 drops; input queue 4/75, 0 drops
 5 minute input rate 102000 bits/sec, 31 packets/sec
 5 minute output rate 31000 bits/sec, 30 packets/sec
   7841018 packets input, 4191596924 bytes,
ƒ0 no buffer
   Received 209 broadcasts, 0 runts, 0 giants,
ƒ0 throttles
   0 input errors, 0 CRC, 0 frame, 0 overrun,
 ƒ0 ignored
   0 input packets with dribble condition detected
   7375598 packets output, 1233071510 bytes,
ƒ0 underruns
   6309 output errors, 9998 collisions,
ƒ2 interface resets
   0 babbles, 0 late collision, 0 deferred
   0 lost carrier, 0 no carrier
   0 output buffer failures, 0 output buffers ƒswapped out
FastEthernet0 is up, line protocol is up
Hardware is PQUICC_FEC, address is 0007.eb32.d6a2 ƒ(bia 0007.eb32.d6a2)
 Internet address is 10.1.1.2/16
 MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
   reliability 255/255, txload 1/255, rxload 1/255
 Encapsulation ARPA, loopback not set
 Keepalive set (10 sec)
```

```
 Auto-duplex, 10Mb/s, 100BaseTX/FX
```

The `show ip interface brief` command is great for getting a quick look at the IP address and whether the interface is functioning. Let¡¯s take a look at the output from the command:

```
Media Inc.#show ip int brief
Interface IP-Address  OK? Method Status Protocol
Ethernet0  207.212.78.110 YES NVRAM  up  up

FastEthernet0  10.1.1.2   YES NVRAM up  up
```

Exam Essentials

Remember what IP tools are at your disposal to verify connectivity with another host. ICMP is your friend. You can use `ping` or `trace` commands from a router¡¯s Privileged Mode prompt to verify that you can contact another host on the network.

Know the command to view the configuration on the router. The `show running-config` command displays the running configuration of the router.

Know the command to view the interface status and configuration. Use the `show interface` command to view the router¡¯s interface configuration and status to make sure that they are up.

Key Terms and Concepts

show interface This command displays the configuration, status, and statistics on for an interface.

show running-config This command displays the configuration of the router in privileged mode.

List the required IPX address and encapsulation types.

At some point, most network administrators have encountered *Internetwork Packet Exchange (IPX)*. Novell NetWare, the most popular network operating system during the late 1980s and early 1990s, used IPX as its default protocol. As a result, millions of IPX networks have been installed. But Novell changed things with the release of NetWare 5. Now TCP/IP is the default communications protocol instead of IPX, although Novell still supports IPX. After all, considering the multitude of installed IPX clients and servers, it would be pretty impractical to yank the support for it.

Before you can understand IPX addressing and the encapsulation types, you must know your IPX routing protocols. This objective gives you the critical information you need to pass the exam, as well as to configure IPX on Cisco routers.

Critical Information

IPX doesn¡¯t map directly to the OSI model, but its protocols do function in layers. Back when they designed IPX, engineers were more concerned with performance than they were with strict compliance to existing standards or models. Even so, comparisons can be made.

Figure 3.4 illustrates the IPX protocols, layers, and functions relative to those of the OSI model.

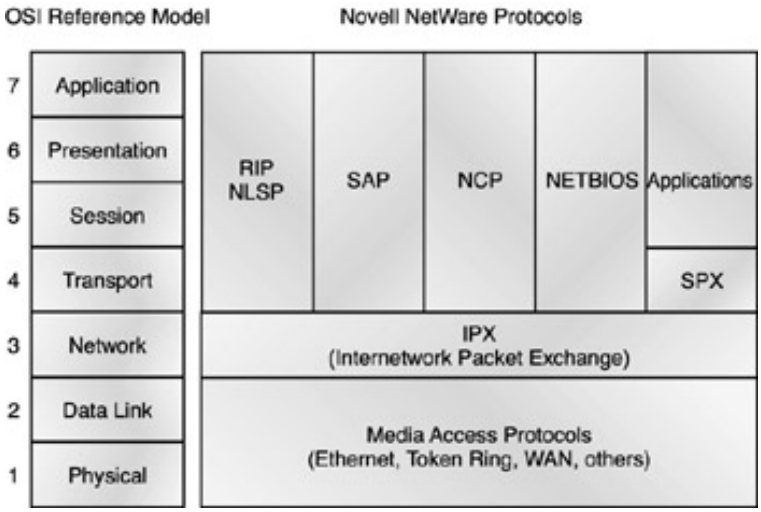

Figure 3.4: The IPX protocol stack and the OSI model

Here are some of the terms that you should be familiar with:

Internetwork Packet Exchange (IPX) Performs functions at layers 3 and 4 of the OSI model. It controls the assignment of IPX addresses (software addressing) on individual nodes, governs packet delivery across internetworks, and makes routing decisions based on information provided by the routing protocols, RIP or NLSP.

Service Advertising Protocol (SAP) Used to advertise and request services. Servers use it to advertise the services they offer, and clients use it to locate network services.

Routing Information Protocol (RIP) A distance-vector routing protocol used to discover IPX routes through internetworks. It employs ticks (1/18 of a second) and hop counts (number of routers between nodes) as metrics for determining preferred routes.

Sequenced Packet Exchange (SPX) Adds connection-oriented communications to the otherwise connectionless IPX.

NetWare Link Services Protocol (NLSP) An advanced link-state routing protocol developed by Novell, intended to replace both RIP and SAP.

Cisco with IPX

As you would think, NetWare clients are dependent on servers to locate all network resources. Every

NetWare server builds a SAP table containing all the network resources that it¡¯s aware of. When a client requires access to a certain resource, it issues an IPX broadcast called a Get Nearest Server (GNS) request to locate a NetWare server that provides that resource. In turn, the servers receiving the GNS request check their SAP tables to locate a NetWare server that matches the specific request; they respond to the client with a GNS reply.

If there are no local NetWare servers, however, the local Cisco router that connects the client¡¯s segment to the IPX internetwork can respond to the client¡¯s GNS request. This saves the client from having to wait for remote NetWare servers to respond. A second advantage of this arrangement is that precious WAN bandwidth isn¡¯t occupied with GNS conversations between clients on a segment with no local NetWare server and remote NetWare servers, as shown in Figure 3.5.

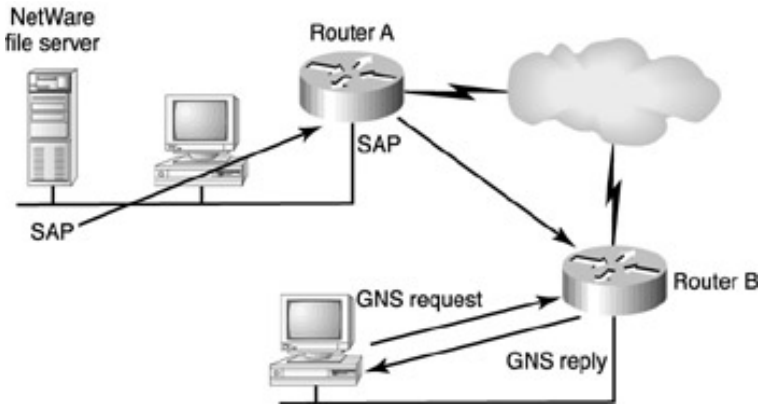

Figure 3.5: Remote IPX clients on a serverless network

In this figure, you can see client workstations at the remote office site requiring access to server resources at the main office. In this situation, router A would answer client GNS requests from its SAP table rather than forwarding the request across the WAN to the main office servers. The clients never realize or care that there isn¡¯t a NetWare server present on their LAN.

Service Advertising Protocol (SAP)

NetWare servers use *Service Advertising Protocol (SAP)* to advertise the services they offer by sending out a SAP broadcast every 60 seconds. The broadcast includes all services that the server has learned about from other servers¡ªnot just the ones they furnish. All servers receiving the SAP broadcast incorporate the information into their own SAP tables; they then rebroadcast it in their own SAP updates. Because SAP information is shared among all servers, all servers eventually become aware of all available services, and are thereby equipped to respond to client GNS requests. As new services are introduced, they¡¯re added to SAP tables on local servers and are rebroadcast until every server knows they exist and where to get them.

So how does a Cisco router fit in here? Well, as far as SAP is concerned, that router acts just like another NetWare server. By default, a SAP broadcast won¡¯t cross a Cisco router. A Cisco router catalogs all SAPs heard on any of its IPX-enabled interfaces into its SAP table; it then broadcasts the whole table from each of those interfaces at 60-second intervals, unless you change the settings¡ªjust as NetWare servers do. This is an important point, especially with WAN links. The router isolates SAP broadcasts to individual segments and passes along only the summarized information to each segment.

Routing Information Protocol (RIP)

Routing Information Protocol (RIP) information is exchanged between servers much the same way that SAP information is. Servers build routing tables that contain entries for the networks they¡¯re directly connected to, then broadcast this information to all IPX- enabled interfaces. Other servers on those segments receive those updates and broadcast their RIP tables on their IPX interfaces. Just as SAP information travels from server to server until all servers are enlightened, RIP information is proliferated until all servers and routers know of the internetwork¡¯s routes. Like SAP information, RIP information is broadcast at 60-second intervals.

IPX Addressing

IPX addresses use 80 bits, or 10 bytes, of data. As with TCP/IP addresses, they are hierarchical, and are divided into network and node portions. The first four bytes always represent the network address, and the last six bytes always represent the node address. There¡¯s none of that Class A, Class B, or Class C TCP/IP stuff in IPX addressing¡ªthe network and node portions of the address are always the same length. After subnet masking, this is sweet indeed!

IPX addresses can be written in several formats. Most often, though, they¡¯re written in hex, such as

00007C80.0000.8609.33E9. The first eight hex digits (00007C80) represent the network portion of the address. When referring to the IPX network, it¡¯s a common IPX custom to drop leading zeros. Thus, the above network address would be referred to as IPX network 7C80.

The remaining 12 hex digits (0000.8609.33E9) represent the node portion and are commonly divided into three sections of four hex digits each divided by periods. These are the MAC address of the workstation.

Encapsulation

Encapsulation, or framing, is the process of taking packets from upper-layer protocols and building frames to transmit across the network. As you probably recall, frames live at layer 2 of the OSI model. When you¡¯re dealing with IPX, encapsulation is the specific process of taking IPX datagrams (layer 3) and building frames (layer 2) for one of the supported media.

Why is this significant? Well, for the very good reason that NetWare supports multiple, incompatible framing methods, and it does so on the same media. For instance, take Ethernet. NetWare has four different frame types to choose from, depending on your needs (see Table 3.4), and each of those frame types is incompatible with the others.

Table 3.4: Novell Ethernet Encapsulations

NetWare Frame Type	Features
Ethernet_802.3	Default up to NetWare 3.11
Ethernet_802.2	Default since NetWare 3.12
Ethernet_II	Supports both TCP/IP and IPX
Ethernet_snap	AppleTalk, IPX, and TCP/IP

Sometimes¡ªand only sometimes¡ªyou can intentionally have multiple frame types present on the same network. Typically, you¡¯ll start working in an environment that already has all frame types configured¡ªusually because the administrator didn¡¯t know what to do and just configured all available frame types on all routers and servers, as shown in Figure 3.6.

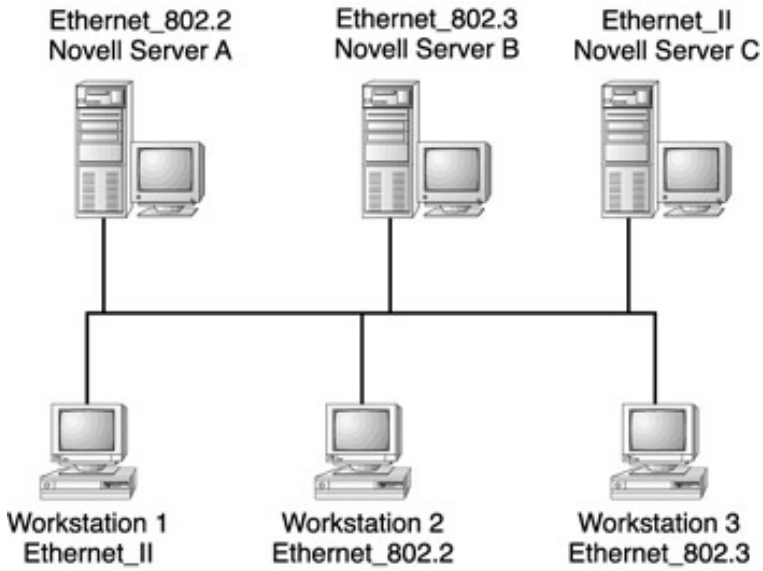

Figure 3.6: Multiple frame types on a single Ethernet segment

Each frame type in Figure 3.6 has a unique IPX network address. Even though there¡¯s a single Ethernet segment, there are three virtual IPX networks and, therefore, three unique IPX network addresses. Each network will be broadcast across the internetwork every 60 seconds.

When configuring a router, you¡¯ll need to know both the frame type and the IPX network address information for each segment that you plan to attach that router to. To find this information, ask the network administrator, or go to one of the NetWare servers and type **config** at the server console.

Necessary Procedures

To configure IPX routing, use the `ipx routing` global configuration command. Here is an example:

```
RouterA#config t
RouterA(config)#ipx routing
```

Once you enable IPX routing on the router, RIP and SAP are automatically enabled as well. However, nothing happens until you configure the individual interfaces with IPX addresses.

Enabling IPX on Individual Interfaces

Once you have IPX routing enabled on the router, the next step is to enable IPX on individual interfaces. To enable IPX on an interface, first enter the interface configuration mode, and then issue the following command:

`ipx network` *`number`* `[encapsulation` *`encapsulation-type`*`] ƒ[secondary]`

The various parts are defined as follows:

number The IPX network address.

[encapsulation *encapsulation-type*] Optional. Table 3.5 lists the default encapsulation type on various media (shown in the Cisco Keyword column).

[secondary] Indicates a secondary encapsulation (frame type) and network address on the same interface.

Here is an example of configuring IPX on a 2501 router named 2501A:

```
2501A#config t
2501A(config)#ipx routing
2501A(config)#int e0
2501A(config-if)#ipx network 10
```

That¡¯s all there is to it. Just add the network number, and the rest is done for you. IPX is a very resilient routed protocol because it broadcasts for everything. However, this is also why it causes problems in larger internetworks.

What frame type is now running on Ethernet 0 on 2501A? By default, the frame type is Novell-Ether (802.3). To change the frame type, or to add another frame type, add the `encapsulation` command to the interface configuration. Table 3.5 lists the different frame types available with IPX.

Table 3.5: Novell IPX Frame Types

Interface Type	Novell Frame Type	Cisco Keyword
Ethernet	Ethernet_802.3	`novell-ether` (default)
	Ethernet_802.2	`sap`
	Ethernet_II	`arpa`
	Ethernet_snap	`snap`
Token Ring	Token-Ring	`sap` (default)
	Token-Ring_snap	`snap`
FDDI	Fddi_snap	`snap` (default)
	Fddi_802.2	`sap`
	Fddi_raw	`novell-fddi`

To change the IPX frame type on Ethernet 0 of 2501A to SAP (802.2), use the `encapsulation` command, as shown below:

```
2501A#config t
2501A(config)#int e0
2501A(config-if)#ipx network 10 encapsulation sap
```

This replaces the existing network number and encapsulation with the 802.2 frame type. If you want to add multiple frame types, you need either to use the `secondary` command at the end of the network command line, or to create subinterfaces. Both the `secondary` command and subinterfaces are discussed later in this chapter.

To configure a Cisco router into an existing IPX internetwork, you¡¯ll need the IPX network address and

frame type information from the ¡°config¡± screen of your NetWare servers for this step. When specifying the encapsulation type on the router, make sure to use the Cisco keyword, *not* the Novell frame type.

Verifying the IPX Routing Tables

To view the IPX routing tables, use the command `show ipx route`. Like IP, IPX routers know about directly connected networks only by default. However, when you turned on IPX routing in the configuration examples above, IPX RIP was automatically started on all routers.

IPX RIP will find all IPX networks in the internetwork and update all routers¡¯ routing tables. Let¡¯s take a look at a router running IPX in an internetwork and see the IPX routing table:

```
2621A#sh ipx route
Codes: C - Connected primary network, c - Connected ƒsecondary network
[output cut]
5 Total IPX routes. Up to 1 parallel paths and 16 hops ƒallowed.
No default route known.
C 10 (NOVELL-ETHER), Fa0/0
R 20 [07/01] via   10.0000.0c8d.3a7b,  16s, Fa0/0
R 30 [07/02] via   10.0000.0c8d.3a7c,  17s, Fa0/0
R 40 [07/02] via   10.0000.0c8d.3a7c,  17s, Fa0/0
R 50 [13/03] via   10.0000.0c8d.3a7c,  17s, Fa0/0
2621A#
```

The `C` means a directly connected IPX network, and the `R`s are IPX RIP found networks. The `[07/01]` is the ticks and hops to the remote network.

Adding a Secondary Network

To configure a secondary address on an Ethernet LAN to support multiple frame types, use the `ipx network` command with the `secondary` parameter at the end of the command.

Here is an example of adding a secondary network to 2501A¡¯s Ethernet connection:

```
2501A#config t
Enter configuration commands, one per line. End with ƒCNTL/Z.
2501A(config)#int e0
2501A(config-if)#ipx network 10a encap sap sec
```

If you don¡¯t use the `secondary` command at the end of the line, the `ipx network` command will replace the existing entry. (The shortcut commands `encap` and `sec` were used here instead of the whole commands `encapsulation` and `secondary`.)

The important thing to understand is that each frame type must have a different IPX network number. Notice the `10a` in the above example. The 802.3 frame type is using 10, so you cannot configure the 802.2 frame type with that number.

Supporting Multiple Networks with Subinterfaces

To define IPX network numbers to router interfaces that support multiple networks, you can use a subinterface instead of the `secondary` command. This allows one physical interface to support multiple logical IPX networks. Each subinterface, like a secondary, must have a unique IPX network number and a unique encapsulation type.

To define subinterfaces, use the `interface ethernet` *`port.number`* command. You can use numbers between e0.0 and e0.4292967295¡ª that¡¯s a lot of subinterfaces! An example of adding the 802.2 frame type is shown here:

```
2621A(config)#int e0.10
2621A(config-subif)#ipx network 10a encap sap
2621A(config-subif)#^Z
2621A#
```

Monitoring IPX on Cisco Routers

Once you have IPX configured and running, there are several ways to verify and track that your router is communicating correctly. The following commands are important to understand:

show ipx servers This command is a lot like the `display servers` command in NetWare¡ªit displays the contents of the SAP table in the Cisco router, so you should see the names of all SAP services here.

show ipx route This command displays the IPX routing table entries that the router knows about. The router reports networks to which it is directly connected, then reports networks that it has learned of since the router has come online.

show ipx traffic This command shows the RIP and SAP traffic sent and received on all interfaces of the router.

show ipx interface This command shows the RIP and SAP information sent and received on each individual interface. Also, it shows the IPX network number and encapsulation for each interface.

show protocol This command shows the routed protocol addresses for each interface.

debug ipx This command provides diagnostics for IPX routing.

IPX ping This command allows you to ping IPX router interfaces for diagnostic.

Load Balancing with IPX

If you were to set up parallel IPX paths between routers, the Cisco IOS would not learn about these paths by default. The router will learn a single path to a destination and discard information about alternative, parallel, equal-cost paths. To be able to perform a round- robin load balance over multiple equal-cost paths, you need to add the command `ipx maximum-paths [#]` (with # being any number up to 64); this will allow the router to accept the possibility that there might be more than one path to the same destination.

The Cisco IOS will perform per-packet load sharing by default over these parallel lines. Packets will be sent on a round-robin basis between all equal-cost lines, regardless of the destination. However, if you want to ensure that all packets sent to a destination or host will always go over the same line, use the `IPX per-host-load-share` command.

The `ipx maximum-paths` command is shown below. It tells the IPX RIP protocol to perform a round-robin load balance across two equal-cost paths.

```
Router#config t
Router(config)#ipx maximum-paths 2
Router(config)#^Z
Router#sh ipx route
Codes: C - Connected primary network,  c - Connected ƒ[output cut]
5 Total IPX routes. Up to 2 parallel paths and 16 hops ƒallowed.
[output cut]
```

The `show ipx route` command shows that two parallel paths are now supported.

Exam Essentials

Remember the IPX address format. The syntax for an IPX address is *net.node.node.node*. There are no class distinctions and no other syntax types for IPX addresses.

Remember the output each command gives you. When practicing the commands on your Cisco router, pay close attention to the output each command displays.

Remember the IPX encapsulation methods used on an Ethernet LAN. Studying and practicing on a Cisco router will help you remember the different keywords.

Key Terms and Concepts

debug A command used to display real-time network updates on a console.

extended ping Program that allows you to specify arguments in the `ping` command. This is useful when you want to ping other protocols besides IP.

Internet Protocol (IP) A protocol specified at the Internet layer of the Department of Defense (DoD) model. Used to route packets through an internetwork and for network addressing.

Internetwork Packet Exchange (IPX) A protocol stack developed by Xerox (which they called XNS). Novell copied the protocol and called it IPX. It is used for routing packets through an internetwork and for network addressing.

Routing Information Protocol (RIP) A distance-vector routing protocol that is used to update routing

tables dynamically.

Service Advertising Protocol (SAP) A Novell protocol defined at the Application layer of the OSI model and used to advertise network services on an internetwork.

Chapter 4: Routing

Cisco Certified Network Associate Exam Objectives Covered in This Chapter:

- Define flow control and describe the three basic methods used in networking.*(pages 114¡ª119)*
- Add the RIP routing protocol to your configuration.*(pages 119¡ª131)*
- Add the IGRP routing protocol to your configuration.*(pages 131¡ª134)*

This chapter focuses on routing, specifically IP routing. Interior gateway protocols are used to share information within an autonomous system (AS). This chapter concentrates on distance- vector interior routing protocols.

This is an important chapter to understand both for the exam and when working in a production environment.

Define flow control and describe the three basic methods used in networking.

For the exam, you need to know what flow control is and why we need it. You also need to know the three flow-control methods, particularly windowing, which is used in TCP. Windowing is a very efficient method of providing a stable environment for a TCP virtual circuit.

Critical Information

During a transfer, congestion can occur because a high-speed computer is generating data traffic faster than the network can transfer it, or because many computers are simultaneously sending datagrams through a single gateway or destination. In the latter case, a gateway or destination can become congested even though no single source caused the problem.

When a machine receives a flood of datagrams too quickly for it to process, it stores them in a section in memory called a buffer. This buffering action solves the problem only if the datagrams are part of a small burst. However, if the datagram deluge continues, eventually a device¡¯s memory will be exhausted, its flood capacity will be exceeded, and it will discard any additional datagrams that arrive.

But, no worries¡ªbecause of the transport function, network *flow control* systems work quite well. Instead of dumping resources and allowing data to be lost, the transport can issue a ¡°not ready¡± indicator (see Figure 4.1) to the sender, or source, of the flood. This mechanism works kind of like a stop light, signaling the sending device to stop transmitting segment traffic to its overwhelmed peer. When the peer receiver has processed the segments already in its memory reservoir, it sends out a ¡°ready¡± transport indicator. When the machine waiting to transmit the rest of its datagrams receives this ¡°go¡± indictor, it can then resume its transmission.

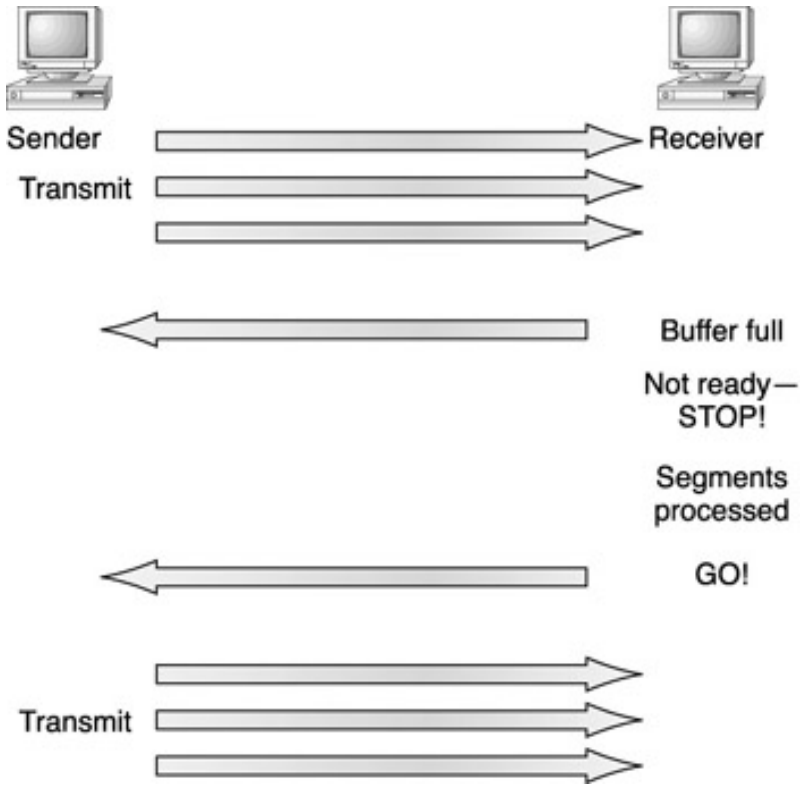

Figure 4.1: Transmitting segments with flow control

In fundamental, reliable, connection-oriented data transfer, datagrams are delivered to the receiving host in exactly the same sequence they¡¯re transmitted; the transmission fails if this order is breached. If any data segments are lost, duplicated, or damaged along the way, this will cause a failure to transmit. The answer to the problem is to have the receiving host acknowledge receiving each and every data segment.

Data integrity is ensured at this layer by maintaining flow control and by allowing users the option of requesting reliable data transport between systems. Flow control prevents the problem of a sending host on one side of the connection overflowing the buffers in the receiving host¡ªan event that can result in lost data. Reliable data transport employs a connection-oriented communication session between systems, and the protocols involved ensure that the following will be achieved:

- The segments delivered are acknowledged back to the sender upon their reception.
- Any segments not acknowledged are retransmitted.
- Segments are sequenced back into their proper order upon arrival at their destination.

A manageable data flow is maintained in order to avoid congestion, overloading, and the loss of any data.

Windowing

Data throughput would be low if the transmitting machine had to wait for an acknowledgment after sending each segment. Since there¡¯s time available after the sender transmits the data segment and before it finishes processing acknowledgments from the receiving machine, the sender uses the break to transmit more data. The quantity of data segments the transmitting machine is allowed to send without receiving an acknowledgment for them is called a window.

Windowing controls how much information is transferred from one end to the other. While some protocols quantify information by observing the number of packets, TCP/IP measures it by counting the number of bytes. Figure 4.2 illustrates a window size of 1 and a window size of 3. When a window size of 1 is configured, the sending machine waits for an acknowledgment for each data segment it transmits before transmitting another. Configured to a window size of 3, it¡¯s allowed to transmit three data segments before an acknowledgment is received. In our simplified example, both the sending and receiving machines are workstations. Reality is rarely that simple, and most often, acknowledgments and packets will commingle as they travel over the network and pass through routers. Routing complicates things, but not to worry, you¡¯ll learn about applied routing later in the book.

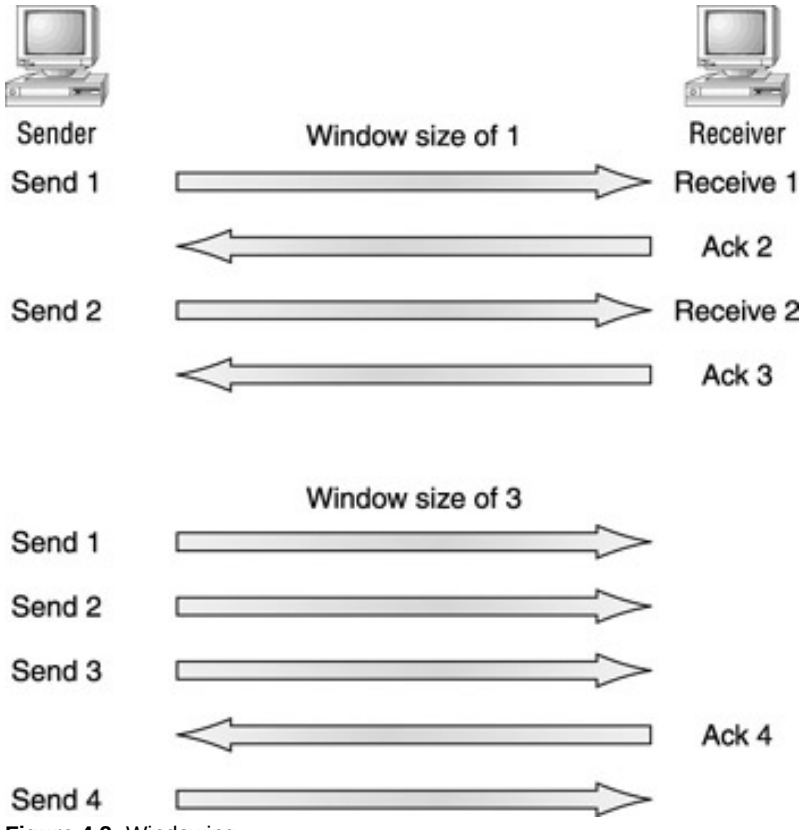

Figure 4.2: Windowing

Buffering

Buffering is used by network devices to temporarily store excess data the device has received and cannot successfully process in real time. If the sudden receipt of data is minimal, the data can be easily stored by buffering the data. However, another method must be used if the sudden receipt of data is enough to exhaust the available buffering space. In this situation, if only buffering is used, excess data that cannot be stored is discarded.

Source-Quench Messages

A receiving device uses *source-quench messages* to keep the device¡¯s buffer space from being exhausted. When a receiving device sends a source-quench message to another device, it is telling the sending device to slow its current rate of data transmission. Once a receiving device begins discarding data because of overflowing buffers, the receiving device begins to send source-quench messages to tell the sending device to slow down at the rate of one message for each packet dropped. When the sending device receives the source-quench messages, it reduces its transmission speed until it no longer receives the source-quench messages. The sending device will gradually return to its sending rate as long as no source-quench requests are received.

Exam Essentials

Understand that TCP uses windowing. TCP uses windowing as a flow control method.

Know the three methods of flow control. These methods are windowing, buffering, and source-quench messages.

Key Terms and Concepts

buffering The ability for a receiving device to store data it receives that it cannot process in real time.

flow control Method implemented on networks to stop a receiving host¡¯s buffers from overflowing and dropping data.

source-quench messages Messages sent by a receiving device to inform another device that it has discarded data due to its buffers being full.

Windowing Flow-control method implemented by TCP where a sending device waits for acknowledgments and a set window size.

Add the RIP routing protocol to your configuration.

Before jumping right into configuring Routing Information Protocol (RIP), you need to take a look at routing and make sure that you have a clear understanding of the differences between static and dynamic routing. You should also understand default routes and administrative distances. This section familiarizes you with all of these topics.

Critical Information

Routing is taking a packet from one device and sending it through the network to another device on a different network. If your network has no routers, then you are not routing. Routers are used to direct and transmit traffic to all the networks in your internetwork. To be able to route packets, a router must have, at a minimum, knowledge of the following:

- Destination address
- Neighbor routers from which it can learn about remote networks
- Possible routes to all remote networks
- The best route to each remote network
- How to maintain and verify routing information

The router learns about remote networks from neighbor routers or from an administrator. The router then builds a routing table that describes how to find the remote networks. If the network is directly connected, then the router already knows how to get to the network. If the networks are not attached, the router must learn how to get to the remote network with either static routing, which means that the administrator must hand-type all network locations into the routing table, or dynamic routing. Dynamic routing is the process of routing protocols running on the router communicating with neighbor routers. The routers then update each other about all the networks they know about. If a change occurs in a network, the dynamic routing protocols automati- cally inform all routers about the change. If static routing is used, the administrator is responsible for updating all changes manually into all routers.

Routers can send packets to remote networks only by looking at the routing table and finding out how to get to them. But our configured routers have information only containing directly connected networks in each routing table. What happens when a router receives a packet with a network that is not listed in the routing table? It discards it! It doesn¡¯t send a broadcast looking for the remote network¡ª the router just discards the packet. Period.

There are a few different ways to configure the routing tables to include all the networks in our little internetwork so that packets will be forwarded. However, the best way for one network is not necessarily the best way for another. If you understand the different routing types, you will be able to decide what fits best in your business environment.

The different types of routing covered in this objective include:

- Static routing
- Default routing
- Dynamic routing

Static Routing

Static routing is the process of an administrator adding routes by hand in the routing table of each router.

The command used to add a static route to a routing table is:

```
ip route [destination_network] [mask] [next_hop_ f
address or exitinterface] [administrative_ fdistance] [permanent]
```

The following list describes each command in the string:

ip route Command used to create the static route.

destination_network Network you are placing in the routing table.

mask Subnet mask being used on the network.

next_hop_address Address of the next hop router that will receive the packet and forward it to the remote network. This is a router interface that is on a directly connected network. You must be able to ping the router interface before you add the route.

exitinterface Used in place of the next-hop address, if desired. Must be on a point-to-point link, such as a WAN. This command does not work on a LAN such as Ethernet.

administrative_distance By default, static routes have an administrative distance of 1. You can change the default value by adding an administrative weight at the end of the command.

permanent If the interface is shut down or the router cannot communicate to the next-hop router, the route is automatically discarded from the routing table. Choosing the `permanent` option keeps the entry in the routing table no matter what happens.

Default Routing

Default routing, also known as the ¡°gateway of last resort,¡± is used to send packets with a remote destination network not in the routing table to a next hop router. You can use default routing only on stub networks, which have only one exit port out of the network.

To configure a default route, you use wildcards in the network address and mask locations of a static route. Think of a default route as a static route that uses wildcards instead of network and mask information.

The command used to add a default route to a routing table is:

```
ip route 0.0.0.0 0.0.0.0 [next_hop_interface]
```

This command tells the router that any address it doesn¡¯t know about, because of a static route or a directly connected network, goes to the next hop router, which should be directly connected.

Note The next hop address is the *`next_hop_interface`* connected to the next hop router. This interface must be in the same network as the network configured on the outgoing interface.

Dynamic Routing

Dynamic routing is the process of using protocols to find and update routing tables on routers. This is easier than static or default routing, but you use it at the expense of router CPU processes and bandwidth usage on the network links. A routing protocol defines the set of rules used by a router when it communicates between neighbor routers. There are three classes of dynamic routing protocols:

Distance-Vector The distance-vector routing protocols use a distance to a remote network to find the best path. Each time a packet goes through a router, it¡¯s called a hop. The route with the least number of hops to the network is determined to be the best route. The vector is the determination of direction to the remote network. RIP and IGRP are examples of distance-vector routing protocols.

Link-State Typically called shortest path first, each router creates three separate tables. One of these tables keeps track of directly attached neighbors, one determines the topology of the entire internetwork, and one is used for the routing table. Link-state routers know more about the internetwork than any distance-vector routing protocol. An example of an IP routing protocol that is completely link-state is OSPF.

Hybrid Uses aspects of distance-vector and link-state; for example, EIGRP.

There is no set way of configuring routing protocols for use with every business. This is a task that is performed on a case-by-case basis. However, if you understand how the different routing protocols work, you can make good business decisions.

Distance-Vector Routing Protocols

The distance-vector routing algorithm passes complete routing tables to neighbor routers. The neighbor

routers then combine the received routing table with their own routing tables to complete the internetwork map. This is called routing by rumor, as a router receiving an update from a neighbor router believes the information about remote networks without actually finding out for itself.

It is possible to have a network that has multiple links to the same remote network. If that is the case, the administrative distance is checked first. If the administrative distance is the same, a router will have to use other metrics to determine the best path to use to that remote network.

RIP uses only hop count to determine the best path to an internetwork. If RIP finds more than one link to the same remote network with the same hop count, it will automatically perform a round-robin load balance. RIP can perform load balancing for up to six equal-cost links.

Routing Loops

Distance-vector routing protocols keep track of any changes to the internetwork by broadcasting periodic routing updates to all active interfaces. This broadcast includes the complete routing table. This works fine, although it takes up CPU processes and link bandwidth. However, if a network outage happens, problems can occur. The slow convergence of distance-vector routing protocols can cause inconsistent routing tables and routing loops. The following are used in distance-vector routing protocols to reduce loop problems:

Split Horizon A *split horizon* reduces incorrect routing information and routing overhead in a distance-vector network by enforcing the rule that information cannot be sent back in the direction from which it was received.

Route Poisoning with Poison Reverse Sets a downed link to infinity. By poisoning a downed route, neighbor routers are not susceptible to incorrect updates about the downed route. When the neighbor routers received a *route poison*, they send an update, called a *poison reverse*, back to the router with the downed link. This ensures that all routes on the segment have received the poisoned route information.

Hold-Downs Used to prevent regular update messages from reinstating a route that has gone down. *Hold-downs* help prevent routes from changing too rapidly by allowing time for either the downed route to come back or the network to stabilize somewhat before changing to the next best route. These also tell routers to restrict, for a specific time period, any changes that might affect recently removed routes. This prevents inoperative routers from being prematurely restored to other routers¡¯ tables.

Triggered Updates Hold-downs use triggered updates, which reset the hold-down timer, to let the neighbor routers know of a change in the network. Unlike update messages from neighbor routers, triggered updates create a new routing table that is sent immediately to neighbor routers because a change was detected in the internetwork. There are three instances when triggered updates will reset the hold- down timer:

- The hold-down timer expires.
    - The router receives a processing task proportional to the number of links in the internetwork.
    - Another update is received indicating the network topology has changed.

Routing Information Protocol (RIP)

Routing Information Protocol (RIP) for IP is a true distance-vector routing protocol. It sends the complete routing table out to all active interfaces every 30 seconds. RIP uses only hop count to determine the best way to a remote network, but it has a maximum allowable hop count of 15, meaning that 16 is deemed unreachable. RIP works well in small networks, but it is inefficient on large networks with slow WAN links or on networks with a large number of routers installed.

RIP version 1 uses only classful routing, which means that all devices in the network must use the same subnet mask. This is because RIP version 1 does not send updates with subnet-mask information in tow. RIP version 2 provides what is called prefix routing and *does* send subnet-mask information with the route updates; this is called classless routing.

Administrative Distances

When configuring routing protocols, you need to be aware of *administrative distances*. These are used to rate the trustworthiness of routing information received on a router from a neighbor router. An administrative distance is an integer from 0 to 255, where 0 is the most trusted, and 255 means no traffic will be passed via this route.

Table 4.1 shows the default administrative distances that a Cisco router will use to decide which route to

use to a remote network. EIGRP (Enhanced Interior Gateway Routing Protocol) and OSPF (Open Shortest Path First) are additional protocols not covered by this objective but that you might encounter in advanced routing problems.

Table 4.1: Default Administrative Distances

Route Source	Default Distance
Connected interface	0
Static route	1
EIGRP	90
IGRP	100
OSPF	110
RIP	120
External EIGRP	170
Unknown	255 (this route will never be used)

If a network is directly connected, the router will always use the interface connected to the network and configured to be an interface on the network; the router will always believe its own configuration before that of a static route. If an administrator configures a static route on the router, it will believe that route over any other learned routes obtained from a routing protocol. This means that there can be multiple ways of obtaining a route to a destination network, but the administrative distance decides the route to use. You can change the administrative distance of static routes, which is 1 by default.

Verifying Your Configurations

It is very important to be able to verify your configurations once you have completed them, or at least, once you *think* you have completed them. The following list includes the commands you can use to verify the routed and routing protocols configured on your Cisco routers:

show ip route Shows the routes the router knows about.

show protocols Shows the routed protocol information configured on the router.

show ip protocol Shows the routing protocol information configured on the router.

debug ip rip Shows the console session, routing updates as they are sent and received on the router.

debug ip igrp events Summarizes the IGRP routing information that is running on the network.

debug ip igrp transactions Shows message requests from neighboring routers asking for an update and the broadcasts sent from your router toward those neighbors.

Necessary Procedures

This section shows you how to configure the routing table using:

- Static routing
- Default routing
- RIP routing

Configuring Static Routing

The router output below shows the configuration of static routes on a Cisco router. The command is:

```
ip route remote_network mask next_hop
```

Here are some examples:

```
2621A(Config)#ip route 172.16.20.0 255.255.255.0
 172.16.10.2
2621A(Config)#ip route 172.16.30.0 255.255.255.0
```

```
 172.16.10.2
2621A(Config)#ip route 172.16.40.0 255.255.255.0
 172.16.10.2
2621A(Config)#ip route 172.16.50.0 255.255.255.0
 172.16.10.2
```

After the router is configured, you can type **show running-config** and **show ip route** to see the static routes. Here is an example:

```
2621A#sh ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, ƒM¡ª[output cut]
Gateway of last resort is not set

   172.16.0.0/24 is subnetted, 5 subnets
S    172.16.50.0 [1/0] via 172.16.10.2
S    172.16.40.0 [1/0] via 172.16.10.2
S    172.16.30.0 [1/0] via 172.16.10.2
S    172.16.20.0 [1/0] via 172.16.10.2
C    172.16.10.0 is directly connected, ƒFastEthernet0/0
2621A#
```

The S is for static routes, the C is for directly connected routes.

Note Remember that if the routes don¡¯t show up in the routing table, it is because the router cannot communicate to the next-hop address you configured. You can use the `permanent` parameter to keep the route in the routing table even if the next hop device cannot be contacted.

Configuring Default Routing

To configure a default route on a router, use the following command:

```
ip route 0.0.0.0 0.0.0.0 next_hop
```

Here is an example:

```
2501C(Config)#ip route 0.0.0.0 0.0.0.0 172.16.40.1
```

If you configure only the default route, you¡¯ll see only the directly connected networks, plus an S*, which indicates that this entry is the candidate for a default route:

```
2501C#sh ip route
Codes: C - connected, S - static, I - IGRP, R - ƒRIP, M ¨C
[output cut]
 - IS-IS level-1, L2 - IS-IS level-2, * - candidate
ƒdefault U - per-user static route, o¡ªODR

Gateway of last resort is 172.16.40.1 to network ƒ0.0.0.0
   172.16.0.0/24 is subnetted, 5 subnets
C    172.16.50.0 is directly connected, Ethernet0
C    172.16.40.0 is directly connected, Serial0
S*   0.0.0.0/0 [1/0] via 172.16.40.1
2501C#
```

Notice also in the routing table that the gateway of last resort is now set. However, there is one more command you must be aware of when using default routes: the `ip classless` command.

All Cisco routers are classful routers, which means they expect a default subnet mask on each interface of the router. When a router receives a packet for a destination subnet not in the routing table, it will drop the packet by default. If you are using default routing, you must use the `ip classless` command because no remote subnets will be in the routing table. The command is shown below:

```
2501C(Config)#ip classless
```

Notice that it is a global configuration mode command. Since version 11.2 of the IOS, the `ip classless` command has been enabled by default. In a classful network, a router believes that it knows all subnets based on the subnet assigned to the interface¡¯s IP address. If a packet is addressed to a host within the classed network space, but the routing table does not have a route to it, the packet will be discarded.

Configuring RIP Routing

To configure RIP routing, just turn on the protocol with the `router rip` command and tell the RIP routing protocol which networks to advertise. For example:

```
2621A(config)#router rip
2621A(config-router)#network 172.16.0.0
2621A(config-router)#^Z
2621A#
```

That¡¯s it. Two commands, and you¡¯re done¡ªsure makes your job a lot easier than when using static routes, doesn¡¯t it? However, keep in mind the extra router CPU process and bandwidth that you¡¯re consuming.

Verifying the RIP Routing Tables

Each routing table should now have the routers¡¯ directly connected routes as well as RIP-injected routes received from neighbor routers.

The router output below shows the contents of a router¡¯s routing table:

```
2621A#sh ip route
Codes: C - connected, S - static, I - IGRP, R - RIP,
ƒM¡ª[output cut]
Gateway of last resort is not set

   172.16.0.0/24 is subnetted, 5 subnets
R 172.16.50.0 [120/3] via 172.16.10.2, FastEthernet0/0
R 172.16.40.0 [120/2] via 172.16.10.2, FastEthernet0/0
R 172.16.30.0 [120/2] via 172.16.10.2, FastEthernet0/0
R 172.16.20.0 [120/1] via 172.16.10.2, FastEthernet0/0
C 172.16.10.0 is directly connected, FastEthernet0/0
2621A#
```

In the above output, the `R` means that the networks were added dynamically using the RIP routing protocol. The `[120/3]` is the administrative distance of the route (120) along with the number of hops to that remote network (3).

Exam Essentials

Understand how RIP works in an internetwork. RIP uses hop counts to determine the best route to a network. It has an upper hop-count limit of 15.

Go through the commands to add RIP to your router. To add the RIP routing protocol to your router, go into global configuration mode and type **router rip**. You then need to add the number(s) of the network(s) for which your router will advertise.

Know how to view the routing table. To view routing tables, you can use the command `show ip route` or `show ip route rip`.

Understand what the routing table shows. You must know how to read a routing table. Make sure you can find the hop count, destination network, and next hop router address.

Remember what the arguments are in a static route. To create a static route, use the `ip route` command followed by the destination network, subnet mask, next hop address, and the metric.

Key Terms and Concepts

administrative distance Used to rate the trustworthiness of routing information received on a router from a neighbor router. An administrative distance is an integer from 0 to 255, where 0 is the most trusted, and 255 means no traffic will be passed via this route.

distance-vector A routing algorithm that typically uses hop counts to find the best path to a network. Some of the newer distance-vector algorithms use other variables such as bandwidth, delay, and line speed. RIP uses only hop count.

dynamic routing Using a routing protocol to discover routes through the network.

hold-downs A method of stopping routing loops by not sending out updates about networks that have gone down.

route poisoning with poison reverse Sets a downed link to the maximum number of valid hops or to infinity.

Routing Information Protocol (RIP) A routing algorithm that uses the distance-vector method of finding the best path to a network (hop count).

split horizon A method of stopping routing loops by not sending updates out the same interface through which they were received.

static route A route manually entered into the router¡¯s configuration.

Add the IGRP routing protocol to your configuration.

Interior gateway protocols (IGPs) are used to dynamically configure routers in an autonomous system (AS). Exterior gateway protocols (EGPs) are used to communicate between IGPs; one example is Border Gateway Protocol (BGP).

The two IGPs discussed in this book are Routing Information Protocol (RIP) and Interior Gateway Routing Protocol (IGRP), which is a Cisco proprietary dynamic routing protocol. To pass the CCNA exam, you must know the protocols discussed in this objective.

Critical Information

Interior Gateway Routing Protocol (IGRP) is a Cisco proprietary distance-vector routing protocol. This means that to use IGRP in your network, all your routers must be Cisco routers. Cisco created this routing protocol to overcome the problems associated with RIP such as the 16-hop-count limit.

IGRP has a maximum hop count of 255 with a default of 100. This is helpful in larger networks and solves the problem of the 15-hop maximum in a RIP network. IGRP also uses a different *metric*, a value used to calculate the best route. IGRP uses bandwidth and delay of the line by default as a metric for determining the best route to an internetwork; this is called a composite metric. Reliability, load, and maximum transmission unit (MTU) can also be used, although they are not used by default.

Configuring IGRP Routing

The command used to configure IGRP is the same as the one used to configure RIP routing, with one important difference: You use an autonomous system (AS) number. All routers within an autonomous system must use the same AS number, or they will not communicate with routing information. Here is an example of how to turn on IGRP routing, using an AS number of 10:

```
RouterA#config t
RouterA(config)#router igrp 10
RouterA(config-router)#network 172.16.0.0
```

The configuration in the above router commands is as simple as in RIP routing, except that IGRP uses an AS number. This number is used to advertise only to routers with which you want to share routing information.

IGRP can load-balance to six unequal links to a remote network. RIP networks must have the same hop count to be able to load-balance, whereas IGRP uses bandwidth to determine how to load-balance. To load-balance over unequal-cost links, the `variance` command controls the load balancing between the best metric and the worst acceptable metric.

Verifying the IGRP Routing Tables

Once the routers are configured, you need to verify the configuration with the `show ip route` command.

```
2621A#sh ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, ƒM ¨C
[output cut]
    T - traffic engineered route
Gateway of last resort is not set

   172.16.0.0/24 is subnetted, 5 subnets
I    172.16.50.0 [100/160360] via 172.16.10.2, ƒFastEthernet0/0
I    172.16.40.0 [100/160260] via 172.16.10.2, ƒFastEthernet0/0
I    172.16.30.0 [100/158360] via 172.16.10.2, ƒFastEthernet0/0
I    172.16.20.0 [100/158260] via 172.16.10.2, ƒFastEthernet0/0
C    172.16.10.0 is directly connected, ƒFastEthernet0/0
```

The `I` means IGRP-injected routes. The `[100/160360]` is the administrative distance of IGRP and the composite metric. The lower the composite metric, the better the route.

Exam Essentials

Remember what an AS is. An autonomous system (AS) is a group of routers that share the same routing information.

Understand the difference between RIP and IGRP. RIP uses only hop counts in determining the best route to a destination network. IGRP can look at bandwidth, load, reliability, MTU, and hop count to find the best route to a destination network.

Key Terms and Concepts

Interior Gateway Routing Protocol (IGRP) A proprietary Cisco distance-vector routing algorithm.

metric The distance or weight of a link. This value can be used to find the best path to a remote network.

Chapter 5: WAN Protocols

Cisco Certified Network Associate Exam Objectives Covered in This Chapter:

- Recognize key Frame Relay terms and features.*(pages 136¡ª140)*
- List commands to configure Frame Relay LMIs, maps, and subinterfaces.*(pages 140¡ª145)*
- List commands to monitor Frame Relay operation in the router.*(pages 146¡ª147)*
- State a relevant use and context for ISDN networking.*(pages 148¡ª152)*
- Identify ISDN protocols, function groups, reference points, and channels.*(pages 152¡ª155)*
- Identify PPP operations to encapsulate WAN data on Cisco routers.*(pages 155¡ª162)*

This chapter covers the wide area network (WAN) protocols used by the Cisco Internetwork Operating System (IOS). After reading this chapter you should have a good understanding of the WAN protocols including Frame Relay, ISDN, and PPP. For Frame Relay and ISDN, you should know not only how to configure them on a router, but also how to support and monitor their usage.

Recognize key Frame Relay terms and features.

This section discusses the terminology used for the various features within a Frame Relay network. You will learn how two internetwork devices communicate end-to-end through a Frame Relay cloud by using a DLCI number, DTE, DCE, demarcation (demarc), local loop, and PSE.

It is important to understand the difference between these devices and to know the terms used for them, both when you are working in a production environment and when you are studying for your CCNA exam. In a real network, it is helpful if you can visualize how the frame traverses the internetwork, as well; you¡¯ll have a better chance of troubleshooting problems.

Critical Information

To understand the terminology used in Frame Relay networks, first you need to know how the technology works. Figure 5.1 is labeled with the various terms used to describe different parts of a Frame Relay network.

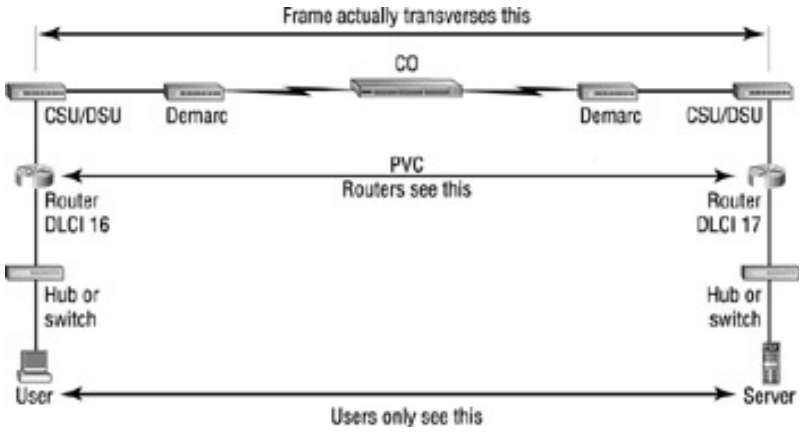

Figure 5.1: Frame relay technology and terms

The basic idea behind Frame Relay is to allow users to communicate between two *data terminal equipment (DTE)* devices through *data communication equipment (DCE)*. The users should not see a difference between connecting to and gathering resources from a local server and a server at a remote site connected with Frame Relay. Chances are that this connection will be slower than a 100Mbps Ethernet LAN, but the difference in the connection should be transparent to the user.

Figure 5.1 illustrates everything that must happen in order for two DTE devices to communicate. Here is how the process works:

1. The user¡¯s network device sends out a frame on the local network. The hardware address of the router (default gateway) will be in the frame header.

2. The router picks up the frame, extracts the packet, and discards the frame. It then looks at the destination IP address within the packet and checks to see if it knows how to get to the destination network by looking in the routing table.

3. The router then forwards the data to the interface that it thinks can find the remote network. (If the router can¡¯t find the network in its routing table, it discards the packet.) Since this will be a serial interface encapsulated with Frame Relay, the router puts the packet onto the Frame Relay network encapsulated within a Frame Relay frame. It will add the Data Link Connection Identifier (DLCI; discussed later in this chapter) number associated with the serial interface. DLCIs identify the type of virtual circuit¡ª*permanent virtual circuit (PVC)* or *switched virtual circuit (SVC)*¡ªto the routers and switches participating in the Frame Relay network.

4. The channel service unit/data service unit (CSU/DSU) receives the digital signal and encodes it into the type of digital signaling that the switch at the *packet switching exchange (PSE)* can understand. The PSE receives the digital signal and extracts the 1s and 0s from the line. The CSU/DSU is connected to a *demarcation point (demarc)* installed by the service provider, and its

location is the service provider¡¯s first point of responsibility (the last point on the receiving end). The demarc is typically just an RJ-45 jack installed close to the router and CSU/DSU.

5. The demarc is typically a twisted-pair cable that connects to the *local loop*, which connects to the closest *central office (CO)*, sometimes called a point of presence (POP). The local loop can connect using various physical media, but twisted-pair or fiber is very common.

6. The CO receives the frame and sends it through the Frame Relay ¡°cloud¡± to its destination. This cloud can be dozens of switching offices¡ªor more! The CO looks for the DLCI number, which is mapped locally to an IP address in IP networks. Typically it can find the DLCI number of the remote device or router by looking up an IP-to-DLCI mapping. Frame Relay mappings are usually created statically by the service provider, but they can be created dynamically.

7. Once the frame reaches the switching office closest to the destination office, it is sent through the local loop. The frame gets to the demarc and then to the CSU/DSU. Finally, the router extracts the packet, or datagram, from the frame and puts it in a new LAN frame to be delivered to the destination host. Whew!

The user and the server do not need to know, nor should they know, everything that happens as the frame makes its way across the Frame Relay network. The remote server should be as easy to use as a locally connected resource.

Exam Essential

Understand where each of the terms is used in a Frame Relay network. Remember that a DTE is typically the router; the DCE is typically the CSU/DSU and switch located at the provider.

Key Terms and Concepts

central office (CO) Point at which the local loop gains access to the service provider¡¯s high-speed trunk lines. This is often referred to as a point of presence (POP).

data communication equipment (DCE) Specific communications equipment, such as packet switches, that interface between a PSE and DTE devices. DCEs are typically found in carrier facilities.

data terminal equipment (DTE) End-systems that communicate over an X.25 network (such as host systems, terminals, and PCs that belong to the individual subscriber) and that are present at the same site.

demarcation point (demarc) The boundary between the customer¡¯s in-house wiring and the service provider¡¯s wiring. This is the point where the service provider¡¯s responsibility ends.

local loop Wiring running from the demarc to the CO.

packet switching exchange (PSE) Switches that constitute the majority of a carrier¡¯s network and handle the transfer of data between DTE devices via the X.25 packet-switched network.

permanent virtual circuit (PVC) An established connection used for recurrent, steady data transfer. PVC sessions are continuously active, so DTEs can transmit data whenever necessary.

switched virtual circuit (SVC) A temporary connection used for intermittent data transfers. When using an SVC, DTE devices must establish, maintain, and then terminate a session every time they need to communicate.

List commands to configure Frame Relay LMIs, maps, and subinterfaces.

To prepare you for this portion of the CCNA exam, this section demonstrates how to configure a Cisco router to be used in a Frame Relay network. It explains the steps for configuring a router to use the Frame Relay encapsulation, assigning a DLCI number, and choosing a Local Management Interface (LMI) type. Additionally, you will learn how to create a subinterface and why you should use one. You¡¯ll finish the configuration by creating a Frame Relay mapping.

Critical Information

The next few sections jump right into configuring Frame Relay¡¯s LMIs, maps, and the router¡¯s subinterfaces.

Necessary Procedures

It¡¯s important to learn the commands and procedures for configuring a router for use on a Frame Relay network. Frame Relay is used in many internetworks, and Cisco requires you to understand how to configure it if you are going to be a CCNA.

When configuring Frame Relay on Cisco routers, the first thing you do is specify an *encapsulation* type on serial interfaces. The encapsulation type is used ensure that both routers communicating are speaking the same language; a mismatched encapsulation type would make it difficult for the routers to communicate. There are only two encapsulation types: Cisco and IETF (Internet Engineering Task Force). Use these commands:

```
RouterA(config)#int s0
RouterA(config-if)#encapsulation frame-relay ?
 ietf Use RFC1490 encapsulation
 <cr>
```

Cisco is the default encapsulation unless you type **ietf**. Use Cisco encapsulation when you are connecting two Cisco devices. Use IETF encapsulation when you are connecting a Cisco device to a non-Cisco device using Frame Relay.

Data Link Connection Identifiers (DLCIs)

As mentioned earlier, Frame Relay virtual circuits are identified by *Data Link Connection Identifiers (DLCIs)*. Because many virtual circuits can be terminated on a multipoint Frame Relay interface, many DLCIs are affiliated with one interface. For the IP devices at each end of a virtual circuit to communicate, their IP addresses are mapped to DLCIs. This is so that a multipoint device can point out the appropriate destination virtual circuit on the Frame Relay network to each packet sent over the single physical interface.

Each DLCI can have a local meaning. In other words, two DTE devices connected via a virtual circuit use different DLCI values when referring to the same connection.

Here is an example that shows how to configure a DLCI number to an interface:

```
RouterA(config-if)#frame-relay interface-dlci ?
<16-1007> Define a DLCI as part of the current ƒsubinterface
RouterA(config-if)#frame-relay interface-dlci 16
```

Local Management Interface (LMI)

The *Local Management Interface (LMI)* was developed in 1990 by Cisco Systems, StrataCom, Northern Telecom, and Digital Equipment Corporation. The protocol produced by this group became known as the Gang-of-Four LMI, or Cisco LMI. This ¡°gang¡± took the basic Frame Relay protocol and added extensions to its features that allowed internetworking devices to communicate easily with a Frame Relay network. LMI is used only between the router and the service provider¡¯s switch.

LMI messages provide information about the current DLCI values, the global or local significance of the

DLCI values, and the status of virtual circuits. You will need to check with your Frame Relay provider to find out which LMI type to use. The default type is Cisco, but you may need to change to ANSI or Q.933A. You can display the three LMI types on your screen using the command shown here:

```
RouterA(config-if)#frame-relay lmi-type ?
 cisco
 ansi
 q933a
```

All standard LMI signaling formats are supported by the following:

ANSI Annex D, defined by ANSI standard T1.617.

ITU-T (Q.933A) Annex A, defined by ITU-T Recommendation Q.933A.

Cisco LMI, defined by the ¡°Gang of Four¡± (default).

Note With Cisco IOS version 11.2 and above, the LMI type is set to auto-detect by default.

Subinterfaces

You can have multiple virtual circuits on a single serial interface and treat each virtual circuit as a separate interface, called a subinterface. Think of a subinterface as a hardware interface defined by the IOS software.

The advantage to using subinterfaces is that you can assign different Network-layer characteristics to each subinterface and virtual circuit, such as IP routing on one virtual circuit and IPX on another. Define subinterfaces with the command `interface s0.`*`subinterfacenumber`*, as shown in this example:

```
RouterA(config)#int s0.?
 <0-4294967295> Serial interface number
RouterA(config)#int s0.16 ?
 multipoint   Treat as a multipoint link
 point-to-point Treat as a point-to-point link
```

You can define a limitless number of subinterfaces on a given physical interface, keeping router memory in mind. In the above example, we chose to use subinterface 16 because that is the DLCI number of that interface. You can choose any number between 0 and 4294967295.

The two types of subinterfaces are point-to-point and multipoint. Point-to-point subinterfaces are used when a single virtual circuit connects one router to another. Multipoint subinterfaces are used when the router is at the center of a star of virtual circuits.

Mapping Frame Relay

As explained earlier, in order for IP devices at the ends of virtual circuits to communicate, their addresses must be mapped to the DLCIs. There are two ways to make this mapping happen:

- Use the `frame-relay map` command.
- Use the `inverse-arp` function.

For each packet sent out of a physical interface, mappings allow a multipoint device to identify a virtual circuit on the Frame Relay network.

This is an example program that uses the `frame-relay map` command:

```
RouterA(config)#int s0.16 point-to-point
RouterA(config-if)#encap frame-relay ietf
RouterA(config-if)#no inverse-arp
RouterA(config-if)#ip address 172.16.30.1 255.255.255.0
RouterA(config-if)#frame-relay map ip 172.16.30.17 20 ƒcisco broadcast
RouterA(config-if)#frame-relay map ip 172.16.30.18 30 ƒbroadcast
RouterA(config-if)#frame-relay map ip 172.16.30.19 40
```

Here¡¯s what we did: First, we chose our subinterface and set the encapsulation to IETF. Then we turned off `inverse-arp` (IARP) and mapped three virtual circuits and their corresponding DLCI numbers. (IARP would map our DLCIs to IP addresses dynamically, as demonstrated below.) Notice that we specified Cisco encapsulation on the first virtual circuit. The other two virtual circuits will use the encapsulation type specified in the interface command (IETF). The `frame-relay map` command is

the only way to mix both Cisco and IETF encapsulation types. The `broadcast` keyword at the end of the `map` command tells the router to forward broadcasts for this interface to this specific virtual circuit.

Instead of putting in `map` commands for each virtual circuit, you can use the `inverse-arp` (IARP) function to perform dynamic mapping of the IP address to the DLCI number. In that case, your configuration program would look like this:

```
RouterA(config)#int s0.16 multipoint
RouterA(config-if)#encap frame-relay ietf
RouterA(config-if)#ip address 172.16.30.1 255.255.255.0
```

Yes, this is a whole lot easier, but it¡¯s not as stable as using the `map` command. Why? Sometimes when you use the `inverse-arp` function, configuration errors occur, because virtual circuits can be insidiously and dynamically mapped to unknown devices.

Note Frame Relay mapping isn¡¯t something an administrator would typically do. This process is usually performed at the switching office. Check with your provider before doing any Frame Relay configurations.

Exam Essentials

Understand how to configure Frame Relay on a Cisco router. It is crucial that you understand the difference between encapsulation, DLCI, LMI, and mappings.

Know how many encapsulation and LMI types Cisco supports. Cisco supports two encapsulation methods (Cisco and IETF) and three LMI types (Cisco, ANSI, and Q.933A).

Key Terms and Concepts

Data Link Connection Identifiers (DLCIs) Used to identify a Frame Relay virtual circuit. A Frame Relay service provider, like a telephone company, typically assigns DLCI values that are used by the Frame Relay protocol to distinguish between different virtual circuits on the network.

encapsulation A method of encasing or wrapping data (packets) within a protocol that is understood by the device on the opposite side of the link.

Local Management Interface (LMI) LMI messages are used to provide three types of information¡ªthe current DLCI values, the global or local significance of the DLCI values, and the status of virtual circuits¡ªto routers participating in the Frame Relay network.

List commands to monitor Frame Relay operation in the router.

When you are working in a production environment that uses Frame Relay and while you are studying for the CCNA exam, this topic is an important one. You must have a fundamental understanding not only of how to configure Frame Relay but also of the commands to monitor and troubleshoot Frame Relay.

Critical Information

Frame Relay on Cisco routers is both stable and popular. If you want to work in a production environment, the ability to configure and maintain Frame Relay networks is sometimes a prerequisite to landing such a job. Knowing how to monitor and troubleshoot this protocol is a big part of that skill.

There are several ways to check the status of your interfaces and PVCs once you have Frame Relay encapsulation set up and running. Use the `show frame-relay ?` command at the router prompt to display all the commands you can use to view Frame Relay specifications:

```
Router#sh frame-relay ?
 ip    show frame relay IP statistics
 lapf   show frame relay lapf status/statistics
 lmi   show frame relay lmi statistics
 map   Frame-Relay map table
 pvc   show frame relay pvc statistics
 route  show frame relay route
 svc   show frame relay SVC stuff
 traffic Frame-Relay protocol statistics
```

For monitoring purposes, the commands you¡¯ll be using are `show frame-relay pvc`, `show frame-relay lmi`, `show frame-relay traffic`, and `show interface`. Here¡¯s how to use each command:

show frame-relay pvc Gives the statistics of your PVCs on all configured Frame Relay interfaces.

show frame-relay lmi Displays the LMI statistics and the LMI type used on your Frame Relay network.

show frame-relay traffic Shows you the global Frame Relay statistics since the last time the router was booted.

show interface s0 Displays your LMI information and DLCI type (local or switched) but not the DLCI number.

Exam Essentials

Remember which commands display your DLCI number and LMI type. The commands `show frame-relay pvc` and `show running- config` display your DCLI number. The `show interface` and `show frame-relay lmi` commands give you the router¡¯s LMI and bandwidth information.

Know how to configure a Cisco router¡¯s subinterface. You should have a good understanding of the commands to configure a Cisco router¡¯s subinterface and the commands and procedures to configure Frame Relay.

Key Terms and Concepts

permanent virtual circuit (PVC) An established connection used for recurrent, steady data transfer. PVC sessions are continuously active, so DTEs can transmit data whenever necessary.

switched virtual circuit (SVC) A temporary connection used for intermittent data transfers. When using an SVC, DTE devices must establish, maintain, and then terminate a session every time they need to communicate.

State a relevant use and context for ISDN networking.

Integrated Services Digital Network (ISDN) is a very popular type of connectivity, if you can get it. It provides enough bandwidth to allow voice and data transmission at fast speeds, making it very useful for telecommuters. Another nice thing about this technology is that it allows digital services over standard telephone cable.

However, the problem with ISDN is that it is not available everywhere. This is because some types of telephone cable cannot support the encoding necessary to transmit large amounts of data.

To pass this portion of the CCNA exam, make sure you understand the purpose of ISDN and its advantages, ISDN protocols, and the reference points used in ISDN.

Critical Information

Integrated Services Digital Network (ISDN) is a digital service designed to run over existing telephone networks. Because it can support both data and voice transmissions, ISDN is perfect for the users on your network who telecommute. But ISDN applications require high bandwidth. Typical uses for ISDN include high-speed image applications (such as Group IV facsimile), high-speed file transfer, videoconferencing, and multiple links into the homes of telecommuters.

ISDN is actually a set of communication protocols and standards devised by telephone companies that define the hardware and call- setup schemes for end-to-end digital connectivity. With it they can provide digital services that simultaneously convey data, text, voice, music, graphics, and video to end users, all the while using the telephone systems that are already in place. ISDN is referenced by a suite of standards, issued by the *International Telecommunication Union* Telecommunication Standardization Sector (ITU-T), that encompass the OSI model¡¯s Physical, Data Link, and Network layers.

ISDN supports virtually every upper-layer network protocol (IP, IPX, AppleTalk, and so on), and you can choose Point-to-Point Protocol (PPP), High-Level Data-Link Control (HDLC), or Link Access Procedure on the D Channel (LAPD) as your encapsulation protocol.

People in the networking industry tend to use a lot of acronyms and other lingo to describe basic things. The parts of ISDN are no exception. This section defines some of these terms and the features they describe.

The components discussed are really the nuts and bolts of ISDN, which are very important for you to understand when setting up an ISDN connection and when studying for the CCNA exam.

Cisco¡¯s Implementation of ISDN BRI

Basic Rate Interface (BRI) service is very popular in the U.S. because it provides 128Kbps transmission at a good price. BRI is not the best choice for large, steady data streams, but it works well for bursts of data.

ISDN BRI, also known as 2B+1D, provides two B channels and one D (data) channel. The BRI B-channel service operates at 64Kbps and carries data, while the BRI D-channel service operates at 16Kbps and usually carries control and signaling information. The D-channel signaling protocol spans the OSI Reference Model¡¯s Physical, Data Link, and Network layers. BRI also provides framing control for a total bit rate of up to 192Kbps.

When configuring ISDN BRI, you will need to obtain Service Profile Identifiers (SPIDs); you should have one SPID for each B channel or two for BRI. SPIDs can be thought of as the telephone number of each B channel. The ISDN device gives the SPID to the ISDN switch, which then allows the device to access the network for BRI or PRI (Primary Rate Interface) service. If an ISDN device doesn¡¯t have an SPID, many ISDN switches won¡¯t allow it to place a call on the network.

NT1 and NT2

The NT1 is a device that resides between the ISDN switch and the Cisco ISDN interface or terminal adapter (TA), both of which are referred to as the terminal endpoints. The NT1 is used to convert two-wire copper loop from the telephone company. This point in the network is called the U-loop. From the U-loop, it converts the two-wire into a four-wire ISDN interface called the S/T bus. Many ISDN terminal

equipment (TE) devices have an NT1 built into the BRI interface.

The NT2 is a device used in older ISDN networks connecting to terminals or other older equipment.

Q.921 and Q.931

In ISDN, the Data Link layer goes by the name of Q.921, which is the ITU standard for ISDN operations at layer 2 of the OSI Reference Model. One surprising aspect of ISDN is that it has been around since the 1960s. Understanding this and Frame Relay will help you to understand how LAPB (Link Access Procedure Balanced) uses sequence numbers and delivers ISDN layer 3 messages on the D channel, without error, from the TE BRI interface to the ISDN switch. Checking and retransmissions are handled at the Data Link layer. LAPB messages are passed only between the TE and ISDN switch, not end-to-end.

Q.931 architecture, operating at layer 3, offers flexibility that allows it to be customized for use in environments such as Frame Relay SVCs, ATM SVCs, Voice over IP, and digital cellular networks. Q.931 SETUP messages are created by the TE and are then carried in Q.921 LAPD frames to the ISDN switch. The ISDN switch can then route calls over the PSTN (public switched telephone network) to its final destinations based on information in the Q.931 messages.

Let¡¯s take a look at how to configure ISDN in the next section.

Necessary Procedures

In order to use ISDN with a Cisco router, you need to purchase either a network termination type 1 (NT1) device or an ISDN modem. If your router has a BRI interface, you¡¯re all set. Otherwise, you can use one of your router¡¯s serial interfaces¡ªif you can get a hold of a TA. A router with a BRI interface is called a TE1 (terminal equipment type 1) device; one that requires a TA is called a TE2 device.

ISDN supports virtually every upper-layer network protocol (IP, IPX, AppleTalk, etc.), and you can choose PPP, HDLC, or LAPD as your encapsulation protocol.

Note When configuring ISDN, you¡¯ll need to know the type of switch that your service provider is using, because each manufacturer has a proprietary protocol for signaling. To see which switches your router will support, use the `isdn switch-type ?` command in global configuration mode.

For each ISDN BRI interface, you need to specify the SPIDs by using the `isdn spid1` and `isdn spid2` interface subcommands. Here¡¯s an example:

```
RouterA#config t
Enter configuration commands, one per line. End with ƒCNTL/Z.
RouterA(config)#isdn switch-type basic-dms100
RouterA(config)#int bri0
RouterA(config-if)#encap ppp
RouterA(config-if)#isdn spid1 775456721
RouterA(config-if)#isdn spid2 775456722
```

This configuration assumes that the interfaces on both ends of the link have already been configured with an IP address in the same network. The encapsulation is PPP; ISDN specifies this method, used to establish the digital phone call.

Exam Essentials

Remember the different services that ISDN can run. ISDN can run both voice and data services over existing telephone lines.

Know the difference between a B channel and a D channel. A BRI uses two B channels and one D channel. Each B channel is 64Kbps; a D channel is 16Kbps.

Key Terms and Concepts

Basic Rate Interface (BRI) An ISDN interface composed of two B channels and one D channel for circuit-switched communication of voice, video, and data.

Integrated Services Digital Network (ISDN) A digital communication protocol that permits telephone networks to carry data and voice transmissions at higher speeds than typical analog transmission rates.

International Telecommunication Union Telecommunication Standardization Sector (ITU-T) A group that creates international standards for internetworks and telecommunications.

Identify ISDN protocols, function groups, reference points, and channels.

In order to have a good understanding of ISDN, you need to know more than its uses, as you learned in the last section. You need to know about ISDN¡¯s protocol groups, its protocols, how to identify reference points, and ISDN channels.

Critical Information

This section takes an in-depth look at the following ISDN topics:

- ISDN Protocols
- ISDN Function Groups
- ISDN Reference Points
- ISDN Channels

ISDN Protocols

ISDN protocols are defined by the ITU-T. There are three diverse categories of ISDN protocols whose functions are specified by their first letter:

- E protocols apply to ISDN on an existing telephone network.
- I protocols deal with concepts, terminology, and services.
- Q protocols pertain to switching and signaling.

ISDN Function Groups

Function groups connecting to the ISDN network are known as terminals. These come in two types:

- TE1 (terminal equipment type 1) devices are BRI machines that understand ISDN standards.
- TE2 (terminal equipment type 2) devices predate ISDN standards. To use a TE2 device, you have to use a terminal adapter (TA) to generate BRI signals for a Cisco router interface.

ISDN Reference Points

ISDN uses four different *reference points* to define logical interfaces between functional groupings such as TAs and NT (network termination) devices. They are as follows:

- R defines the reference point between non-ISDN equipment and a TA.
- S defines the reference point between user terminals and an NT2 device.
- T defines the reference point between NT1 and NT2 devices.
- U defines the reference point between NT1 devices and line-termination equipment in a carrier network. (This type of reference point is used only in North America, where the NT1 function isn¡¯t provided by the carrier network.)

Figure 5.2 shows the ISDN functions and reference points.

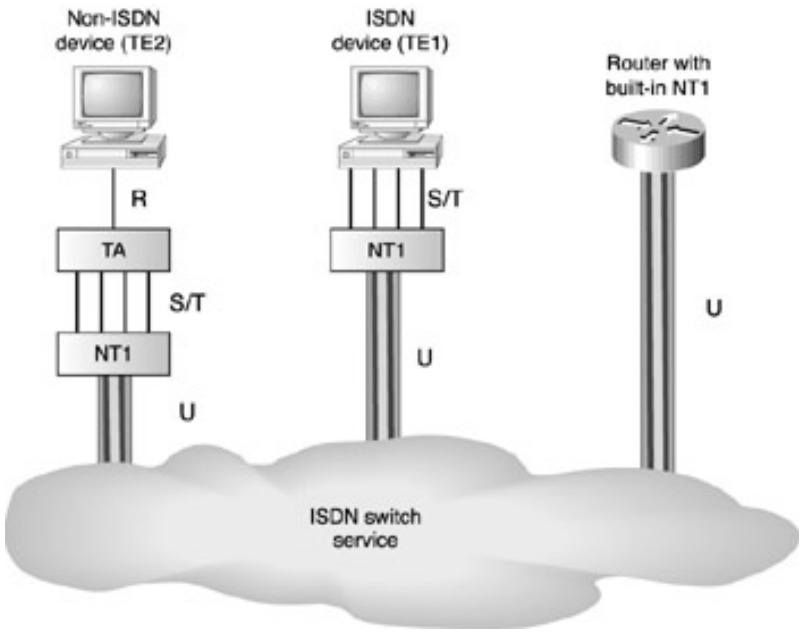

Figure 5.2: ISDN functions and reference points

Note The S and T reference points are generally one and the same.

ISDN Channels

As discussed earlier, there are two types of channels used in BRI ISDN: B and D. Here¡¯s what each one does:

- B, or bearer, channels have a 64Kbps capacity. They can be used for voice or data. Two B channels in a BRI can be combined for a total of 128Kbps.
- D, or data, channels are used for call signaling or clocking. This type of channel has a 16Kbps capacity.

Exam Essential

Understand the different protocols used in ISDN. The Q protocols specify switching and signaling. E protocols apply to ISDN on an existing telephone network. I protocols deal with concepts, terminology, and services.

Key Term and Concept

reference point Used to define logical interfaces in ISDN.

Identify PPP operations to encapsulate WAN data on Cisco routers.

P*oint-to-Point Protocol (PPP)* is a data-link protocol that can be used over either asynchronous serial (dial-up) or synchronous serial (ISDN) media, and uses the Link Control Protocol (LCP) to build and maintain data-link connections.

PPP was created to work with multiple protocols at the Network layer and to replace Serial Line Internet Protocol (SLIP), which could run only IP at the Network layer. This section covers Cisco support for PPP encapsulation as well as authentication.

Critical Information

PPP can be used in asynchronous and synchronous networks. The steps for configuring PPP for synchronous networks on Cisco routers are covered in the ¡°Necessary Procedures¡± section. Configuring PPP encapsulation on an interface is a fairly straightforward process.

Of course, in order for PPP encapsulation to work, it must be enabled on both interfaces that are connected to a serial line. Once you have PPP encapsulation enabled, you can verify that it¡¯s up and running with the `show interface` command.

The basic purpose of PPP is to transport layer-3 packets across a Data Link layer point-to-point link. Figure 5.3 shows the protocol stack compared to the OSI Reference Model.

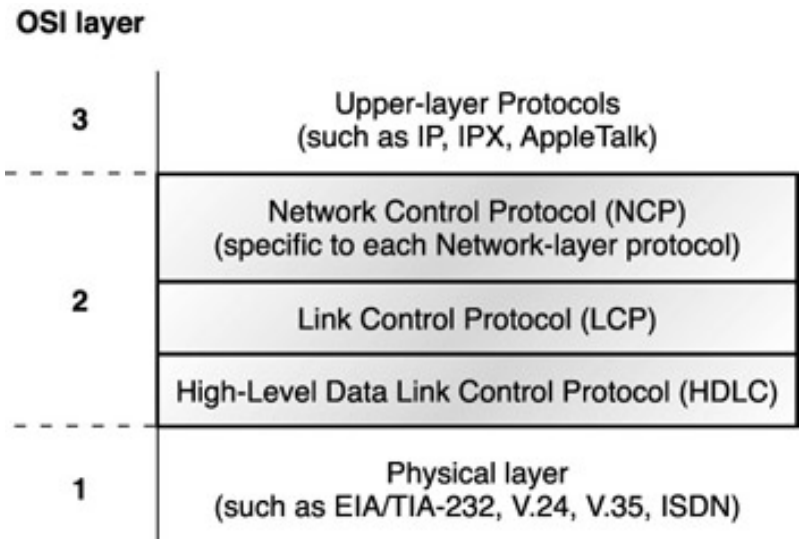

Figure 5.3: Point-to-Point Protocol stack

PPP contains four main components:

EIA/TIA-232-C A Physical-layer international standard for serial communication.

High-Level Data Link Control (HDLC) Protocol A method for encapsulating datagrams over serial links.

Link Control Protocol (LCP) A method of establishing, configuring, maintaining, and terminating the point-to-point connection.

Network Control Protocol (NCP) A method of establishing and configuring different Network-layer protocols. PPP is designed to allow the simultaneous use of multiple Network-layer protocols. Some examples of protocols here are Internet Protocol Control Protocol (IPCP) and Internetwork Packet Exchange Control Protocol (IPXCP).

It is important to understand that the PPP protocol stack is specified at the Physical and Data Link layers only. NCP is used to allow communication of multiple Network-layer protocols by encapsulating

the protocols across a PPP data link.

LCP Configuration Options

Link Control Protocol (LCP) offers PPP encapsulation different options, including the following:

Authentication This option tells the calling side of the link to send information that can identify the user. The two methods you need to know are PAP and CHAP.

compression This is used to increase the throughput of PPP connections. PPP decompresses the data frame on the receiving end. Cisco uses the Stacker and Predictor compression methods.

Error Detection PPP uses Quality and Magic Number options to ensure a reliable, loop-free data link.

Multilink Starting in IOS version 11.1, multilink is supported on PPP links with Cisco routers. This splits the load for PPP over two or more parallel circuits. The grouping of these multiple links from one location to another is referred to as a bundle.

PPP Session Establishment

PPP can be used with authentication. This means that routers communicating must provide information to identify the link as a valid communication link. When PPP connections are started, the links go through three phases of session establishment:

Link-Establishment Phase LCP packets are sent by each PPP device to configure and test the link. The LCP packets contain a field called Configuration Option that allows each device to see the size of the data, compression, and authentication. If no Configuration Option field is present, then the default configurations are used.

Authentication Phase If configured, either CHAP or PAP can be used to authenticate a link. Authentication takes place before Network- layer protocol information is read.

Network-Layer Protocol Phase PPP uses NCP to allow multiple Network-layer protocols to be encapsulated and sent over a PPP data link.

PPP Authentication Methods

There are two methods of authentication that can be used with PPP links: either *Password Authentication Protocol (PAP)* or *Challenge Authentication Protocol (CHAP)*.

Password Authentication Protocol (PAP) This is the less secure of the two methods. Passwords are sent in cleartext, and PAP is performed only upon the initial link establishment. When the PPP link is first established, the remote node sends the username and password back to the sending router until authentication is acknowledged. That¡¯s it.

Challenge Authentication Protocol (CHAP) This is used at the initial startup of a link and at periodic checkups to make sure the router is still communicating with the same host. After PPP finishes its initial phase, the local router sends a challenge request to the remote device. The remote device sends a value calculated using a one-way hash function called MD5. The local router checks this hash value to make sure it matches. If the values don¡¯t match, the link is immediately terminated.

Necessary Procedures

PPP is used when you need to connect routers from different manufacturers. Authentication can be used with PPP as well. Let¡¯s take a look at configuring PPP on a Cisco router.

Configuring PPP on Cisco Routers

Configuring PPP encapsulation on an interface is a fairly straightforward process. To configure it, follow these router commands:

```
Router#config t
Enter configuration commands, one per line. End with ƒCNTL/Z.
Router(config)#int s0
Router(config-if)#encapsulation ppp
Router(config-if)#^Z
Router#
```

Of course, PPP encapsulation must be enabled on both interfaces connected to a serial line to work, and there are several additional configuration options available by using the `help` command.

Configuring PPP Authentication

After you configure your serial interface to support PPP encapsulation, you can then configure authentication using PPP between routers. First, set the hostname of the router if it is not already set. Then set the username and password for the remote router connecting to your router. Here is an example:

```
Router#config t
Enter configuration commands, one per line. End with ƒCNTL/Z.
Router(config)#hostname RouterA
RouterA(config)#username todd password cisco
```

When using the `hostname` command, remember that the username is the hostname of the remote router connecting to your router. It is case-sensitive. Also, the password on both routers must be the same. It is a plaintext password and can be seen with a `show run` command. You can configure the password to be encrypted by using the command `service password-config` before you set the username and password. You must have a username and password configured for each remote system you are going to connect to. The remote routers must also be configured with usernames and passwords.

After you set the hostname, usernames, and passwords, choose the authentication type, either CHAP or PAP:

```
RouterA#config t
Enter configuration commands, one per line. End with ƒCNTL/Z.
RouterA(config)#int s0
RouterA(config-if)#ppp authentication chap
```

If both methods are configured, then only the first method is used during link negotiation. If the first method fails, then the second method will be used.

Verifying PPP Encapsulation

Now that we have PPP encapsulation enabled, let¡¯s take a look to verify that it¡¯s up and running. You can verify the configuration with the `show interface` command:

```
RouterA#show int s0
Serial0 is up, line protocol is up
 Hardware is HD64570
 Internet address is 172.16.20.1/24
 MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
   rely 255/255, load 1/255
 Encapsulation PPP, loopback not set,
   keepalive set (10 sec)
 LCP Open
 Listen: IPXCP
 Open: IPCP, CDPCP, ATCP
 Last input 00:00:05, output 00:00:05,
   output hang never
 Last clearing of "show interface" counters never
 Input queue: 0/75/0 (size/max/drops);
   Total output drops: 0
 Queueing strategy: weighted fair
 Output queue: 0/1000/64/0
   (size/max total/threshold/drops)
  Conversations 0/2/256
   (active/max active/max total)
  Reserved Conversations 0/0
   (allocated/max allocated)
 5 minute input rate 0 bits/sec, 0 packets/sec
 5 minute output rate 0 bits/sec, 0 packets/sec
  670 packets input, 31845 bytes, 0 no buffer
  Received 596 broadcasts, 0 runts, 0 giants,
    0 throttles
  0 input errors, 0 CRC, 0 frame, 0 overrun,
    0 ignored, 0 abort
  707 packets output, 31553 bytes, 0 underruns
```

```
  0 output errors, 0 collisions,
    18 interface resets
  0 output buffer failures,
    0 output buffers swapped out
21 carrier transitions
  DCD=up DSR=up DTR=up RTS=up CTS=up
RouterA#
```

Notice that the fifth line lists encapsulation as PPP, and the sixth line tells us that LCP is open. Remember that LCP¡¯s job is to build and maintain connections. The eighth line tells us that IPCP, CDPCP, and ATCP are open. This shows the IP, CDP, and AppleTalk support from NCP. The seventh line reports that we are listening for IPXCP.

Note You can verify the PPP authentication configuration by using the `debug ppp authentication` command.

Exam Essential

Know what PPP is and what its features are. PPP is the most commonly used authentication protocol for dial-up Internet access. Its features include address notification, authentication using PAP or CHAP, support of many protocols, and link monitoring.

Key Terms and Concepts

Challenge Authentication Protocol (CHAP) Supported on lines using PPP. This security feature uses encrypted passwords that identify the remote end of a connection, helping to keep out unauthor- ized users.

Link Control Protocol (LCP) Used to provide session setup, authentication, dynamic addressing, compression, and multilink.

Network Control Protocol (NCP) Used to provide multiple Network- layer protocols to run over the same PPP link.

Password Authentication Protocol (PAP) Unlike CHAP, PAP uses unencrypted passwords in PPP to identify a user for authentication. PAP is much less secure than CHAP.

Point-to-Point Protocol (PPP) A data encapsulation method that uses the Physical-, Data Link¨C, and Network-layer specifications of the OSI model. PPP provides synchronous and asynchronous circuits.

Chapter 6: Network Management

Cisco Certified Network Associate Exam Objectives Covered in This Chapter:

- Configure standard access lists to figure IP traffic.*(pages 164¡ª169)*
- Configure extended access lists to filter IP traffic.*(pages 170¡ª181)*
- Monitor and verify selected access list operations on the router.*(pages 182¡ª193)*

This chapter discusses access lists, which are used to filter traffic on a network. Without access lists, packets are free to transmit anywhere in the network. The following section focuses on IP (Internet Protocol) access lists. In the last section, you¡¯ll learn how to monitor and verify an access list operation. Access lists usage with IPX (Internetwork Packet Exchange) is also covered.

Configure standard access lists to figure IP traffic.

Essentially, access lists are lists of conditions; they¡¯re powerful tools that control access both to and from network segments. They can filter unwanted packets and can be used to implement security policies. With the right combination of access lists, network managers are armed with the power to enforce nearly any access policy they can invent.

Critical Information

An IP *access list* is a packet filter that packets are compared with, categorized by, and acted upon. Once the lists are built, they can be applied to either inbound or outbound traffic, on any interface. Applying an access list causes the router to analyze every packet crossing that interface in the specified direction and to take action accordingly.

There are a few important rules a packet follows when it¡¯s being compared with an access list:

- A packet is always compared with each line of the access list in sequential order (in other words, it¡¯ll always start with line 1, then go to line 2, then line 3, and so on).
- A packet is compared with lines of the access list only until a match is made. Once the packet matches a line of the access list, it¡¯s acted upon, and no further comparisons take place.
- There is an implicit ¡°deny¡± at the end of each access list. This means that if a packet doesn¡¯t match up to any lines in the access list, it¡¯ll be discarded.

Each of these rules has some powerful implications when filtering IP packets with access lists.

There are two types of access lists used with IP:

Standard Access Lists These use only the source IP address in an IP packet to filter the network, which basically permits or denies all messages from that address.

Extended Access Lists These check for both source and destination IP address, Protocol field in the Network-layer header, and Port Number in the Transport-layer header. Once you create an access list, you apply it to an interface with either an inbound or outbound list:

> **Inbound Access Lists** Packets are processed through the access list before being routed to the outbound interface.
>
> **Outbound Access Lists** Packets are routed to the outbound interface and then processed through the access list.

There are also some guidelines that should be followed when creating and implementing access lists on a router:

- You can assign only one access list per interface, per protocol, and per direction. This means that if you are creating IP access lists, you can have only one inbound access list and one outbound access list per interface.
- Organize your access lists so that the more specific tests are at the top of the access list.
- Anytime a new test is added to the access list, it will be placed at the bottom of the list.
- You cannot remove one line from an access list. If you try to do this, you will remove the entire list. It is best to copy the access list to a text editor before trying to edit the list. The only exception is when using named access lists.
- Unless your access list ends with a `permit any` command, all packets will be discarded if they do not meet any of the list¡¯s tests. Every list should have at least one `permit` statement, or you might as well shut down the interface.
- Create access lists and *then* apply them to an interface. It¡¯s possible to issue a command to apply

an access list to an interface before the list has been created; obviously, if you do that, you will not filter any traffic on that interface until the access list has been created.

- You should remove any active access lists applied to interfaces before deleting or altering the router¡¯s access list.
- Access lists are designed to filter traffic going through the router. They will not filter traffic originating from the router.
- Place IP standard access lists as close to the destination as possible.
- Place IP extended access lists as close to the source as possible.

IP Access Lists

IP access lists are configured in global configuration mode and are identified by the number assigned to the access list. The numbers 0 through 99 represent a standard IP access list, and 100 to 199 represent an extended IP access list.

Standard IP Access Lists

IP *standard access lists* can analyze the source IP addresses of TCP/IP packets and then take action based upon that analysis. Each line of a standard IP access list is created with a command in the following format:

`access-list` *`[number]`* `[permit or deny]` *`[source address]`*

To define access lists, use the `access-list` command in configuration mode. Each access list is assigned a unique number to distinguish it from the other lists. IP standard access lists are given numbers between 1 and 99, but other access-list types require different number ranges. Here is a sample command:

```
access-list 10 permit 172.16.30.2
```

This command adds a line to access list 10. The `permit` or `deny` keyword indicates whether to allow or discard matching packets, and the *`[source address]`* is used to define which source IP addresses should be acted upon.

Applying an IP Access List to an Interface

Even though you configure an access list, it won¡¯t filter anything until you apply it to an interface. First, enter configuration mode and select the Ethernet 0 interface. Then use the `ip access-group` command to specify `10 out`. Here is an example:

```
(config-int)ip access-group 10 out
```

Wildcard Masking

Wildcard masking allows you to specify either an entire network or a specific host. You can use wildcard masking in both standard and extended access lists.

In this example, we¡¯ve used a wildcard mask to specify the source address:

Address	172.	16.	30.	0
Mask	0.	0.	0.	255

It consists of a 32-bit binary string of 0s followed by 1s, broken into octets and written in decimal. Ones are considered throwaway bits, meaning that their corresponding positions in the address are irrelevant. By specifying the source address and mask as shown above, we¡¯re saying that the 172, 16, and 30 are required to match up, but the last octet of the IP address can be any value (remember that 255 is decimal format for binary 11111111). Likewise, when you specify a mask as follows, you¡¯re requiring 172, 16, 30, and 2 all to match up exactly, because you¡¯ve set all mask values to 0:

Address	172.	16.	30.	2
Mask	0.	0.	0.	0

Necessary Procedures

Here is an example of configuring with standard access lists:

```
RouterA#config t
RouterA(config)#access-list ?
 <1-99>        IP standard access list
 <100-199>     IP extended access list
 <1000-1099>   IPX SAP access list
 <1100-1199>   Extended 48-bit MAC address access list
 <1200-1299>   IPX summary address access list
 <200-299>     Protocol type-code access list
 <300-399>     DECnet access list
 <600-699>     Appletalk access list
 <700-799>     48-bit MAC address access list
 <800-899>     IPX standard access list
 <900-999>     IPX extended access list
```

To apply this configuration to an Ethernet interface, you could use this example:

```
RouterA#config t
Enter configuration commands, one per line. End with ƒCNTL/Z.
RouterA(config)#int e0
RouterA(config-if)#ip access-group 10 out
RouterA(config-if)#^Z
RouterA#
```

Wildcards can be used in a standard access list as follows:

```
RouterA#config t
RouterA(config)#access-list 10 permit 172.16.50.2 ƒ0.0.0.0
RouterA(config)#access-list 10 permit 172.16.30.0 ƒ0.0.0.255
RouterA(config)#int e0
RouterA(config-if)#ip access-group 10 out
RouterA(config-if)#^Z
RouterA#
```

Exam Essential

Know how to identify a standard access list. Standard access lists can filter only by source address. Also, they cannot filter by protocol or port.

Key Terms and Concepts

access list Used in routers to filter IP and IPX packets trying to either enter or leave an interface.

extended access list Security used in Cisco routers that can filter by source and destination address. It can filter by network address or by protocol and port.

standard access list Security used in Cisco routers that can filter only by source address.

wildcard masking A way to specify either an entire network or a specific host by applying a subnet mask used in Cisco access lists.

Configure extended access lists to filter IP traffic.

In the last section, you learned about standard access lists that are very limited in their ability to filter data packets. This section talks about extended access lists, which can filter data traffic at more specific variables. Let¡¯s take a close look at these lists and then check out an actual production router¡¯s configured access lists.

Critical Information

The function of extended access lists is pretty much the same as that of standard access lists. The difference centers on what can be filtered. In standard access lists, your decisions to permit or deny packets are limited to comparisons with the packets¡¯ source address information. But with extended access lists, you can act on any of the following:

- Source address
- Destination address
- IP protocol (TCP, UDP, ICMP, etc.)
- Port information (WWW, DNS, FTP, etc.)

So with extended access lists, your abilities are extended. You can make much more detailed lists than you can with the standard type. The syntax for each line on extended access lists is similar to that of standard access lists. The first three fields¡ªaccess-list, *number*, and permit or deny¡ªare exactly the same. But additionally you can specify a protocol before the *source* field, and create *destination* and *port* fields after the source address. Here¡¯s a template for each part of an IP extended access list (detailed examples of how to use this command are in the following Necessary Procedures section):

```
access-list [number] [permit or deny] [protocol] f[source] [destination] [port]
```

Necessary Procedures

This section provides you with configuration examples of IP access lists. Here is an example program that could be used to configure an extended access list:

```
RouterA#config t
RouterA(config)#access-list 110 permit tcp host f172.16.50.2 host 172.16.10.2 eq 8080
RouterA(config)#access-list 110 permit tcp f172.16.30.0 0.0.0.255 host 172.16.10.2 eq 8080
RouterA(config)#access-list 110 permit tcp any any feq www
RouterA(config)#int e0
RouterA(config-if)#ip access-group 110 out
RouterA(config-if)#^Z
```

Here¡¯s how the three access-list lines above map to our new template for IP extended access lists:

Protocol	Source	Destination	Port
tcp	host 172.16.50.2	host 172.16.10.2	eq 8080
tcp	172.16.30.0 0.0.0.255	host 172.16.10.2	eq 8080
tcp	any	any	eq www

The new field is for the protocol, and it¡¯s specified as TCP. In this case, you chose to allow TCP connections to your proxy on port 8080.

Here is an example of wildcard masking, but there are two new methods presented here; in reality, we¡¯re just using some keywords to save ourselves the effort of typing in the masks:

- host 172.16.10.2 is the same as specifying 172.16.10.2 0.0.0.0 with wildcard masking. Setting all the bits in the wildcard mask to 0s basically says there are no wildcards, so you can be referring to only a single machine or host. This means you can use the host keyword instead of the mask of 0.0.0.0.
- any is equivalent to specifying 0.0.0.0 255.255.255.255 with wildcard masking. When you set all bits in a wildcard mask to 1s, you get 255.255.255.255, so you¡¯re saying that none of the bits really matters. You can use this when you don¡¯t care about source or destination addresses because you¡¯re filtering based on some other parameter. In this example, you¡¯re filtering based upon the port.

Finally, you can specify the port to be acted upon. How well do you remember your TCP ports? You can enter a question mark (**?**) to get the list of available ports, as shown below. At this point, you could just end the command without specifying any port information, in which case all ports would be allowed. We chose to use the eq operator, but there are other numeric comparisons available that can be selected to specify more than one port. Once you select eq, you again have many options available:

```
RouterA#config t
RouterA(config)#access-list 110 permit tcp host f172.16.50.2 host 172.16.10.2 eq ?
 <0-65535>    Port number
 bgp          Border Gateway Protocol (179)
 chargen      Character generator (19)
 cmd          Remote commands (rcmd, 514)
 daytime      Daytime (13)
 discard       Discard (9)
```

```
 domain        Domain Name Service (53)
 echo          Echo (7)
 exec          Exec (rsh, 512)
 finger        Finger (79)
 ftp           File Transfer Protocol (21)
 ftp-data      FTP data connections (used ƒinfrequently, 20)
 gopher        Gopher (70)
 hostname      NIC hostname server (101)
 ident         Ident Protocol (113)
 irc           Internet Relay Chat (194)
 klogin        Kerberos login (543)
 kshell        Kerberos shell (544)
 login         Login (rlogin, 513)
 lpd           Printer service (515)
 nntp          Network News Transport Protocol (119)
 pim-auto-rp   PIM Auto-RP (496)
 pop2          Post Office Protocol v2 (109)
 pop3          Post Office Protocol v3 (110)
 smtp          Simple Mail Transport Protocol (25)
 sunrpc        Sun Remote Procedure Call (111)
 syslog        Syslog (514)
 tacacs        TAC Access Control System (49)
 talk          Talk (517)
 telnet        Telnet (23)
 time          Time (37)
 uucp          Unix-to-Unix Copy Program (540)
 whois         Nicname (43)
 www           World Wide Web (HTTP, 80)
```

You can either specify the number of the port or use one of the keywords listed above. Notice that in the description, the port that¡¯s actually filtered is listed. If you can¡¯t remember that Simple Mail Transfer Protocol (SMTP) uses port 25, just enter **smtp**. This can make reading long access lists a whole lot easier.

Let¡¯s take a look at a Cisco 1710 router. This router has some very defined access lists used to stop employees using certain IP addresses from accessing the Internet. You can see this in access list 101. This is a great configuration to keep handy. It has Cisco VPN service configured on it, which is apparent by the ¡°crypto¡± statements. Also used is the *Network Address Translation (NAT)* protocol, which allows everyone to leave the network using the address of 110.111.112.110. Let¡¯s take a look at this configuration:

```
NMS-Outside-RTR#show run
Building configuration¡-

Current configuration : 9401 bytes
!
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname NMS-Outside-RTR
!
no logging console
enable password routerpassword
!
username sean password 0 r3mot3
memory-size iomem 15
ip subnet-zero
!
!
!
ip audit notify log
ip audit po max-events 100
ip ssh time-out 120
ip ssh authentication-retries 3
!
crypto isakmp policy 3
 encr 3des
 authentication pre-share
 group 2
!
crypto isakmp client configuration group NMSvpn
 key r3mot3
 dns 10.1.2.2 206.13.31.12
 wins 10.1.2.1
 domain NMS.bz
 pool NMSpool
!
!
crypto ipsec transform-set NMSset esp-3des esp-sha-hmac
crypto mib ipsec flowmib history tunnel size 200
crypto mib ipsec flowmib history failure size 200
!
crypto dynamic-map NMSmap 10
 set transform-set NMSset
!
!
crypto map clientmap isakmp authorization list ƒgroupauthor
crypto map clientmap client configuration address ƒrespond
crypto map clientmap 10 ipsec-isakmp dynamic NMSmap
```

```
!
!
interface Loopback0
 ip address 192.168.1.1 255.255.255.0
!
interface Ethernet0
 ip address 110.111.112.110 255.255.255.248
 ip nat outside
 no ip route-cache
 no ip mroute-cache
 half-duplex
 crypto map clientmap
!
interface FastEthernet0
 ip address 10.1.1.2 255.255.0.0
 ip nat inside
 no ip route-cache
 ip policy route-map vpn
 no ip mroute-cache
 speed auto
!
router rip
 network 10.0.0.0
 network 110.111.112.0
!
ip local pool NMSpool 10.5.1.1 10.5.1.254
ip nat inside source route-map nonat interface ƒEthernet0 overload
ip nat inside source static 10.1.2.65 ƒ110.111.112.108
ip nat inside source static tcp 10.1.2.2 53 ƒ110.111.112.106 53 extendable
ip nat inside source static udp 10.1.2.2 53 ƒ110.111.112.106 53 extendable
ip nat inside source static 10.1.2.2 110.111.112.106
ip nat inside source static tcp 10.1.4.27 5631 ƒ110.111.112.110 5631 extendable
ip nat inside source static tcp 10.1.2.1 110 ƒ110.111.112.107 110 extendable
ip nat inside source static tcp 10.1.2.1 25 ƒ110.111.112.107 25 extendable
ip nat inside source static udp 10.1.2.2 50 ƒ110.111.112.106 50 extendable
ip nat inside source static udp 10.1.2.2 47 ƒ110.111.112.106 47 extendable
ip nat inside source static udp 10.1.2.2 6 ƒ110.111.112.106 6 extendable
ip nat inside source static udp 10.1.2.2 1723 ƒ110.111.112.106 1723 extendable
ip nat inside source static udp 10.1.2.2 1023 ƒ110.111.112.106 1023 extendable
ip nat inside source static tcp 10.1.2.2 50 ƒ110.111.112.106 50 extendable
ip nat inside source static tcp 10.1.2.2 47 ƒ110.111.112.106 47 extendable
ip nat inside source static tcp 10.1.2.2 6 ƒ110.111.112.106 6 extendable
ip nat inside source static tcp 10.1.2.2 1723 ƒ110.111.112.106 1723 extendable
ip nat inside source static tcp 10.1.2.2 1023 ƒ110.111.112.106 1023 extendable
ip nat inside source static 10.1.2.1 110.111.112.107
ip nat inside source static tcp 10.1.4.27 5632 ƒ110.111.112.110 5632 extendable
ip classless
ip route 0.0.0.0 0.0.0.0 110.111.112.105
ip route 110.111.112.106 255.255.255.255 10.1.2.2
ip route 110.111.112.107 255.255.255.255 10.1.2.1
no ip http server
ip pim bidir-enable
!
access-list 1 deny  10.1.2.2
access-list 1 permit 10.0.0.0 0.255.255.255
access-list 101 permit ip 10.3.0.0 0.0.255.255 any
access-list 101 permit ip 10.1.2.0 0.0.0.255 any
access-list 101 permit ip 10.2.2.0 0.0.0.255 any
access-list 101 permit ip 10.4.2.0 0.0.0.255 any
access-list 101 permit ip 10.5.1.0 0.0.0.255 any
access-list 101 permit tcp any any eq telnet
access-list 101 permit tcp any any eq ftp
access-list 101 permit tcp any host 10.1.2.1 eq pop3
access-list 101 permit tcp any host 10.1.2.1 eq smtp
access-list 101 deny   tcp any any eq pop3
access-list 101 deny   tcp any any eq smtp
access-list 101 permit tcp any any eq domain
access-list 101 permit udp any any eq domain
access-list 101 permit ip host 10.1.4.27 any
access-list 101 permit tcp host 10.1.4.200 any eq www
access-list 101 permit tcp host 10.1.4.201 any eq www
access-list 101 permit ip host 10.1.4.202 any
access-list 101 permit tcp host 10.1.4.203 any eq www
access-list 101 permit tcp host 10.1.4.204 any eq www
access-list 101 permit tcp host 10.1.4.205 any eq www
access-list 101 permit tcp host 10.1.4.206 any eq www
access-list 101 permit tcp host 10.1.4.207 any eq www
access-list 101 permit tcp host 10.1.4.208 any eq www
access-list 101 permit tcp host 10.1.4.209 any eq www
access-list 101 permit tcp host 10.1.4.210 any eq www
access-list 101 permit tcp host 10.1.4.211 any eq www
access-list 101 permit tcp host 10.1.4.212 any eq www
access-list 101 permit tcp host 10.1.4.213 any eq www
access-list 101 permit tcp host 10.1.4.214 any eq www
access-list 101 permit tcp host 10.1.4.215 any eq www
access-list 101 permit tcp host 10.1.4.216 any eq www
access-list 101 permit tcp host 10.1.4.217 any eq www
access-list 101 permit tcp host 10.1.4.218 any eq www
access-list 101 permit tcp host 10.1.4.219 any eq www
```

```
access-list 101 permit tcp host 10.1.4.220 any eq www
access-list 101 permit tcp host 10.1.4.221 any eq www
access-list 101 permit tcp host 10.1.4.222 any eq www
access-list 101 permit tcp host 10.1.4.223 any eq www
access-list 101 permit tcp host 10.1.4.224 any eq www
access-list 101 permit tcp host 10.1.4.225 any eq www
access-list 101 permit tcp host 10.1.4.226 any eq www
access-list 101 permit tcp host 10.1.4.227 any eq www
access-list 101 permit tcp host 10.1.4.228 any eq www
access-list 101 permit tcp host 10.1.4.229 any eq www
access-list 101 permit tcp host 10.1.4.230 any eq www
access-list 101 permit tcp host 10.1.4.231 any eq www
access-list 101 permit tcp host 10.1.4.232 any eq www
access-list 101 permit tcp host 10.1.4.233 any eq www
access-list 101 permit tcp host 10.1.4.234 any eq www
access-list 101 permit tcp host 10.1.4.235 any eq www
access-list 101 permit tcp host 10.1.4.236 any eq www
access-list 101 permit tcp host 10.1.4.237 any eq www
access-list 101 permit tcp host 10.1.4.238 any eq www
access-list 101 permit tcp host 10.1.4.239 any eq www
access-list 101 permit tcp host 10.1.4.240 any eq www
access-list 101 permit tcp host 10.1.4.241 any eq www
access-list 101 permit tcp host 10.1.4.245 any eq www
access-list 101 permit tcp host 10.1.4.246 any eq www
access-list 101 permit tcp host 10.1.4.247 any eq www
access-list 101 permit tcp host 10.1.4.248 any eq www
access-list 101 permit tcp host 10.1.4.249 any eq www
access-list 101 permit tcp host 10.1.4.250 any eq www
access-list 101 permit tcp host 10.1.4.251 any eq www
access-list 101 permit tcp host 10.1.4.252 any eq www
access-list 101 permit tcp host 10.1.4.253 any eq www
access-list 101 permit tcp host 10.2.4.200 any eq www
access-list 101 permit tcp host 10.2.4.201 any eq www
access-list 101 permit tcp host 10.2.4.202 any eq www
access-list 101 permit tcp host 10.2.4.203 any eq www
access-list 101 permit tcp host 10.2.4.204 any eq www
access-list 101 permit tcp host 10.2.4.205 any eq www
access-list 101 permit tcp host 10.2.4.206 any eq www
access-list 101 permit tcp host 10.2.4.207 any eq www
access-list 101 permit tcp host 10.2.4.208 any eq www
access-list 101 permit tcp host 10.2.4.209 any eq www
access-list 101 permit tcp host 10.2.4.210 any eq www
access-list 101 permit tcp host 10.2.4.211 any eq www
access-list 101 permit tcp host 10.2.4.212 any eq www
access-list 101 permit tcp host 10.2.4.213 any eq www
access-list 101 permit tcp host 10.2.4.214 any eq www
access-list 101 permit tcp host 10.2.4.215 any eq www
access-list 101 permit tcp host 10.2.4.216 any eq www
access-list 101 permit tcp host 10.2.4.217 any eq www
access-list 101 permit tcp host 10.2.4.218 any eq www
access-list 101 permit tcp host 10.2.4.219 any eq www
access-list 101 permit tcp host 10.2.4.220 any eq www
access-list 101 permit tcp host 10.2.4.241 any eq www
access-list 101 permit tcp host 10.2.4.245 any eq www
access-list 101 permit tcp host 10.2.4.246 any eq www
access-list 101 permit tcp host 10.2.4.247 any eq www
access-list 101 permit tcp host 10.2.4.248 any eq www
access-list 101 permit tcp host 10.2.4.249 any eq www
access-list 101 permit tcp host 10.4.4.200 any eq www
access-list 101 permit tcp host 10.4.4.201 any eq www
access-list 101 permit tcp host 10.4.4.202 any eq www
access-list 101 permit tcp host 10.4.4.230 any eq www
access-list 101 permit tcp host 10.4.4.245 any eq www
access-list 101 permit tcp host 10.4.4.246 any eq www
access-list 101 permit tcp host 10.4.4.247 any eq www
access-list 101 deny   tcp 10.0.0.0 0.255.255.255 any ƒeq www
access-list 101 permit ip any any
access-list 102 deny   ip 10.1.0.0 0.0.255.255 ƒ10.5.1.0 0.0.0.255
access-list 102 deny   ip 10.2.0.0 0.0.255.255 ƒ10.5.1.0 0.0.0.255
access-list 102 deny   ip 10.3.0.0 0.0.255.255 ƒ10.5.1.0 0.0.0.255
access-list 102 deny   ip 10.4.0.0 0.0.255.255 ƒ10.5.1.0 0.0.0.255
access-list 102 permit ip 10.1.0.0 0.0.255.255 any
access-list 102 permit ip 10.2.0.0 0.0.255.255 any
access-list 102 permit ip 10.3.0.0 0.0.255.255 any
access-list 102 permit ip 10.4.0.0 0.0.255.255 any
access-list 103 permit ip 10.1.0.0 0.0.255.255 ƒ10.5.1.0 0.0.0.255
access-list 103 permit ip 10.2.0.0 0.0.255.255 ƒ10.5.1.0 0.0.0.255
access-list 103 permit ip 10.3.0.0 0.0.255.255 ƒ10.5.1.0 0.0.0.255
access-list 103 permit ip 10.4.0.0 0.0.255.255 ƒ10.5.1.0 0.0.0.255
!
route-map vpn permit 10
 match ip address 103
 set ip next-hop 192.168.1.2
!
route-map nonat permit 10
 match ip address 102
!
!
line con 0
```

```
 exec-timeout 0 0
 password routerpassword
 login
line aux 0
line vty 0 4
 password routerpassword
 login
!
end
```

Exam Essentials

Practice setting IP extended access lists. The only way to select the right answer for access-list questions is to understand the command syntax.

Know the difference between IP standard and extended access lists. Standard access lists can filter only by source address; they cannot filter by protocol or port. Extended access lists can filter by source and destination address, protocol, and port. IP standard access lists use numbers 1¨C99; IP extended access lists use 100¨C199.

Key Term and Concept

Network Address Translation (NAT) *A* protocol run on a router whose main function allows everyone to leave the network using the same IP address. NAT uses port numbers to identify individual network conversations.

Monitor and verify selected access list operations on the router.

You need to make sure that you know how to verify IP access- list configurations and how to monitor their usage. Access lists can be quite deceiving, even for the most experienced network administrator. Although we have covered only IP access lists, you also need to have an understanding of IPX access lists and how to monitor their usage on a router. This section covers all these items.

Critical Information

Here are some specific access-list commands for monitoring and verifying the lists and descriptions of the functions they provide:

show access-list This command lists all of the access lists running on the router. It also lists each line of the access list and reports the number of packets that matched each line. This information is priceless when you are troubleshooting access lists. If you configure an access list and then use this command, you should be able to see the counter increments change as packets hit the access list. Let¡¯s look at an example of using this command on an actual production router:

```
NMS-Outside-RTR#show access-list 101
Extended IP access list 101
  permit ip 10.3.0.0 0.0.255.255 any
  permit ip 10.1.2.0 0.0.0.255 any
  permit ip 10.2.2.0 0.0.0.255 any
  permit ip 10.4.2.0 0.0.0.255 any
  permit ip 10.5.1.0 0.0.0.255 any
  permit tcp any any eq telnet
  permit tcp any any eq ftp
  permit tcp any host 10.1.2.1 eq pop3
  permit tcp any host 10.1.2.1 eq smtp
  deny tcp any any eq pop3
  deny tcp any any eq smtp
  permit tcp any any eq domain
  permit udp any any eq domain
  permit ip host 10.1.4.27 any
  permit tcp host 10.1.4.200 any eq www
  permit tcp host 10.1.4.201 any eq www
  permit ip host 10.1.4.202 any
  permit tcp host 10.1.4.203 any eq www
  permit tcp host 10.1.4.204 any eq www
  permit tcp host 10.1.4.205 any eq www
  permit tcp host 10.1.4.206 any eq www
  permit tcp host 10.1.4.207 any eq www
  permit tcp host 10.1.4.208 any eq www
  permit tcp host 10.1.4.209 any eq www
  permit tcp host 10.1.4.210 any eq www
  permit tcp host 10.1.4.211 any eq www
  permit tcp host 10.1.4.212 any eq www
  permit tcp host 10.1.4.213 any eq www
  permit tcp host 10.1.4.214 any eq www
  permit tcp host 10.1.4.215 any eq www
  permit tcp host 10.1.4.216 any eq www
  permit tcp host 10.1.4.217 any eq www
  permit tcp host 10.1.4.218 any eq www
  permit tcp host 10.1.4.219 any eq www
```

```
permit tcp host 10.1.4.220 any eq www
permit tcp host 10.1.4.221 any eq www
permit tcp host 10.1.4.222 any eq www
permit tcp host 10.1.4.223 any eq www
permit tcp host 10.1.4.224 any eq www
permit tcp host 10.1.4.225 any eq www
permit tcp host 10.1.4.226 any eq www
permit tcp host 10.1.4.227 any eq www
permit tcp host 10.1.4.228 any eq www
permit tcp host 10.1.4.229 any eq www
permit tcp host 10.1.4.230 any eq www
permit tcp host 10.1.4.231 any eq www
permit tcp host 10.1.4.232 any eq www
permit tcp host 10.1.4.233 any eq www
permit tcp host 10.1.4.234 any eq www
permit tcp host 10.1.4.235 any eq www
permit tcp host 10.1.4.236 any eq www
permit tcp host 10.1.4.237 any eq www
permit tcp host 10.1.4.238 any eq www
permit tcp host 10.1.4.239 any eq www
permit tcp host 10.1.4.240 any eq www
permit tcp host 10.1.4.241 any eq www
permit tcp host 10.1.4.245 any eq www
permit tcp host 10.1.4.246 any eq www
permit tcp host 10.1.4.247 any eq www
permit tcp host 10.1.4.248 any eq www
permit tcp host 10.1.4.249 any eq www
permit tcp host 10.1.4.250 any eq www
permit tcp host 10.1.4.251 any eq www
permit tcp host 10.1.4.252 any eq www
permit tcp host 10.1.4.253 any eq www
permit tcp host 10.2.4.200 any eq www
permit tcp host 10.2.4.201 any eq www
permit tcp host 10.2.4.202 any eq www
permit tcp host 10.2.4.203 any eq www
permit tcp host 10.2.4.204 any eq www
permit tcp host 10.2.4.205 any eq www
permit tcp host 10.2.4.206 any eq www
permit tcp host 10.2.4.207 any eq www
permit tcp host 10.2.4.208 any eq www
permit tcp host 10.2.4.209 any eq www
permit tcp host 10.2.4.210 any eq www
permit tcp host 10.2.4.211 any eq www
permit tcp host 10.2.4.212 any eq www
permit tcp host 10.2.4.213 any eq www
permit tcp host 10.2.4.214 any eq www
permit tcp host 10.2.4.215 any eq www
permit tcp host 10.2.4.216 any eq www
permit tcp host 10.2.4.217 any eq www
permit tcp host 10.2.4.218 any eq www
permit tcp host 10.2.4.219 any eq www
permit tcp host 10.2.4.220 any eq www
permit tcp host 10.2.4.241 any eq www
permit tcp host 10.2.4.245 any eq www
permit tcp host 10.2.4.246 any eq www
permit tcp host 10.2.4.247 any eq www
permit tcp host 10.2.4.248 any eq www
permit tcp host 10.2.4.249 any eq www
```

```
  permit tcp host 10.4.4.200 any eq www
  permit tcp host 10.4.4.201 any eq www
  permit tcp host 10.4.4.202 any eq www
  permit tcp host 10.4.4.230 any eq www
  permit tcp host 10.4.4.245 any eq www
  permit tcp host 10.4.4.246 any eq www
  permit tcp host 10.4.4.247 any eq www
  deny tcp 10.0.0.0 0.255.255.255 any eq www
  permit ip any any
NMS-Outside-RTR#
```

show ip access-list This command shows you only the IP access lists, whereas the `show access-list` command displays all lists. Now let¡¯s look at an actual output from a 1710 router. Values displayed in parentheses, such as `(777 matches)`, indicate how many times the access list found a match. Let¡¯s take a look:

```
NMS-Outside-RTR#show ip access-list
Standard IP access list 1
  deny  10.1.2.2 (60049 matches) check=4483
  permit 10.0.0.0, wildcard bits 0.255.255.255 ƒ(6603979 matches) check=495590
Extended IP access list 102
  deny ip 10.1.0.0 0.0.255.255 10.5.1.0 0.0.0.255 ƒ(8 matches)
  deny ip 10.2.0.0 0.0.255.255 10.5.1.0 0.0.0.255
  deny ip 10.3.0.0 0.0.255.255 10.5.1.0 0.0.0.255
  deny ip 10.4.0.0 0.0.255.255 10.5.1.0 0.0.0.255
  permit ip 10.1.0.0 0.0.255.255 any (37337 matches)
  permit ip 10.2.0.0 0.0.255.255 any (3879 matches)
  permit ip 10.3.0.0 0.0.255.255 any (946 matches)
  permit ip 10.4.0.0 0.0.255.255 any (3107 matches)
Extended IP access list 103
  permit ip 10.1.0.0 0.0.255.255 10.5.1.0 ƒ0.0.0.255 (777 matches)
  permit ip 10.2.0.0 0.0.255.255 10.5.1.0 ƒ0.0.0.255 (120 matches)
  permit ip 10.3.0.0 0.0.255.255 10.5.1.0 ƒ0.0.0.255 (35 matches)
  permit ip 10.4.0.0 0.0.255.255 10.5.1.0 ƒ0.0.0.255 (21 matches)
NMS-Outside-RTR#
```

show log If you add this log syntax at the end of your extended access list, a log will be generated with the following information:

Access-list number

Source address

Source port

Destination address

Destination port

Number of packets

All of this log information could be redirected to the syslog server and stored for security purposes.

clear access-list counter This command clears the counters for the `show access-list` commands.

Tip You can use the `show ip interfaces` and the `show run` commands to see which interfaces have IP access lists set.

IPX Access Lists

This section covers the IPX access-list commands featured in the CCNA exam. It is important that you pay close attention to the fine details of the output that a command provides. In this section, you will learn how IPX access lists are used to control IPX traffic. We discuss IPX standard access lists, IPX extended access lists, and IPX SAP filters.

You should have a basic understanding of how access lists are created and how they are applied to an interface.

IPX Standard Access Lists

IPX standard access lists allow or deny packets based on source and destination IPX addresses. With IP standard access lists, you can use only a source IP address. The syntax for each line of an IPX standard access list is as follows:

```
access-list [number] [permit or deny] [source] f[destination]
```

The second argument is a list number. This tells the router what type of access list is being used. Below is an example of the types of access lists that can be used:

```
RouterA(config)#access-list ?
 <1-99>       IP standard access list
 <100-199>    IP extended access list
 <1000-1099>  IPX SAP access list
 <1100-1199>  Extended 48-bit MAC address access list
 <1200-1299>  IPX summary address access list
 <200-299>    Protocol type-code access list
 <300-399>    DECnet access list
 <600-699>    Appletalk access list
 <700-799>    48-bit MAC address access list
 <800-899>   IPX standard access list
 <900-999>   IPX extended access list
```

Notice that IPX standard access lists use any number from 800 to 899.

IPX Extended Access Lists

IPX standard access lists filter only on source or destination access lists. IPX extended access lists can filter based on any of the following:

- Source network/node
- Destination network/node
- IPX protocol (SAP, SPX, etc.)
- IPX socket

Extended access lists are in the range 900¨C999 and are configured just like standard access lists, with the addition of protocol and socket information. Here¡¯s a template for building lines in an IPX extended access list:

```
access-list [number] [permit or deny] [protocol] f[source] [socket] [destination] [socket]
```

When you move from standard into extended access lists, you¡¯re simply adding the ability to filter based on protocol, socket (or port, for IP), and destination node/network.

Configuring an IPX Standard Access List

To configure IPX standard access lists, use the same commands as IP standard access lists, but with list numbers 800¨C899 in the configur- ation (instead of the numbers 1¨C99 for IP lists). Here is an example:

```
RouterA#config t
RouterA(config)#access-list 810 permit 30 10
RouterA(config)#access-list 810 deny 50 10
RouterA(config)#int e0
RouterA(config-if)#ipx access-group 810 out
RouterA(config-if)#^Z
RouterA#
```

The number 810 corresponds to the range 800¨C899, which is reserved for IPX standard access lists. The `permit/deny` parameter is the same as it is with IP packets. Here, the specified source and destination addresses are based on IPX network addresses. No wildcard masking is required to specify an entire IPX network¡ªjust list the network address, and you¡¯re done!

Configuring an IPX Extended Access List

Use the online help to wade through the syntax of creating an IPX extended access list.

```
RouterA(config)#access-list ?
 <1-99>      IP standard access list
 <100-199>   IP extended access list
 <1000-1099> IPX SAP access list
 <1100-1199> Extended 48-bit MAC address access list
 <1200-1299> IPX summary address access list
 <200-299>   Protocol type-code access list
 <300-399>   DECnet access list
 <600-699>   Appletalk access list
 <700-799>   48-bit MAC address access list
 <800-899>   IPX standard access list
 <900-999>   IPX extended access list

RouterA(config)#access-list 910 ?
 deny  Specify packets to reject
 permit Specify packets to permit

RouterA(config)#access-list 910 permit ?
 ¨C1    Any IPX protocol type
 <0-255> Protocol type number (DECIMAL)
 <cr>

RouterA(config)#access-list 910 permit -1 ?
 ¨C1      Any IPX net
 <0-FFFFFFFF> Source net
 N.H.H.H      Source net.host address
 <cr>

RouterA(config)#access-list 910 permit -1 -1 ?
 <0-FFFFFFFF> Source Socket (0 for all sockets) ƒHEXIDECIMAL
 <cr>

RouterA(config)#access-list 910 permit -1 ¨C1 0 ?
 ¨C1      Any IPX net
 <0-FFFFFFFF> Destination net
 N.H.H.H    Destination net.host address
 <cr>
RouterA(config)#access-list 910 permit -1 ¨C1 0 ¨C1 ?
```

```
 <0-FFFFFFFF> Destination Socket (0 for all sockets) ƒHEXIDECIMAL
 <cr>
RouterA(config)#access-list 910 permit -1 ¨C1 0 ¨C1 0 log
```

The `log` command can be used to log any attempts from, say, network 50 to access network 10, and record the following information:

- Source address
- Source socket
- Destination address
- Destination socket
- Protocol type

IPX SAP Filters

IPX SAP filters are implemented using the same tools discussed above. They have an important place in controlling IPX SAP traffic. Why is this important? Because if you can control the SAPs, you can control the access to IPX devices. Access lists in the 1000¨C1099 range are used to specify IPX SAP filters. Here¡¯s the template for each line of an IPX SAP filter:

```
access-list [number] [permit or deny] [source] ƒ[service type]
```

Now let¡¯s practice creating an IPX SAP filter. Assume that on your Admin LAN network, you have three NetWare servers, but you want only the one with internal IPX network address 11.0000.0000.0001 to be seen by the outside world. To accomplish that, you¡¯d configure and apply an access list as follows:

```
RouterA#config t
RouterA(config)#access-list 1010 permit ƒ11.0000.0000.0001 0
RouterA(config)#int e0
RouterA(config-if)#ipx input-sap-filter 1010
RouterA(config-if)#^Z
RouterA#
```

Here¡¯s how the above `access-list` command maps to the template:

Access List	Number	Permit or Deny	Source	Service Type
access-list	1010	permit	11.0000.0000.0001	0

The number 1010 falls into the range 1000¨C1099, reserved for IPX SAP filters. The source network is the network/node address of the server. The resulting access list allows packets from 11.0000.0000.0001 to enter the Ethernet interface and be included in SAP updates across the network. As with other access lists, there¡¯s an implicit `deny any` that blocks all other SAP updates arriving at the router on the Ethernet interface. Finally, the 0 entered for service type indicates that all services should be allowed:

```
RouterA#config t
RouterA(config)#access-list 1010 permit ƒ11.0000.0000.0001 ?
 <0-FFFF> Service type-code (0 matches all services)
 N.H.H.H  Source net.host mask
\<cr>
```

To add the IPX SAP filter to an interface, use one of the following commands:

```
RouterA(config-if)#ipx input-sap-filter 1010
```

or

```
RouterA(config-if)#ipx output-sap-filter 1010
```

Applying an IPX Access List to an Interface

After you build an access list, it won¡¯t do anything until you apply it to an interface. You do this with the `ipx access-group` command. Your only options are to choose whether the access list will filter on incoming or outgoing packets. Here is an example:

```
config t
int s0
ipx access-group 110 out
```

Exam Essentials

Know the commands to view access lists. You must remember the commands for viewing access lists set on both global configurations and interfaces.

Know the difference between IPX standard and extended access lists. Standard access lists can filter only by source address; they cannot filter by protocol or port. Extended access lists can filter by source and destination address, protocol, and port. IPX standard access lists use 800¨C899; and IPX extended access lists use 900¨C999.

Know the difference between the types of IPX access lists. It is important to understand what each type of list can filter on.

Remember how to apply an IPX list to an interface. By using the `ipx access-group` command, you can apply access lists to an interface.

Key Terms and Concepts

access list Used in routers to filter IP and IPX packets either trying to enter or leave an interface.

extended access list Security used in Cisco routers that can filter by source and destination address. It can filter by network address or by protocol and port.

standard access list Security used in Cisco routers that can filter only by source address.

Chapter 7: LAN Design

Cisco Certified Network Associate Exam Objectives Covered in This Chapter:

- Describe full- and half-duplex Ethernet operation.*(pages 196¡ª206)*
- Describe network congestion problem in Ethernet networks.*(pages 206¡ª208)*
- Describe the features and benefits of Fast Ethernet.*(pages 209¡ª211)*
- Describe the guidelines and distance limitations of Fast Ethernet.*(pages 211¡ª213)*

This chapter covers the Ethernet standard for LANs using 10Mbps Ethernet as well as Fast Ethernet. It reviews the most common congestion problems, cabling limitations, and the benefits of upgrading to faster Ethernet solutions.

Describe full- and half-duplex Ethernet operation.

In order for you to get an adequate understanding of Ethernet duplexing, you need to understand how Ethernet works at the Physical layer. This section helps familiarize you with Ethernet and its many layers, its addressing, and its protocols.

Critical Information

Ethernet is a contention media access method that allows all hosts on a network to share the same bandwidth of a link. Ethernet is popular because it is easy to implement, easy to troubleshoot, and easy to add new technologies (like Fast Ethernet and Gigabit Ethernet) to existing network infrastructures. Ethernet uses the Data Link and Physical layer specifications, and this section of the book will give you both the Data Link¨C and Physical-layer information you need to effectively implement, troubleshoot, and maintain an Ethernet network.

Ethernet networking uses a protocol called *Carrier Sense Multiple Access with Collision Detection (CSMA/CD)*, which helps devices share bandwidth evenly without having two devices transmit at the same time on the network media.

CSMA/CD was created to overcome the problem of collisions that occur when packets are transmitted simultaneously from different nodes. Good collision management is important, because when a node transmits in a CSMA/CD network, all the other nodes on the network receive and examine that transmission. Only bridges and routers effectively prevent a transmission from propagating through the entire network.

The CSMA/CD protocol works like this: When a host wants to transmit over the network, it first checks for the presence of a digital signal on the wire. If all is clear (if no other host is transmitting), the host will then proceed with its transmission. And it doesn¡¯t stop there. The transmitting host constantly monitors the wire to make sure no other hosts begin transmitting. If the host detects another signal on the wire, it sends out an extended jam signal that causes all nodes on the segment to stop sending data. Other nodes respond to that jam signal by waiting a bit before attempting to transmit again. If collisions keep occurring after 15 tries, the nodes attempting to transmit will then time out.

Ethernet at the Data Link Layer

Ethernet at the Data Link layer is responsible for Ethernet addressing, which is typically called hardware addressing or MAC (Media Access Control) addressing. Ethernet is also responsible for framing packets received from the Network layer and preparing them for transmission on the local network through the Ethernet contention media access method. There are four different types of Ethernet frames available, and we will discuss all four in later sections.

Ethernet Addressing

Ethernet addressing uses the Media Access Control (MAC) address burned into each and every Ethernet network interface card (NIC). The MAC address, sometimes referred to as a hardware address, is a 48-bit address written in a canonical format to ensure that addresses are at least written in the same format, even if different LAN techno- logies are used.

Figure 7.1 shows the 48-bit MAC address and how the bits are divided.

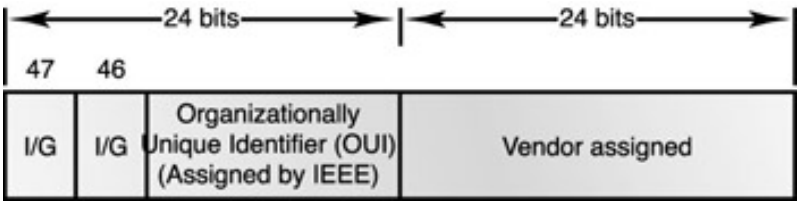

Figure 7.1: Ethernet addressing using MAC addresses

The IEEE assigns an organizationally unique identifier (OUI) to an organization (24 bits, or three bytes). That organization, in turn, assigns a globally administered address (24 bits, or three bytes) that is unique (supposedly) to each and every adapter they manufacture. Notice bit 46. Bit 46 must be 0 if it is a globally assigned bit from the manufacturer, and it must be 1 if it is locally administered from the

network administrator.

Address Resolution Protocol

Address Resolution Protocol (ARP) is used by the IP to provide dynamic mapping of 32-bit IP addresses to 48-bit MAC addresses. The ARP cache is a table of these listings and is checked every time communication is initiated between machines in an IP network. If the required hardware address cannot be found in the cache, a broadcast is sent out to resolve it. The broadcast address of (FFFFFFFF) is already stored, but is not visible in the table. If the router receives a reply to an ARP broadcast, the previously unknown address is entered in the cache. The next time the IP address needs to be resolved to an IP address, no broadcast will be necessary. Every listing in the cache has a timestamp and a TTL (time to live). When this time expires, the entry is deleted from the table to make room for new address resolutions. Should the cache become full and no TTLs have expired yet, then the oldest entry or entries are purged.

Ethernet Frames

The Data Link layer is responsible for combining bits into bytes and bytes into frames. A *frame* is used at the Data Link layer to encapsulate *packets.* Packets are data from upper OSI layers that are encapsulated with layer 3 information. These packets are handed down from the Network layer for transmission on a type of media access. There are three types of media-access methods: contention (Ethernet), token passing (Token Ring and FDDI), and polling (IBM Mainframes and 100VG-Anylan). The CCNA exam covers primar- ily Ethernet (contention) media access.

The function of Ethernet stations is to pass data frames between each other by using a group of bits known as a MAC frame format. This provides error detection from a cyclic redundancy check (CRC). However, remember that this is error detection, not error correction. The 802.3 and Ethernet frames are shown in Figure 7.2.

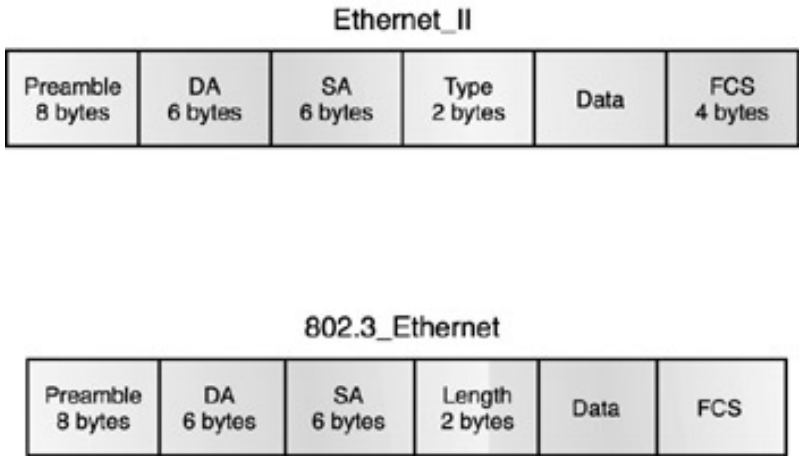

Figure 7.2: 802.3 and Ethernet frame formats

These are the fields in the 802.3 and Ethernet frame types:

Preamble An alternating 1,0 pattern provides a 5MHz clock at the start of each packet, which allows the receiving devices to lock the incoming bit stream. Uses either a Start Frame Delimiter (SFD) or Synch field to indicate to the receiving station that the data portion of the message will follow. The SFD field alternates 1,0,1,0,1,0, etc., and the Synch field is all 1s. The preamble and SFD/Synch field are 64 bits long.

Destination Address (DA) Transmits a 48-bit value using the least significant bit first. Used by each receiving station to determine whether an incoming packet is addressed to its particular node. The destination address can be an individual address, a broadcast, or a multicast MAC address. Remember that a broadcast is all 1s, or Fs, in hex and is sent to all devices, where a multicast is sent only to a similar subset of nodes on a network.

Source Address (SA) 48-bit MAC address supplied by the transmitting device. It uses the least significant bit first. Broadcast and multicast address formats are illegal within the Source Address field.

Length or Type 802.3 uses a Length field, where the Ethernet frames uses a Type field, to identify the Network-layer protocol. 802.3 cannot identify the upper-layer protocol and must be used with a proprietary LAN (for example, IPX).

Data Packet sent down to the Data Link layer from the Network layer; 46 to 1500 bytes.

Frame Check Sequence (FCS) A field at the end of the frame, used to store the CRC.

Let¡¯s take a look at some frames caught on our trusty Etherpeek network analyzer. The frame below has only three fields¡ªDestination, Source, and Type:

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

This is an Ethernet_II frame. Notice the Type field is IP, or 08-00 in hexadecimal.

The next frame has the same fields, so it must also be an Ethernet_II frame. We put this one in so you could see that the frame can carry more than just IP. It can also carry IPX, or 81-37h.

```
Destination:  ff:ff:ff:ff:ff:ff Ethernet Broadcast
Source:       02:07:01:22:de:a4
Protocol Type:81-37 NetWare
```

Notice that this frame was a broadcast: You can tell because the destination hardware address is all 1s in binary, or all Fs in hexadecimal.

Notice the length field in the next frame:

```
Flags:        0x80  802.3
Status:       0x00
Packet Length:64
Timestamp:    12:45:45.192000 06/26/1998
Destination:  ff:ff:ff:ff:ff:ff Ethernet Broadcast
Source:       08:00:11:07:57:28
Length:       34
```

This must be an 802.3 frame. What protocol is this going to be handed to? It doesn¡¯t say in the frame, so it must be IPX. Why? Because when Novell created the 802.3 frame type (before the IEEE did, and the IEEE called it 802.3 Raw), Novell was pretty much the only LAN server out there. So, Novell assumed that if you¡¯re running a LAN, it must be IPX.

802.2 and SNAP

Remember that the 802.3 Ethernet frame cannot identify the upper- layer (Network) protocol by itself. It needs help. The IEEE defined the 802.2 LLC specifications to provide this function and more. Figure 7.3 shows the IEEE 802.3 with LLC (802.2) and the Sub-Network Access Protocol (SNAP) frame types. This illustration shows how the LLC header information is added to the data portion of the frame.

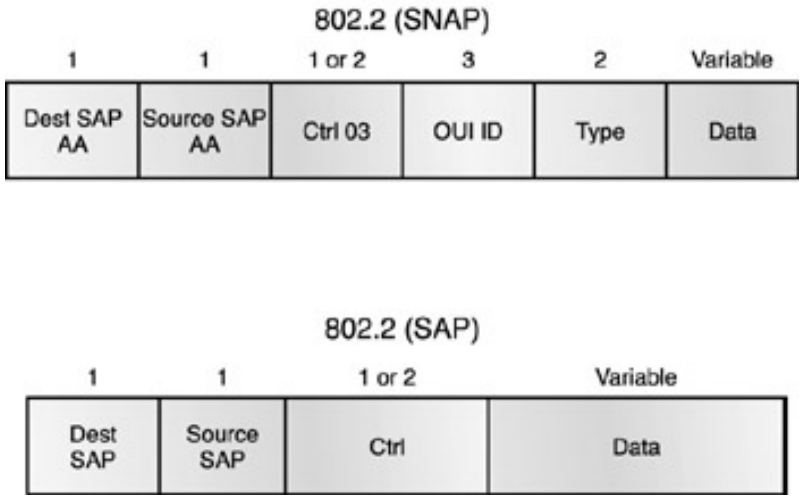

Figure 7.3: 802.2 and SNAP frame types

Now, let¡¯s take a look at an 802.2 frame and SNAP captured from our analyzer.

802.2 Frame

The following is an 802.2 frame captured with a protocol analyzer:

```
 Flags:        0x80 802.3
 Status:       0x02 Truncated
 Packet Length:64
 Slice Length: 51
 Timestamp:    12:42:00.592000 03/26/1998
 Destination:  ff:ff:ff:ff:ff:ff Ethernet Broadcast
 Source:       00:80:c7:a8:f0:3d
 LLC Length:   37
 Dest. SAP:    0xe0 NetWare
 Source SAP:   0xe0 NetWare Individual LLC
 ƒSublayer Management Function
 Command:      0x03 Unnumbered Information
```

Notice the first frame has a length field, so it¡¯s probably an 802.3, right? But look again¡ªit also has a DSAP and a SSAP, so it has to be an 802.2 frame. (Remember that an 802.2 frame is an 802.3 frame with the LLC information in the data field of the header, so we know what the upper-layer protocol is.)

SNAP Frame

The SNAP frame has its own Protocol field to identify the upper-layer protocol. This is really a way to allow an Ethernet_II frame to be used in an 802.3 frame. Even though the following network trace shows a protocol field, it is really an Ethernet_II type (Ether-Type) field. Here is a SNAP frame:

```
Flags:         0x80 802.3
 Status:       0x00
 Packet Length:78
 Timestamp:  09:32:48.264000 01/04/2000
802.3 Header
 Destination: 09:00:07:FF:FF:FF AT Ph 2 Broadcast
 Source:      00:00:86:10:C1:6F
 LLC Length:  60
802.2 Logical Link Control (LLC) Header
 Dest. SAP:   0xAA SNAP
 Source SAP:  0xAA SNAP
 Command:     0x03 Unnumbered Information
 Protocol:    0x080007809B AppleTalk
```

You can identify a SNAP frame, because the DSAP and SSAP fields are always AA, plus the command field is always 3. The reason this frame type was created is because not all protocols worked well with the 802.3 Ethernet frame that didn¡¯t have an Ether-Type field. To allow the proprietary protocols created by application developers to be used in the LLC frame, the IEEE then defined the SNAP format. It is not used that often, and it is mostly seen with AppleTalk and proprietary frames. Cisco uses a SNAP frame with their proprietary protocol CDP.

Ethernet at the Physical Layer

In a shared-hub Ethernet environment, if one station sends a frame, then all devices must synchronize to the digital signal being transmitted and extract the frame from the wire. All devices that use the same physical media and listen to each frame are considered to be in the same collision domain. This means that only one device can transmit at any given time, and any other device on the network segment must synchronize with the signal and extract the frame. If two stations try to transmit at the same time, a collision will occur. In 1984, the IEEE Ethernet committee released the CSMA/CD protocol. This basically tells all stations to constantly be listening for any other device trying to transmit at the same time they are, and to stop and wait for a predetermined time if they do sense a collision.

Ethernet uses a bus topology, which means that whenever a device transmits, the signal must run from one end of the segment to the other. Ethernet also defined baseband technology, which means that when a station does transmit, it will use the entire bandwidth on the wire and will not share it.

Full-duplex Ethernet uses point-to-point connections and 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 circuits and receive circuits between the nodes.

If you have a full-duplex 10Mbps Ethernet operating bidirectionally on the same switch port, theoretically you can have aggregate throughput of 20Mbps. Full-duplex can now be used in 10BaseT, 100BaseT, and 100BaseFL media, but only if all the other network devices (NICs, for example) can support full-duplex transmission.

Full-Duplex Ethernet Design

Full-duplex Ethernet switch technology provides a point-to-point connection between the transmitter of the transmitting station and the receiver of the receiving station. With half-duplex circuitry, a standard Ethernet can usually provide only 50 to 60 percent of the bandwidth available. In contrast, full-duplex Ethernets can provide a full 100 percent, because they can transmit and receive simultaneously and because collisions don¡¯t occur.

In order to run a full-duplex Ethernet, you must have the following:

- Two 10Mbps or 100Mbps paths
- Full-duplex NICs
- Loopback and collision detection disabled
- Software drivers supporting two simultaneous data paths
- Adherence to Ethernet distance standards

Half-Duplex Ethernet Design

Half-duplex Ethernet has been around a long time. Ethernet_II came out in 1984 and is still the most popular of all LAN topologies. When a station is sending to another station, the transmitting circuitry is active at the transmitting station, and the receiving circuitry is active at the receiving station. This circuitry uses a single cable similar to a narrow, one-way bridge.

Exam Essentials

Remember what is needed to run full-duplex. You do not have to know the distance requirements for this objective, but it is important to understand the rest of the configuration requirements for running full-duplex.

Understand the definitions of half- and full-duplex. Half-duplex uses a single cable similar to a narrow, one-way bridge. Full-duplex provides a point-to-point connection between the transmitter of the sending station and the receiver of the destination station. Full-duplex uses two cables¡ªone to send and one to receive¡ªso there should never be data collisions.

Key Terms and Concepts

Address Resolution Protocol (ARP) Used to gain a hardware address from an IP address.

Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Protocol designed to run with Ethernet networks. It helps nodes communicate on a physical medium.

Ethernet Contention media access method.

frame A piece of data formatted with OSI Reference Model layer 2 specifications. Layer 2 is also defined as the Data Link layer, which is used to transmit packets over a LAN.

full-duplex Provides a point-to-point connection between the transmitter of the sending station and the receiver of the destination station.

half-duplex Uses a single cable similar to a narrow, one-way bridge. It uses a single line to send and receive.

packet Defined at the Network layer of the OSI Reference Model and used to route user data to remote networks.

CCNA: Cisco Certified Network Associate Exam Notes, Third Edition

by Todd Lammle and Sean Odom

Sybex ?2002

Printer friendly format ?

Describe network congestion problem in Ethernet networks.

Many of today¡¯s networks have implemented technologies such as switching to deal with growth in the network. As networks get bigger using the old-fashioned technologies utilizing bridges and hubs, the networks slow down because of the amount of data traffic and broadcasts. In this section, you¡¯ll learn about how too many devices and broadcasts in a non-switched network can affect how a network performs. A *broadcast* is a message destined for more than one host on the network. It can be sent to a multicast address for groups, a subnet, or even an entire network.

Critical Information

A flat network topology is a LAN connected by bridges and hubs. Every node in the network sees the data being passed by every other node on the network. This arrangement eats up an incredible amount of processing power and bandwidth, even without collisions forcing data to be re-sent on the physical wire. A flat network topology begins to slow down due to traffic, collisions, and other bottlenecks. As a network administrator, you should have the resources to adequately determine the types of data that are flowing throughout your network. You should have a good network Sniffer, or other such device, to find over-utilization problems as well as faulty equipment and unnecessary protocols running on the network.

Of the layer 3 protocols, TCP/IP is the most popular because it is less chatty than the other common layer 3 protocols, Internetwork Packet Exchange (IPX) and AppleTalk. Most network administrators agree that if you have bandwidth to kill, you can add IPX and AppleTalk, which like to scream ¡°I'm here on the network!¡± quite frequently¡ª thereby eating up bandwidth. A few devices on the network don¡¯t use too much bandwidth; but as the number of network nodes increases, so does the number of broadcasts required to identify the nodes running those protocols on the network.

The processors in each node handle the task of reading each packet to determine if the packet received is for itself or some other device. This takes away from the processing power needed for other tasks and applications, causing a slowdown that the users discover and complain about. Many network administrators pass off this slowness as a problem with the PCs, and the most vital PCs are rebuilt, upgraded or replaced. Of course, upgrading or replacing PCs with faster processors can alleviate the slowness; however, the administrators have no idea that there are other solutions to this problem.

Administrators can upgrade to Fast Ethernet, Gigabit Ethernet, or a switched network instead of hubs. Many administrators who don¡¯t know about switching and its benefits implement different wiring solutions such as fiber optic with its high costs of cabling and installation labor. This is usually because of a salesman who convinced them that fiber is better. And it is in some situations, such as in large factories that deal with electrical equipment, but fiber is very expensive and usually unjustified.

The most cost-effective solution is to upgrade to switches. Doing so confines your collision domains so only the interfaces are attached to the switches¡¯ ports, and you can segment your broadcast domains to as many as you would like by implementing VLANs (as discussed in Chapter 1 ¡°Bridging/Switching¡±). When companies finally decide to upgrade to a switched network, they can typically do so over a weekend by simply replacing the hubs they have. When the network users leave on Friday, their high-powered Pentiums stacked with RAM have the speed of 386s. When they return Monday morning, nothing is more exciting than hearing comments all over the office about how their computers boot up more quickly and run so much faster, and how they like the faster network. But did the users *get* a faster network? In one sense, the network did get an upgrade; but this upgrade merely eliminated the problems of a flat topology network by segmenting the network into smaller collision and broadcast domains.

Sometimes, if you have a 10BaseT network with Category 3 or 4 cabling, the best solution is to fix the immediate problems by upgrading to Category 5 or 6 cabling and implementing a Fast Ethernet network in conjunction with installing switches. However, most network users do not need more than true 10Mbps from the Access-layer switches to their desktops even if they are using high-bandwidth applications. After all, before they had switches, the users were getting along with only 3 or 4Mbps on their 10Mbps link, due to broadcasts, collisions, and network utilization.

Exam Essentials

Remember the causes of congestion. The main problem of congestion is too much traffic, caused by too much data being transmitted, too many broadcasts, and too many collisions.

Remember the benefits of switches and VLANs. Hubs can use only half-duplex on each attached interface, making way for multiple collisions. Switches allow for full-duplex between the transmitter of the sending interfaces. This is because it uses two cables¡ªone to send and one to receive¡ªso there should never be data collisions. A switch makes each port its own collision domain. VLANs allow you to segregate certain ports into their own broadcast domains.

Key Term and Concept

broadcast A frame or packet destined for all hosts on a group, segment, or network.

Describe the features and benefits of Fast Ethernet.

Having a fundamental understanding of Fast Ethernet is useful for administrators working in a production environment. When you take the CCNA exam, this knowledge will help you answer questions regarding other exam objectives, although there may not be any questions pertaining specifically to Fast Ethernet. This section covers how Cisco views the features and benefits of Fast Ethernet.

Critical Information

In 1995, the IEEE approved the IEEE 802.3U, the 100BaseT Fast Ethernet standard. It defines the Physical and Data Link layers, uses the CSMA/CD protocol, and is 10 times faster than 10BaseT. These are some of the new technology stars:

100BaseFX Ethernet over fiber at 100Mbps using 802.3 specs. It uses two-strand¨C, 50/125¨C, or 62.5/125¨Cmicron multimode fiber optic cable.

100BaseT4 Using 802.3 specs, 100BaseT4 carries 100Mbps over Category 3, 4, or 5 UTP cabling with a standard RJ-45 connector. 100BaseT4 uses all eight wires on a RJ-45 connector.

100BaseTX Fast Ethernet over Category 5 UTP cabling. It¡¯s compatible with, and adheres to, 802.3 specifications. It can also use two- pair, 100-ohm shielded twisted-pair (STP) cable or Type 1 STP cable.

100BaseX Refers to either the 100BaseTX or 100BaseFX media. This standard was approved to ensure compatibility between the Ethernet CSMA/CD and the ANSI X3T9.5 standard.

100VG-AnyLAN An IEEE movement into Fast Ethernet and Token Ring that doesn¡¯t appear to be taking off, mostly because it¡¯s not compatible with the 802.3 standards¡ªand Cisco doesn¡¯t support it.

Migrating or upgrading your network to 100BaseT from 10BaseT can substantially improve throughput and overall performance. Because 100BaseT uses the same signaling techniques as 10BaseT, a gradual migration to 100BaseT doesn¡¯t have to be expensive or time- consuming. Partially converting a LAN is a viable alternative to converting all clients simultaneously. These are some of the advantages of 100BaseT over 10BaseT:

- 100BaseT has 10 times the performance of 10BaseT.
- Existing cabling and network equipment can be used.
- It can use 10Mbps and 100Mbps simultaneously on the same network.
- 100BaseT uses CSMA/CD technology.
- Migration is easy.

100BaseT networks use the same ¡°time slots¡± as 10BaseT networks. What are time slots? They require a station to transmit all its bits before another station can transmit its packet. For 100BaseT networks to transmit in the same time slots, the distance must be reduced. This means that instead of the 5-4-3 rule that the standard Ethernet uses (five network segments, four repeaters, only three segments populated), you can use only two Class II repeaters in a 100BaseT network. A *repeater* is a device that merely amplifies the signal it receives. The timing in Fast Ethernet is shorter (10 percent of Ethernet). The maximum frame size, or time slot, is 1518 bytes. The physical distance is reduced because both Fast and regular Ethernet specifications state that the roundtrip time must not exceed 512 bit times. Since Fast Ethernet transmits faster, a signal of 512 bits covers a shorter distance.

Exam Essential

Remember the advantages of Fast Ethernet. It¡¯s much faster than 10BaseT, is easy to migrate, and uses CSMA/CD.

Key Term and Concept

repeater Physical device used to amplify and extend the distance of a digital signal.

Describe the guidelines and distance limitations of Fast Ethernet.

Although some of this was covered in the first section, we need to cover it again to make sure that you understand it. This section discusses the distance limitations of the different types of cabling as well as the guidelines for using Ethernet and Fast Ethernet.

Critical Information

Half-duplex Ethernet has been around a long time. Ethernet_II came out in 1984 and is still the most popular of all LAN topologies. When a station is sending to another station, the transmitting circuitry is active at the transmitting station, and the receiving circuitry is active at the receiving station. This circuitry uses a single cable similar to a narrow, one-way bridge.

Full-duplex Ethernet switch technology, which we have discussed throughout this chapter, provides a point-to-point connection between the transmitter of the transmitting station and the receiver of the receiving station. With half-duplex circuitry, standard Ethernets can usually provide only 50 to 60 percent of the bandwidth available. In contrast, full-duplex Ethernets can provide a full 100 percent, because they can transmit and receive simultaneously, and because collisions don¡¯t occur.

In order to run a full-duplex Ethernet, you must have the following:

- Two 10Mbps or 100Mbps paths
- Full-duplex NICs
- Loopback and collision detection disabled
- Software drivers supporting two simultaneous data paths
- Adherence to Ethernet distance standards

Understanding the difference between the different media access speeds that Ethernet provides is important. The Electronic Industries Association and the newer Telecommunications Industry Association (EIA/TIA) are the standards bodies that create the Physical-layer specifications for Ethernet. The EIA/TIA specifies that Ethernet use a registered jack connector with a 45 wiring sequence (RJ-45) on unshielded twisted-pair (UTP) cabling. The following points outline the different Ethernet media requirements for Gigabit Ethernet:

- 1000BaseCX: Copper shielded twisted-pair that can run only up to 25 meters before losing signal strength
- 1000BaseT: Category 5 or 6 cable, using four-pair UTP wiring, up to 100 meters
- 1000BaseSX: Multimode fiber using 62.5- and 50-micron core, uses a 780-nanometer laser, up to 260 meters
- 1000BaseLX: Single-mode fiber that uses a nine-micron core, 1300-nanometer laser, up to 10 kilometers

Exam Essentials

Remember the distance of 1000BaseSX. This is multimode fiber using 62.5- and 50-micron core; it uses a 780-nanometer laser and can go up to 260 meters.

Remember what is needed to use Fast Ethernet. You should know all that is required to run full-duplex Ethernet. You need to have two 10Mbps or 100Mbps paths, two full-duplex compatible NICs, loopback disabled, collision detection disabled, the correct software drivers that support two simultaneous data paths, and an adherence to Ethernet distance standards.

Remember the distance limitation for Cat 5 cabling. The distance limitation for Category 5 cabling is 100 meters, or approximately 300 feet.

Key Terms and Concepts

1000BaseCX Copper shielded twisted-pair that can run only up to 25 meters.

1000BaseT Category 5 or 6, using four-pair UTP wiring, which can run up to 100 meters.

1000BaseSX Multimode fiber using either 62.5- or 50-micron cores. This cable uses a 780-nanometer laser and can go up to 260 meters before losing signal strength.

1000BaseLX Single-mode fiber using a nine-micron core, a 1300-nanometer laser, and can go up to 10 kilometers before losing signal strength.

Chapter 8: Cisco Basics, IOS, and Network Basics

Cisco Certified Network Associate Exam Objectives Covered in This Chapter:

- Examine router elements.*(pages 216¡ª218)*
- Manage configuration files from the privileged EXEC mode.*(pages 219¡ª223)*
- Control router passwords, identification, and banner.*(pages 224¡ª229)*
- Identify the main Cisco IOS software commands for router startup.*(pages 229¡ª229)*
- Log in to a router in both user and privileged modes.*(pages 229¡ª232)*
- Check an initial configuration using the setup command.*(pages 232¡ª236)*
- Use the context-sensitive help facility.*(pages 236¡ª238)*
- Use the command history and editing features.*(pages 238¡ª240)*
- List the commands to load Cisco IOS software from: Flash memory, a TFTP server, or ROM.*(pages 240¡ª246)*
- Prepare to backup, upgrade, and load a backup Cisco IOS software image.*(pages 246¡ª249)*
- List problems that each routing type encounters when dealing with topology changes, and describe techniques to reduce the number of these problems.*(pages 249¡ª254)*
- Prepare the initial configuration of your router and enable IP.*(pages 254¡ª254)*

This chapter starts with the basics: how to log in to a router, and the two different modes that a router provides. Then you¡¯ll learn how to use the question mark to access help when using Cisco commands. The command history and editing features are talked about in detail, as are the different types of memory a Cisco router uses.

After that, we cover what happens when a router boots up, which files it uses to boot, and how to view and copy these files. One of the most useful topics we discuss is how to set your router passwords, banners, and identification.

Cisco routers can be configured manually or with a setup routine. We go through both methods in this chapter. Also, you will learn how to copy and restore a Cisco IOS.

This chapter ends by covering the problems of different routing protocols, routing type issues, and techniques to reduce these problems.

Examine router elements.

The router¡¯s elements refer to the main components of the Cisco Internetwork Operating System (IOS). In this objective, we introduce you to the router¡¯s NVRAM and the router¡¯s flash, which holds the IOS and the primary commands used in the router¡¯s configuration. You will see these commands many times in these objectives.

Critical Information

The *flash* memory holds the router¡¯s IOS. You can see the IOS currently stored in flash with the `show flash` command (or `show flash`), which displays your flash memory and reveals both the size of your files and the amount of free flash memory. Here is an example:

```
Router#sh flash

System flash directory:
File Length  Name/status
 1  3612396 igs-i-l.110-16
[3612460 bytes used, 4776148 available, 8388608 total]
8192K bytes of processor board System flash (Read ONLY)
```

Cisco has new commands to help administrators manage configuration files from privileged EXEC mode. Table 8.1 is a list of the commands used to start and save configurations on Cisco routers.

Table 8.1: Router Configuration

Command	Purpose
`show startup-config`	Shows the configuration that will be loaded when the router boots.
`show running-config`	Shows the configuration that¡¯s currently loaded into RAM and running.
`copy running-config startup-config`	Copies the configuration stored in running RAM to backup or NVRAM.
`copy startup-config running-config`	Copies the configuration stored in NVRAM to running RAM.
`erase startup-config`	Erases the configuration in the router¡¯s NVRAM and lands it right back into the initial configuration dialog. (Don¡¯t try this one at work!)
`reload`	Reboots the router and reloads the startup configuration into memory.
`setup`	Starts the initial configuration dialog.

Note The commands in Table 8.1 are covered in detail in the next objective.

One of the things you should notice when running these commands is that none of them is run from configuration mode (`config terminal`); all are run from the privileged-mode prompt (`Router#`).

Two other parts of the router can store and run a configuration: the NVRAM and the RAM, which are covered throughout this chapter.

Exam Essentials

Know the primary router configuration commands. You should know in detail all of the primary configuration commands found in Table 8.1. These are covered in detail throughout this chapter.

Know the function of the flash. The flash stores the Cisco IOS, which is the software that runs on the router.

Key Term and Concept

flash An erasable, reprogrammable ROM that holds the operating system (OS) image and microcode. It allows you to ¡°flash¡± the router and perform upgrades without removing and replacing chips on the motherboard. Flash is retained even when the router is turned off.

Manage configuration files from the privileged EXEC mode.

Managing the configuration files stored in *random access memory (RAM)* and in *nonvolatile RAM (NVRAM)* is somewhat easy if you understand the commands and what each does. In this objective, we explain where the configuration is stored as well as the commands to change and modify the configurations that are stored.

Critical Information

The configuration files stored in the different types of memory are defined below:

- `startup-config`
- `running-config`

startup-config

The startup configuration file (`startup-config`) is held in NVRAM. When the router is started, the file is accessed and placed into DRAM (sometimes just referred to as RAM). Type **show startup-config** (or **sh startup-config**, for short) to see the configuration, as in this example:

```
RouterB#show startup-config
Using 661 out of 32762 bytes
!
version 11.0
service udp-small-servers
service tcp-small-servers
!
hostname RouterB
!
enable secret 5 $1$jMYk$21eDXo8XXwrBiVm5RR9wN.
enable password password
!
!
interface Ethernet0
 ip address 172.16.30.1 255.255.255.0
!
interface Serial0
 ip address 172.16.20.2 255.255.255.0
 no fair-queue
 clockrate 56000
!
interface Serial1
 ip address 172.16.40.1 255.255.255.0
 clockrate 56000
```

running-config

The running configuration file (`running-config`) is the configuration from NVRAM placed in RAM at startup. By typing **config terminal** (**config t** will also work), you open the file for updating; any changes you make will amend the `running-config` file. When you¡¯re happy with the new configuration, copy it to `startup-config`, as shown here:

```
Router#copy running-config startup-config
Building configuration¡-
[OK]
```

You can also view the `running-config` file at any time by typing **show running-config**. However, you do not have to type in the full commands. You can abbreviate commands, as long as they are unique. For example, to carry out the command `show running-config`, you can type simply **sh run**. For `show startup-config`, you can type **sh start**. For `copy running-config startup-config`, you can type **copy run start**. See the next section for more on these commands.

Configuration Commands Used to View and Modify Configuration Files

This section explains the following commands to view and make changes to the running and startup configurations:

- `show startup-config`
- show running-config
- copy running-config startup-config
- copy startup-config running-config
- erase startup-config
- reload
- setup

show startup-config

Below is the output of the command `sh start` (short for `show startup-config`) when no configuration has been saved to NVRAM:

```
Router#show start
%% Non-volatile configuration memory has not been ƒset up or has bad checksum
```

show running-config

This command shows you the router configuration that is currently loaded in RAM and running. If you type **config t**, you will be changing this file. The output below was cut for brevity.

```
Router#show run
Building configuration¡-

Current configuration:
!
version 11.2
```

copy running-config startup-config

This command copies the `running-config` file into NVRAM or `startup-config`. This completely erases the existing `startup-config` file and replaces it with the `running-config` file. Here is an example:

```
Router#copy run start
Building configuration¡-
[OK]
```

copy startup-config running-config

This command is used to copy the configuration from NVRAM into running RAM. You can use this if you changed your configuration but had problems with the new setup. Note that this command just appends anything in the `startup-config` that is not in the `running- config`¡ªit doesn¡¯t overwrite anything. Here¡¯s an example:

```
Router#copy startup-config running-config
Building configuration¡-
[OK]
```

erase startup-config

This command is used to erase the configuration in NVRAM:

```
Router#erase startup-config
[OK]
```

If you used the command `show startup-config` after erasing the NVRAM configuration, you would get an error message, as shown earlier in this chapter. You also would be put into setup mode when you rebooted your router.

reload

This command reboots the router. Take a look at this example:

```
Router#reload
Proceed with reload?[Enter]
```

setup

This command puts you into setup mode regardless of what your configuration is set at, as seen here:

```
Router#setup

     --- System Configuration Dialog ---

At any point you may enter a question mark '?' forhelp.
Use ctrl-c to abort configuration dialog at any prompt.
Default settings are in square brackets '[]'.
Continue with configuration dialog? [yes/no]:
```

Exam Essential

Remember the commands to view or change the router¡¯s configuration files. Practice using the many `show`, `copy`, `erase`, and `reload` commands to change and view the router¡¯s configuration files.

Key Terms and Concepts

nonvolatile RAM (NVRAM) Memory that stores the router¡¯s start- up configuration file. NVRAM retains its information even when the router is rebooted or shut down.

random access memory (RAM) Provides caching and packet buffering, plus information like routing tables. RAM is used to hold the running OS when the router is powered on; it is cleared when the router is reset or powered off.

Control router passwords, identification, and banner.

This objective covers the five different password types, how to configure them, how to place router identifiers such as the router¡¯s hostname, and how to configure a banner.

Critical Information

There are five different types of *passwords* used in securing Cisco routers: enable secret, enable, virtual terminal (VTY), auxiliary, and console. These are their functions:

Enable Secret Password This is a one-way cryptographic secret password used in versions 10.3 and up. It takes precedence over the enable password. You can configure it when setting up your router or at any time after that.

Enable Password This is used when there is no enable secret password, and when you are using older software and some boot images. The administrator manually encrypts it. You can define this within setup mode or anytime after that.

Virtual Terminal (VTY) Password This is used for Telnet sessions to the router. You can change the VTY password at any time, but it must be specified or you won¡¯t be able to telnet to the router. You can specify this type of password during setup or anytime after that.

Auxiliary Password This is used for the auxiliary port, which is used to connect a modem to a router for remote console connections. This must be set up manually.

Console Password This is used for the console port, and sets up a password for anyone who connects directly to your router¡¯s console port. It must be set up manually.

MOTD Banner

The MOTD (message of the day) *banner*, configured with the `banner motd` command, is the first message displayed when any user connects to the router.

Router Identification

A router¡¯s identifying information consists of two things: its hostname and its interface. You can set an interface description by using the `description` command.

Hostname

You can change the *hostname* your router displays by using the `hostname` command. For example, to change the name of a router to RouterC, you would type **hostname RouterC**.

Necessary Procedures

You need to practice some commands. This section reviews the processes for setting passwords, the MOTD banner, and the hostname, and for setting the identification of an interface using the `description` command.

Setting Passwords

The following examples show how to set Cisco router passwords. Of course, you should choose your own passwords in place of the ones used in the examples.

Enable Secret Password

To set the enable secret password, type the following commands:

```
Router#config t
Enter configuration commands, one per line. End ƒwith CNTL/Z.
Router(config)#enable secret sean
Router(config)#^Z
```

Enable Password

To set the enable password, type the following commands:

```
Router#config t
Enter configuration commands, one per line. End with ƒCNTL/Z.
Router(config)#enable password sean
The enable password you have chosen is the same as your ƒenable secret.
This is not recommended. Re-enter the enable password.
Router(config)#enable password sean
Router(config)#^Z
```

Notice that if you type the same password as the enable secret password, you get a warning message. If, despite the warning, you choose the same password again, the router would accept it¡ªbut neither the secret nor the enable password would work. Can you say

¡°password recovery¡±?

Virtual Terminal (VTY) Password

To set your VTY password, type the following commands:

```
Router#config t
Enter configuration commands, one per line. End ƒwith CNTL/Z.
Router(config)#line vty 0 4
Router(config-line)#login
Router(config-line)#password sean1
Router(config-line)#^Z
```

The command `line vty 0 4` specifies the number of Telnet sessions allowed in the router. You can also set up a different password for each line by typing **line vty *port number***. The `login` command tells the router to prompt for a password. If no `login` command is used, users can gain access via the VTY port without being prompted for a password.

Auxiliary Password

To set the auxiliary password, use the following commands:

```
Router#config t
Enter configuration commands, one per line. End ƒwith CNTL/Z.
Router(config)#line aux 0
Router(config-line)#login
Router(config-line)#password sean2
Router(config-line)#^Z
```

Console Password

Finally, to set the console password, use these commands:

```
Router#config t
Enter configuration commands, one per line. End ƒwith CNTL/Z.
Router(config)#line con 0
Router(config-line)#login
Router(config-line)#password sean3
Router(config-line)#^Z
```

Configuring Banners

You can add a MOTD banner that is displayed whenever anyone logs in to your Cisco router. The command is `banner motd` *`delimiter`*. You must start the banner with a delimiting character of your choice. Here¡¯s an example using the octothorp (#) as a delimiter:

```
RouterC(config)#banner motd #
Enter TEXT message. End with the character '#'.
If you are not authorized to be in Acme's router, ƒlog out immediately! Violators will be prosecuted!
#[Enter]
RouterC(config)#end
```

The output for this example will look like this when users either telnet to the router or connect to a console port:

```
Router con0 is now available

Press ENTER to get started.

If you are not authorized to be in Acme.com router, ƒlog out immediately!

User Access Verification
Password:
```

This output shows an example of what you¡¯d see when connecting to your router¡¯s console port. It tells you that the router is available, and then to press Enter to get started. You will see the MOTD banner and then be asked for the user-mode password, if one is configured.

Changing Router Identification

You can change the name your router displays by using the `hostname` command. For example, to change the name of a router to RouterC, type the following commands:

```
Router#config t
Enter configuration commands, one per line. End ƒwith CNTL/Z.
Router(config)#hostname RouterC
RouterC(config-line)#^Z
```

Notice that there is no space in the command `hostname`.

Exam Essentials

Remember how to set your passwords. Make sure you know the difference between enable, enable secret, virtual terminal (VTY), console, and auxiliary passwords.

Know how to configure a MOTD banner. Practice setting banners, and notice where they show up when you log in to the router.

Key Terms and Concepts

banner Text that is displayed prior to logging in to a router.

hostname The name used to identify a router. This name appears only on local management and troubleshooting interfaces.

password An identifier, text, or code used to protect assets, essential data, and operating systems from unauthorized use.

Identify the main Cisco IOS software commands for router startup.

For information on this objective, please see the ¡°List the commands to load Cisco IOS software from: Flash memory, a TFTP server, or ROM¡± objective, later in this chapter.

Log in to a router in both user and privileged modes.

In this objective, you learn to log in to a router in both user EXEC mode and privileged EXEC mode. Before you can log in to the router, you need to know how to connect to the router and configure Hyperterminal to begin using the router.

Critical Information

You can connect to a router and log in by attaching a console cable to the console port of the router. The other end of the console cable should be connected to a PC or terminal. If you are using a PC, you must use a terminal emulation program such as Hyperterminal. When using Hyperterminal, set the following options:

Setting	Option
Bits Per Second	9600
Data Bits	8
Parity	None
Stop Bits	1
Flow Control	None

Once this is done, press Enter to continue.

If a user-mode password is configured on the console line, you must enter this password before gaining access to user mode. If no password is assigned, you will be greeted with a `Router>` prompt. The > prompt indicates that you are in user mode. Here is an example:

```
Bob con0 is now available
Press RETURN to get started.
User Access Verification
Password:
Bob>
```

First, you log in to user mode, and then you can change to privileged mode. It is important to remember how to log in to both modes and to know the different commands that can be run in each.

Cisco routers are configured from the user interface, which you can run either from the console port on the router or by telnetting to the router from another host through any router interface. You can also connect a modem to the auxiliary port and dial into the router for console access.

The EXEC Command Interpreter

Cisco IOS software has a command interpreter called the *EXEC*. The EXEC interprets the command you type and then executes the operation you¡¯ve commanded. (You have to log in to the router before an EXEC command can be entered.)

The EXEC has two levels of access: user and privileged. These two levels, sometimes referred to as modes, serve as security for access into the different levels of commands.

User mode is for ordinary tasks like checking a router¡¯s status, connecting to remote devices, making temporary changes to terminal settings, and viewing basic system information. But in this mode, your view of the router¡¯s configuration and your troubleshooting capabilities are very limited.

Privileged mode is used to change the configuration of the router. (From here, you can access the configuration mode using the `config terminal` command.) The commands in privileged mode include all those in user mode plus those used to set OS parameters, get detailed information on a router¡¯s status, test and run debug operations, and access global configuration modes.

Very few procedures are involved in logging in, but they are important to know both when you configure a Cisco router and when you take the CCNA exam.

Once you are in user mode, you can enter privileged mode by typing **enable** and then providing the password when prompted. Type **disable** to return to user mode, as in this example (note that the password does not appear on the screen):

```
SeansRouter>enable
Password:
SeansRouter#disable
SeansRouter>
```

Exam Essentials

Know the difference between user and privileged modes. You cannot see the router configuration in user mode. You can both view and change the router configuration in privileged mode.

Remember how to log in to a router in both modes. When you connect a console cable to a router, you are prompted with this message: `Press Return to continue`. At this point, you must enter a user-mode password if one is assigned. You can then type **enable** to enter privileged mode. You will be prompted for a password if one is assigned.

Key Terms and Concepts

EXEC Cisco IOS software command interpreter.

privileged mode Used to view and change the configuration of the router.

user mode Used for ordinary tasks like checking the router¡¯s status.

Check an initial configuration using the setup command.

This section looks at a router with a clean configuration. First we walk through and erase the `startup-config` file stored in NVRAM. After that, we look at the default configuration of a router.

Critical Information

If you use the `write erase` or `erase startup-config` commands and then either reload your router or power it off and on, you¡¯ll see the system configuration dialog screen. You can also type **setup** within privileged mode to get the screen at any time, which can be helpful in configuring your router.

The `setup` command can be useful, but you won¡¯t necessarily use it in a production environment. It may prompt you for commands that you don¡¯t use in your internetwork, which can be tedious. When going through this section, notice the difference between configuring your router using the initial setup and the `setup` command, including which management prompts you are using.

If you erase the `startup-config` file and reboot your router, you will see the following upon bootup:

```
Notice: NVRAM invalid, possibly due to write erase.
     --- 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 '[]'.
Would you like to enter the initial configuration ƒdialog? [yes][Enter]
```

Press Enter at the `[yes]` prompt to continue with the configuration and see how the router responds:

```
First, would you like to see the current interface ƒsummary? [yes][Enter]

Any interface listed with OK? value "NO" does not have a ƒvalid configuration
Interface  IP-Address OK? Method  Status Protocol
Ethernet0  unassigned NO  not set up   down
Serial0   unassigned NO  not set up   down
Serial1   unassigned NO  not set up   down
Configuring global parameters:
```

By pressing Enter at the `[yes]` prompt to view the current interface summary, you¡¯re assured that the power-on self-test (POST) has found all the interfaces.

In this case, you have two serial ports and one Ethernet port. They aren¡¯t okay (see the `NO not set` next to them?), because they aren¡¯t set up yet. They¡¯re designated as `unassigned`. The router now wants the name of the router you¡¯re trying to configure, which is RouterA in this example. Type that now and then press Enter. The router responds with this dialog (we¡¯ll show the passwords from here on, but remember that they won¡¯t be seen on-screen):

```
Enter hostname [Router]:RouterA
The enable secret is a one-way cryptographic secret ƒused instead of the enable password when it exists.
Enter enable secret:sean
The enable password is used when there is no enable ƒsecret and when using older software and some boot ƒimages.
Enter enable password:seanx
 Enter virtual terminal password:seanvty
 Configure SNMP Network Management? [yes]:n
 Configure IP? [yes][Enter]
Configure IP? [yes][Enter]
  Configure IGRP routing? [yes]:n
  Configure RIP routing? [no]:[Enter]

Configuring interface parameters:

Configuring interface Ethernet0:
 Is this interface in use? [yes][Enter]
 Configure IP on this interface? [yes][Enter]
  IP address for this interface:172.16.10.1
  Number of bits in subnet field [0]:8
  Class B network is 172.16.0.0, 8 subnet bits;
  ƒmask is 255.255.255.0

Configuring interface Serial0:
 Is this interface in use? [yes]:[Enter]
 Configure IP on this interface? [yes]:[Enter]
 Configure IP unnumbered on this interface?
```

```
 ƒ[no]:[Enter]
  IP address for this interface:172.16.20.1
  Number of bits in subnet field [8]:[Enter]
  Class B network is 172.16.0.0, 8 subnet bits;
  ƒmask is 255.255.255.0

Configuring interface Serial1:
 Is this interface in use? [yes]:n
```

Notice that we had you reply no to the routing commands like RIP and IGRP. Also notice that for the subnet mask, you were to enter 8 for the number of bits. The router doesn¡¯t count the default masks in the number of bits, so even though you set the number of bits to 8, the subnet mask will still be realized as 255.255.255.0. The third byte is the only one used for subnetting.

After you answer no to configuring Serial1, the router shows the configuration it created. It then asks whether you want to save the configuration:

```
Use this configuration? [yes/no]:y
```

Type **y** for yes, and then press Enter. The router saves the configuration to nonvolatile RAM (which is explained later in this chapter).

Exam Essential

Know how to use the *setup* command and the information that needs to be entered into the router to complete the setup. There are two ways of using the setup feature. You can start with a default configuration, and the setup feature will start automatically. Alternatively, you can use the `setup` command from the privileged EXEC prompt.

Key Term and Concept

setup The command used to configure a Cisco router¡¯s configuration through a step-by-step process.

Use the context-sensitive help facility.

Some of the commands used to configure and administer a Cisco router can be hard to remember. By using the context-sensitive help facility, you can get either the next possible command or a list of commands that start with a certain letter.

Critical Information

You can access a help screen for any command by typing a question mark (**?**) after the command. This will give you a list of the commands available. You can then choose the next command in the command string and type a question mark again to get the next command, and so on until you have the complete command string.

For example, if you need to set the clock on your router but don¡¯t know what the commands are, you could type **clock ?**. You must leave one space between the command `clock` (or another command) and the question mark, or your query won¡¯t work. In this example, the next command is `set;` you would type **clock set** and then a space and a question mark to get the next command, and so on until you have the complete command string.

Suppose you need to know all the commands that start with *cl* because you can¡¯t remember the command you need. You can type **cl?** to see all the commands that start with *cl*. Notice that there is no space between the letters and the question mark. This tells the EXEC to give you all the commands that start with *cl*.

To master the help features Cisco provides, you need to practice using question-mark commands on a Cisco router. The following example shows how to set the router time using the help screens. Notice the difference between typing **clock ?** and **cl?**:

```
Router#cl?
clear clock
Router#clock ?
set Set the time and date
```

Notice the space between `clock` and `?`. You could also type **clo ?**.

Look at the last line of the previous example. This tells you the next command is `set` and that this command is used to set the date and time. This form of help is called *context-sensitive help*, or command syntax help, because it tells you which keywords or arguments are required to continue with a command.

Next, type **clock set ?**, as follows:

```
Router#clock set ?
 hh:mm:ss Current Time (hh:mm:ss)
```

Doing this has given you even more information on how to set the clock. Now type **clock set 10:29:30 ?**, like this:

```
Router#clock set 10:29:30 ?
 <1-31> Day of the month
 MONTH  Month of the year
```

The router responds by giving you a message that it wants information about the day and month. So type in more information, as in this example:

```
RouterB#clock set 10:29:30 23 5
                  ^
% Invalid input detected at '^' marker
```

Notice that if you type a number (5, in this case) instead of the name of the month (May), you receive a `% Invalid input` message. The router is very clear about what it considers invalid input¡ªit includes a caret symbol (^) to indicate where the error is in the command.

To continue, type **clock set 10:29:30 23 May ?**, as seen here:

```
Router#clock set 10:29:30 23 May ?
 <1993-2035> Year
```

Okay, the router accepted `May` and now wants you to specify the year. So, to finish this command, type **clock set 10:29:30 23 May 2002**.

Exam Essential

Know the different ways to use the question mark. There are two different ways to use the question mark to gain help when administrating your router. You can type it without a space, as in **cl?**, to get all the commands that start with *cl*. Another option is to type a space before the question mark, as in **clock ?**, to get the next argument or command available.

Key Term and Concept

context-sensitive help This form of help is also called command syntax help, because it tells you which keywords or arguments are required to continue with a command.

Use the command history and editing features.

The user interface comes with an *advanced editing* feature that aids in typing repetitive commands. This feature helps administrators configure routers efficiently. The command history and editing features do not change the configuration in any way; their only purpose is to make things easier for the administrator.

Critical Information

First of all, you can turn off the advanced editing feature at any time with the `terminal no editing` command; you can reenable them with the `terminal editing` command.

Using the advanced editing feature is completely up to the administrator configuring the router. None of the advanced editing feature commands is mandatory in any configuration¡ªunless you are taking the CCNA exam, of course!

Table 8.2 describes the different commands used to edit and review the command history.

Table 8.2: Router-Command History

Command	Purpose
Ctrl+A	Move to the beginning of the command line
Ctrl+E	Move to the end of the command line
Ctrl+F (or right arrow)	Move forward one character
Ctrl+B (or left arrow)	Move back one character
Ctrl+P (or up arrow)	Repeat previous command
Ctrl+N (or down arrow)	Repeat most recent command
Esc+B	Move backward one word
Esc+F	Move forward one word
`Router>show history`	Show command buffer
`Router>terminal history size`	Set command buffer size
`Router>terminal no editing`	Disable advanced editing
`Router>terminal editing`	Reenable advanced editing

Another helpful editing feature is Tab, which completes an entry for you. For example, you could type **show running-config** and then press Tab:

```
Router#show run[Tab]
Router#show running-config
```

The router finishes typing in `show running-config` for you. Remember to use Tab for those long commands.

Exam Essential

Remember the commands for editing and viewing the command history. Know how to use using the commands listed in Table 8.2 before taking the exam. In other words, practice!

Key Term and Concept

advanced editing Cisco¡¯s way of creating shortcuts. These key combinations are mostly old Unix commands.

List the commands to load Cisco IOS software from: Flash memory, a TFTP server, or ROM.

In this section, you will learn the commands to load the Cisco IOS from flash memory, a TFTP server, and *read-only memory (ROM)*. First we look at what each of these configuration storage methods are, and then we review the commands you need to know.

Critical Information

These are the different types of memory used in a Cisco router:

ROM Used by the router to store the bootstrap startup program, OS software, and POST. ROM chips are installed in sockets on the router¡¯s motherboard so that they can be replaced or upgraded. The IOS included in the ROM is a scaled-down, and usually older, version.

Flash Basically, an erasable, reprogrammable ROM that holds the OS image and microcode. It allows you to ¡°flash¡± the router and perform upgrades without removing and replacing chips on the motherboard. Flash is retained even when the router is turned off.

RAM Provides caching and packet buffering, plus information like routing tables. RAM is used to hold the running OS when the router is powered on; it is cleared when the router is reset or powered off.

Nonvolatile RAM (NVRAM) Stores the router¡¯s startup configuration file. NVRAM retains its information even when the router is rebooted or shut down.

In order to understand how each of these memory types is used in on a Cisco router, let¡¯s take a look at the boot sequence of the router and how to manage the registers that adjust how the router boots.

The Router Boot Sequence

When a router boots up, it performs a series of steps, called the boot sequence, to test the hardware and load the necessary software. The boot sequence consists of the following steps:

1. The router performs a POST, which tests the hardware to verify that all of the device¡¯s components are operational and present. For example, the POST checks for the different interfaces on the router. The POST is stored in and run from ROM.

2. The bootstrap, a program in ROM that is used to execute programs, looks for and loads the Cisco IOS software. By default, the IOS software is loaded from flash memory in all Cisco routers.

3. The IOS software looks for a valid configuration file stored in NVRAM. This file is called `startup-config` and is there only if an administrator copies the `running-config` file into NVRAM.

4. If a `startup-config` file is in NVRAM, the router will load and run it. The router is now operational. If a `startup-config` file is not in NVRAM, the router will start the setup mode configuration upon bootup.

Managing Configuration Registers

All Cisco routers have a 16-bit software register, which is written into NVRAM. By default, the configuration register is set to load the Cisco IOS from flash memory and to look for and load the `startup- config` file from NVRAM.

Understanding the Configuration Register Bits

The 16 bits of the configuration register are read from 15 to 0, from left to right. The default configuration setting on Cisco routers is 0x2102. The 0x means that the digits that follow are in hexadecimal.

Let¡¯s take a look at the boot field configuration register settings that you need to know for the exam:

0x2100 Boots the router in ROM monitor mode. You must manually boot the router with the b command.

The router will show the `rommon>` prompt.

0x2101 Boots the router from a boot image stored in ROM. The router will show the `router(boot)>` prompt.

0x2102 through 210F Instructs the router to use the boot commands specified in NVRAM. This is the default boot filename.

0x2142 Instructs the router to ignore the configuration stored in NVRAM. This allows you to bypass configured passwords if the password is lost.

Viewing the Current Boot Configuration Register

You can see the current value of the configuration register by using the `show version` command, as in the following example:

```
SeansRouter#show version
Cisco Internetwork Operating System Software
IOS (tm) C2600 Software (C2600-I-M), Version 12.0(3)T3,
RELEASE SOFTWARE (fc1)
[output cut]
Configuration register is 0x2102
```

Changing the Configuration Register

You can change the configuration register with the `config-register` command. For example, the following commands tell the router to boot from ROM monitor mode and then show the current configur- ation register value:

```
SeansRouter(config)#config-register 0x2101
Router(config)#^Z
Router#show version
[cut]
Configuration register is 0x2102 (will be 0x2101
ƒat next reload)
```

Notice that the `show version` command shows the current configur- ation register value, as well as what it will be when the router reboots. Any change to the configuration register will not take effect until the router is reloaded.

Using *copy tftp flash*

You can copy from a TFTP server to flash anytime by typing **copy tftp flash**. This command is very useful for downloading new versions of the Cisco IOS to your router. Here¡¯s an example:

```
RouterC#copy tftp flash
          **** NOTICE ****
Flash load helper v1.0
This process will accept the copy options and then ƒterminate the
current system image to use the ROM ƒbased image for the copy.
Routing functionality will not be available during ƒthat time.
If you are logged in via telnet, this connection ƒwill terminate.
Users with console access can see the results of the ƒcopy operation.
          ---- ******** ----
Proceed? [confirm][Enter]

System flash directory:
File Length  Name/status
 1  3621884 igs-i-l.110-18.bin
[3621948 bytes used, 572356 available, 4194304 ƒtotal]
Address or name of remote host [172.16.10.1]?[Enter]
Source file name?igs-i-l.110-18.bin
Destination file name [igs-i-l.110-18.bin]?[Enter]
Accessing file 'igs-i-l.110-18.bin' on ƒ172.16.10.2¡-
Loading igs-i-l.110-18.bin from 172.16.10.2 (via ƒSerial0): ! [OK]

Erase flash device before writing? [confirm][Enter]
Flash contains files. Are you sure you want to ƒerase? [confirm][Enter]

Copy 'igs-i-l.110-18.bin' from server
 as 'igs-i-l.110-18.bin' into Flash WITH erase? ƒ[yes/no]y
```

```
%SYS-5-RELOAD: Reload requested
%FLH: igs-i-l.110-18.bin from 172.16.10.2 to flash ¡-
System flash directory:
File Length  Name/status
 1  3621884 igs-i-l.110-18.bin
[3621948 bytes used, 572356 available, 4194304 ƒtotal]
Accessing file 'igs-i-l.110-18.bin' on ƒ172.16.10.2¡-
Loading igs-i-l.110-18.bin from 172.16.10.2 (via ƒSerial0): ! [OK]
Erasing device¡- eeeeeeeeeeeeeeee ¡-erased
Loading igs-i-l.110-18.bin from 172.16.10.2 (via ƒSerial0): !!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!! !!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!! !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
! !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!! !!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!! !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!! !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!! !!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!! !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!! !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!! !!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!! !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!! !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!! !
!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 3621884/4194304 bytes]

Verifying checksum¡- OK (0xC248)
Flash copy took 0:21:34 [hh:mm:ss]
%FLH: Re-booting system after download
```

After confirming a few entries, you¡¯re asked if it¡¯s okay to erase the entire contents of flash memory. The program asks this because there¡¯s rarely room for more than one flash file. However, if there is room, you can have many different versions loaded in flash.

Each e in the output stands for *erase*, and each exclamation point (`!`) indicates that one UDP segment has been successfully transferred. The router must be rebooted to load the new image on a 2500 series router, because the currently running IOS image is in flash memory. Use `show flash` to verify that the size matches that of the original file.

Exam Essential

Remember the boot configuration register settings you need to know for the exam. You must remember the boot configuration register settings for 0x2100, 0x2101, 0x2102, and 0x2142.

Key Term and Concept

read-only memory (ROM) Used by the router to store the bootstrap startup program, operating system software, and power-on self-test (POST). ROM chips are installed in sockets on the router¡¯s motherboard so that they can be replaced or upgraded.

Prepare to back up, upgrade, and load a backup Cisco IOS software image.

As an administrator¡ªand to pass the CCNA exam¡ªyou need to know how to back up configuration files in places other than NVRAM. Whenever you are going to make a configuration change, it is good practice to copy the original configuration first to a *Trivial File Transfer Protocol (TFTP)* host before making any changes.

Critical Information

Earlier in this chapter, we reviewed how to use the `copy startup- config running-config` and `copy running-config startup-config` commands. Those commands are used for manipulating and copying configuration files, which is the focus of this section.

However, since those commands were demonstrated previously, here we talk only about copying and manipulating configuration files between Cisco routers and a TFTP host and back again. There are a couple ways of doing this. The first command is `config net`. This is used to copy a configuration from a TFTP host into running RAM. You cannot use this command to copy the configuration into NVRAM.

The second command for copying a configuration file is simply `copy`. You can use this a few different ways. First, you can use it to copy a configuration file from a TFTP host into running RAM. Second, you can use it to copy files from a TFTP host into NVRAM. These commands are `copy tftp run` and `copy tftp start`, respectively.

You can also use the `copy` command to copy the configuration from either `running-config` or `startup-config` to a TFTP host by using the commands `copy run tftp` or `copy start tftp`.

Using *config net*

The `config net` command is not as useful in production networks as the `copy tftp run` command (discussed below). Basically, all `config net` does is copy a configuration file stored on a TFTP host into running RAM. When using `config net`, you must supply the IP address or hostname of the network TFTP host. Here is an example:

```
Router#config net
Host or network configuration file [host]?[Enter]
Address of remote host [255.255.255.255]?172.16.10.1
Name of configuration file [router-confg]?RouterA-confg
Configure using RouterA-confg from 172.16.10.1? ƒ[confirm][Enter]
Loading RouterA-confg
```

Using *copy run tftp*

You can copy the router¡¯s current configuration from a router to a TFTP server by typing **copy running-config tftp**. Doing this gives you a backup of the router configuration and allows you to run the configuration from this server. You can also configure the router by making your changes to the configuration file stored on the TFTP server; when you¡¯re happy with the new configuration, copy the file to the router with the `copy tftp running-config` command (the short form is `copy run tftp`). Take a look at this example:

```
RouterC#copy run tftp
Remote host []?172.16.10.1
Name of configuration file to write [routerc- ƒconfg]?[Enter]
Write file routerc-confg on host 172.16.10.1? ƒ[confirm][Enter]
Building configuration¡-
OK
```

By default, Cisco adds ¨Cconfg to the end of the router¡¯s hostname to create a default filename. When configuring an IOS device from a TFTP server, the device¡¯s default method is to try to load a file with the name of the device followed by the string ¨Cconfg.

Using *copy tftp run*

To copy a configuration from a TFTP host to a router, use the `copy tftp run` or `copy tftp start` commands, as seen here:

```
Router#copy tftp run
Host or network configuration file [host]?[Enter]
Address of remote host [255.255.255.255]?172.16.10.1
Name of configuration file []? detroit-confg[Enter]
Configure using detroit-confg from 172.16.10.1? ƒ[confirm][Enter]
Loading detroit-confg ..from 172.16.10.1 (via ƒEthernet0): !
[OK - 717/32723 bytes]
Detroit#
```

Notice in this example that the hostname of the router changed immediately after the configuration file was loaded. This happened because the configuration file was loaded directly into DRAM. You would need to use a `copy run start` command at this point.

Exam Essentials

Know how to copy a configuration file from a TFTP host. The commands to copy a configuration file from a TFTP host to a router are `config net`, `copy tftp run`, and `copy tftp start`.

Know how to copy a configuration file to a TFTP host. The commands to copy a configuration file from a router to a TFTP host are `copy run tftp` and `copy start tftp`.

Practice copying a Cisco IOS to a TFTP server and back again. You need to understand the output of backing up and restoring a Cisco IOS. The only way to do this is to practice, looking closely at the output of the commands.

Key Term and Concept

Trivial File Transfer Protocol (TFTP) A conceptually stripped- down version of File Transfer Protocol (FTP) that has no browsing capabilities. TFTP can be used only to send and receive files.

List problems that each routing type encounters when dealing with topology changes, and describe techniques to reduce the number of these problems.

Interior gateway protocols (IGPs) are used to dynamically configure routers in an autonomous system (AS). Examples of IGPs are Routing Information Protocol (RIP), Cisco¡¯s Interior Gateway Routing Protocol (IGRP), and Enhanced Interior Gateway Routing Protocol (EIGRP). Exterior gateway protocols (EGPs) are used to communicate between IGPs; one example is Border Gateway Protocol (BGP).

The three IGPs discussed in this book are RIP, IGRP, and EIGRP. To pass the CCNA exam, you must know the protocols discussed in this objective.

Before we can see the problems each routing type encounters, we must have a good understanding of routing and the three *routing protocols*. Let¡¯s first take a look at routing and then the problems with each of the routing protocols. We will also look at static routes, and other techniques that can be used to resolve routing issues or can serve as alternatives to routing protocols.

Warning RIP, IGRP, and EIGRP are only briefly covered in this book. You should obtain the *CCNA Study Guide*, 3rd ed. (Sybex, 2002) or the *CCNP: Routing Study Guide* (Sybex, 2001) for a more in-depth look at these protocols.

Critical Information

Note Please refer to Chapter 4, ¡°Routing,¡± for information on basic, dynamic, and RIP routing.

As discussed earlier in this book, dynamic routing is the process of using protocols to find and update routing tables on routers. Using protocols to do the work of mapping the network is easier than static or default routing, but it¡¯s not always accurate. Let¡¯s review some of the techniques used in distance-vector routing protocols to overcome inconsistent routing tables and to prevent routing loops, which can cause serious problems. For the exam, you need to know the following techniques:

Split Horizon One of the problems with early dynamic-routing protocols was the fact they were designed to advertise to every router on the network, including the routers from which they learned the same information. This created a problem of readvertising a route that no longer exists, making the router that believed the route was gone to start believing the route exists again. Using *split horizon* reduces incorrect routing information and routing overhead in a distance-vector network by enforcing the rule that information cannot be sent back in the direction from which that information was received.

Route Poisoning with Poison Reverse One of the best fixes to overcome a downed route from being readvertised is *route poisoning,* which sets a downed link to infinity. When a router poisons a downed route, neighboring routers are not susceptible to incorrect updates about the downed route because the information they receive back contains a maximum hop-count allocation. When a neighboring router receives a route poison, they send an update, called a *poison reverse*, back to the router with the downed link. This ensures that all routes on the segment have received the poisoned route information.

Hold-Downs *Hold-downs* tell routers to restrict, for a specific time period, any changes that might affect recently removed routes. This prevents inoperative routers from being prematurely restored to other routers¡¯ tables.

Triggered Updates Unlike update messages from neighbor routers, triggered updates create a new routing table that is sent immediately to neighbor routers because a change was detected in the internetwork.

Additional Routing Protocols

Two protocols not discussed in Chapter 4 of which you should have a good understanding for this objective are Routing Information Protocols version 2 (RIPv2) and Enhanced Interior Gateway Routing Protocol (EIGRP). Both of these are improvements from other protocols: RIPv2 is a new and improved version of RIP, and EIGRP has improvements over IGRP.

Routing Information Protocols version 2 (RIPv2)

Routing Information Protocol version 2 (RIPv2) is similar to version 1, but it enables the support of subnet masks, a critical feature that is not available in RIP. It also supports variable-length subnet

masks (VLSMs), with which you can use different masks for the same network number on different interfaces. This allows you to conserve IP addresses and use available address space more efficiently.

Another advantage of using RIPv2 is the availability of support for classless interdomain routing (CIDR).

Note By default, the software receives RIP version 1 and version 2 packets, but sends only version 1 packets. However, you can configure the software to receive and send only version 1 packets.

Enhanced Interior Gateway Routing Protocol (EIGRP)

Enhanced Interior Gateway Routing Protocol (EIGRP) is another Cisco proprietary distance-vector routing protocol, but it uses *Diffusing Update Algorithm (DUAL)* to provide a loop-free operation throughout the network using EIGRP protocol for routing. DUAL grants routers involved in a topology revision the ability to synchronize simultaneously, while routers unaffected by this change are not involved in receiving updates and other unnecessary updates. EIGRP uses both bandwidth and delay of the line by default to determine the best paths through the network. However, maximum transmission unit (MTU), load, and reliability of a link can be used as well.

EIGRP is also a classless routing protocol that sends subnet mask information in the DUAL updates. Classless routing allows for VLSMs and supernetting.

Note Routing protocols that support classless routing are RIPv2, EIGRP, and OSPF.

Verifying Your Configurations

Several commands apply to RIP and IGRP, but let¡¯s review the commands you need to know for this objective and also those that apply to RIPv2 and EIGRP:

show ip route Shows the routes the router knows about.

show protocols Shows the routed protocol information configured on the router.

show ip protocol Shows the routing protocol information configured on the router.

debug ip rip Shows routing updates as they are sent and received on the router to the console session.

debug ip igrp events Summarizes the IGRP routing information that is running on the network.

debug ip igrp transactions

Shows message requests from neighboring routers asking for an update and the broadcasts sent from your router toward those neighbors.

debug ip eigrp events Summarizes the EIGRP routing information that is running on the network.

debug ip eigrp transactions Shows message requests from neighboring EIGRP-enabled routers asking for an update and the broadcasts sent from your router toward those neighbors.

Necessary Procedures

The following lists the `router` command procedures to configure both RIPv2 and EIGRP routing protocols.

Configuring RIPv2

To configure RIPv2, just turn on the protocol with the `router rip` command, and then use the `version 2` command:

```
2621A(config)#router rip
2621A(config)#version 2
2621A(config-router)#network 172.16.0.0
2621A(config-router)#^Z
```

Configuring EIGRP Routing

The command used to configure EIGRP is the same as the one used to configure RIP routing. As with IGRP, you still use an AS number for EIGRP. All routers within an autonomous system must use the same AS number, or they will not communicate with routing information. Here is an example of how to turn on EIGRP routing, using an AS number of 10:

```
RouterA#config t
RouterA(config)#router eigrp 10
RouterA(config-router)#network 172.16.0.0
```

Exam Essential

Understand the differences between the various routing loop solutions. Be able to distinguish between each of these methods: split horizon, poison reverse, and hold-downs (which use triggered updates).

Key Terms and Concepts

Diffusing Update Algorithm (DUAL) An Algorithm used to provide a loop-free operation throughout the network using the EIGRP routing protocol for routing.

Enhanced Interior Gateway Routing Protocol (EIGRP) A proprietary Cisco distance-vector routing algorithm, which includes improvements from Cisco¡¯s IGRP routing protocol.

Routing Information Protocol version 2 (RIPv2) A routing algorithm that uses the distance-vector method of finding the best path to a network (hop count).

Prepare the initial configuration of your router and enable IP.

For information on this objective, please see ¡°Configure IP addresses¡± in Chapter 3, ¡°Network Protocols.¡±