# Cisco Networking Academy Program CCNA 3.0 Training Edition

**Cisco Press**

201 West 103rd Street

Indianapolis, Indiana 46290 USA

**www.ciscopress.com**

# Cisco Networking Academy Program
# CCNA 3.0 Training Edition

Published by:
Cisco Press
201 West 103rd Street
Indianapolis, IN 46290 USA

ISBN: 1-58713-126-9

## Warning and Disclaimer

This book is a training edition and is designed to help Networking Academy instructors optimize their CCNA 3.0 training experience while providing advance insight into the CCNA 3.0 texts and companion products from Cisco Press. Every effort has been made to make this training edition as complete and as accurate as possible, but no warranty or fitness is implied.

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

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

## Trademark Acknowledgments

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

This book is part of the Cisco Networking Academy® Program series from Cisco Press. The products in this series support and complement the Cisco Networking Academy Program curriculum. If you are using this book outside the Networking Academy program, then you are not preparing with a Cisco trained and authorized Networking Academy provider.

CISCO SYSTEMS

For information on the Cisco Networking Academy Program or to locate a Networking Academy, please visit www.cisco.com/edu.

## Feedback Information

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

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

We greatly appreciate your assistance.

| | | |
|---|---|---|
| Publisher | *John Wait* | |
| Editor-in-Chief | *John Kane* | |
| Executive Editor | *Carl Lindholm* | |
| Cisco Representative | *Anthony Wolfenden* | |
| Cisco Press Program Manager | *Sonia Torres Chavez* | |
| Manager, Marketing Communications, Cisco Systems | *Scott Miller* | |
| Cisco Marketing Program Manager | *Edie Quiroz* | |
| Production Manager | *Patrick Kanouse* | |
| Assistant Editor | *Sarah Kimberly* | |
| Development Editors | *Chris Cleveland* | *Andrew Cupp* |
| Project Editors | *Sheri Cain* | *San Dee Phillips* |
| Copy Editors | *Karen Gill* | *Kevin Kent* |
| Team Coordinator | *Tammi Ross* | |
| Cover Designer | *Louisa Adair* | |
| Production Team | *Mark Shirar* | |

CISCO SYSTEMS

**Corporate Headquarters**
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

**European Headquarters**
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

**Americas Headquarters**
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

**Asia Pacific Headquarters**
Cisco Systems, Inc.
Capital Tower
168 Robinson Road
#22-01 to #29-01
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the **Cisco.com Web site at www.cisco.com/go/offices.**

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia • Czech Republic Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland • Israel • Italy Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

Printed in the USA

## Contents at a Glance

## Contents

# Cisco Networking Academy Program CCNA 3.0 Training Edition

**Cisco Press**

201 West 103$^{rd}$ Street

Indianapolis, Indiana 46290 USA

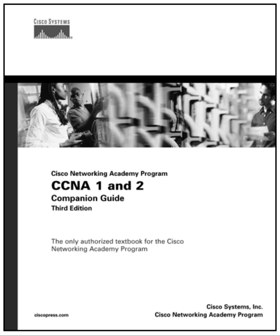
**www.ciscopress.com**

## Cisco Press Product Family Overview

Cisco Press works in conjunction with the Cisco Systems Worldwide Education Group to develop the only official books and resources for the Cisco Networking Academy Program. There are three types of core Networking Academy textbooks that Cisco Press publishes—Companion Guides, Lab Companions, and Engineering Journals and Workbooks. These materials enhance your students' learning experiences and lend support to you and the web-based curriculum developed for the Cisco Networking Academy Program.

### Companion Guides

The Companion Guide textbook serves as the main volume for the course. These comprehensive texts contain key objectives, Skillbuilder activities, figures and tables, margin notes, chapter summaries, and "Check Your Understanding" review questions. CD-ROMs that contain additional enrichment tools such as practice exam questions within a customizable test engine, e-Lab Activities, PhotoZooms, and instructional videos are included with the hardbound textbook. Often Companion Guides also include additional chapters and exercises that reach beyond the online curriculum.



Cisco Systems

Cisco Networking Academy Program
**CCNA 1 and 2**
Companion Guide
Third Edition

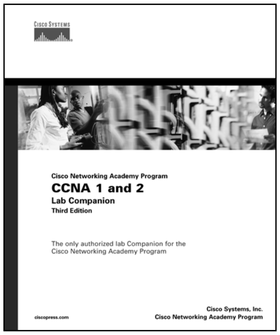
The only authorized textbook for the Cisco Networking Academy Program

ciscopress.com

Cisco Systems, Inc.
Cisco Networking Academy Program

### Lab Companions

Practice the concepts presented in the correlating Companion Guide. The Lab Companion serves as a tool for hands-on practice within the lab environment and can used for homework and tests. Most Lab Companions contain bonus labs or additional questions for further study.



Cisco Systems

Cisco Networking Academy Program
**CCNA 1 and 2**
Lab Companion
Third Edition

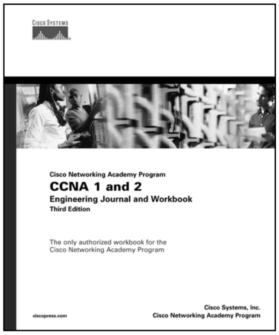
The only authorized lab Companion for the Cisco Networking Academy Program

ciscopress.com

Cisco Systems, Inc.
Cisco Networking Academy Program

### Engineering Journal and Workbooks

Have your students begin the best-practice method of keeping an engineering journal for the workplace with this resource tool that includes training exercises to reinforce classroom learning. Each chapter includes review questions and focus questions to prepare students for the corresponding course exam.



Cisco Systems

Cisco Networking Academy Program
**CCNA 1 and 2**
Engineering Journal and Workbook
Third Edition

The only authorized workbook for the Cisco Networking Academy Program

ciscopress.com

Cisco Systems, Inc.
Cisco Networking Academy Program

# Cisco Press Companion Guide Features

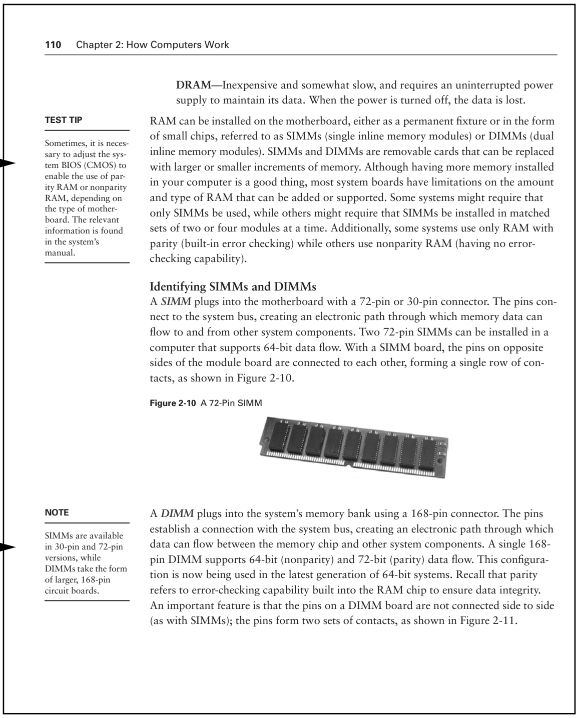
## Interior Design

Interior design features of Cisco Press Companion Guides support your teaching efforts and present components that are distinctive, readily identified, and facilitate better comprehension of course content.

### Margin Notes

Important and interesting concepts are highlighted using various types of margin notes:

- **Test tips** identify facts students need to know for certification exam success
- **Notes** mark ideas and concepts students will find interesting
- **Cautions** instruct students when to be careful or risk damage to equipment
- **Warnings** indicate dangers and hazards students must know for their personal safety



110 Chapter 2: How Computers Work

**DRAM**—Inexpensive and somewhat slow, and requires an uninterrupted power supply to maintain its data. When the power is turned off, the data is lost.

**TEST TIP**

Sometimes, it is necessary to adjust the system BIOS (CMOS) to enable the use of parity RAM or nonparity RAM, depending on the type of motherboard. The relevant information is found in the system's manual.

RAM can be installed on the motherboard, either as a permanent fixture or in the form of small chips, referred to as SIMMs (single inline memory modules) or DIMMs (dual inline memory modules). SIMMs and DIMMs are removable cards that can be replaced with larger or smaller increments of memory. Although having more memory installed in your computer is a good thing, most system boards have limitations on the amount and type of RAM that can be added or supported. Some systems might require that only SIMMs be used, while others might require that SIMMs be installed in matched sets of two or four modules at a time. Additionally, some systems use only RAM with parity (built-in error checking) while others use nonparity RAM (having no error-checking capability).

**Identifying SIMMs and DIMMs**

A *SIMM* plugs into the motherboard with a 72-pin or 30-pin connector. The pins connect to the system bus, creating an electronic path through which memory data can flow to and from other system components. Two 72-pin SIMMs can be installed in a computer that supports 64-bit data flow. With a SIMM board, the pins on opposite sides of the module board are connected to each other, forming a single row of contacts, as shown in Figure 2-10.

**Figure 2-10** A 72-Pin SIMM

**NOTE**

SIMMs are available in 30-pin and 72-pin versions, while DIMMs take the form of larger, 168-pin circuit boards.

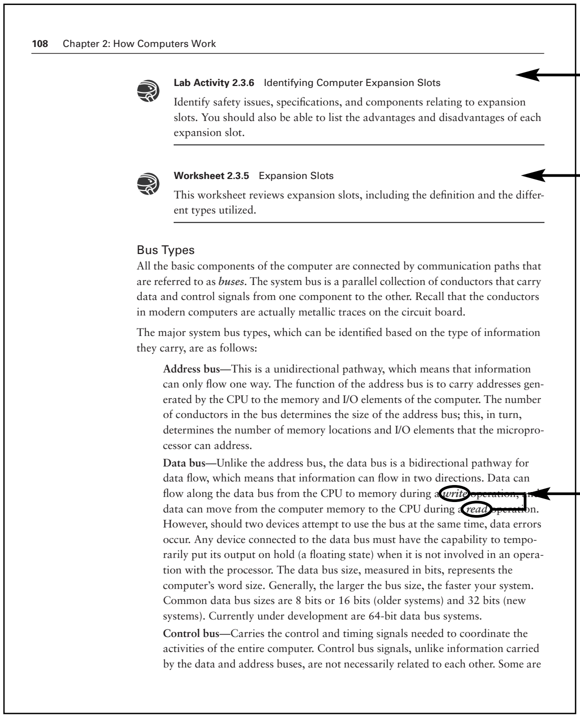
A *DIMM* plugs into the system's memory bank using a 168-pin connector. The pins establish a connection with the system bus, creating an electronic path through which data can flow between the memory chip and other system components. A single 168-pin DIMM supports 64-bit (nonparity) and 72-bit (parity) data flow. This configuration is now being used in the latest generation of 64-bit systems. Recall that parity refers to error-checking capability built into the RAM chip to ensure data integrity. An important feature is that the pins on a DIMM board are not connected side to side (as with SIMMs); the pins form two sets of contacts, as shown in Figure 2-11.

## Book Features

In addition to distinctive design elements, Cisco Press builds the following book features into every Companion Guide:

### Figures and Tables

Figures and tables are clearly rendered and labeled, and are plainly positioned near corresponding text, making it easy for students to refer to them while studying.



108 Chapter 2: How Computers Work

**Lab Activity 2.3.6** Identifying Computer Expansion Slots

Identify safety issues, specifications, and components relating to expansion slots. You should also be able to list the advantages and disadvantages of each expansion slot.

**Worksheet 2.3.5** Expansion Slots

This worksheet reviews expansion slots, including the definition and the different types utilized.

Bus Types

All the basic components of the computer are connected by communication paths that are referred to as *buses*. The system bus is a parallel collection of conductors that carry data and control signals from one component to the other. Recall that the conductors in modern computers are actually metallic traces on the circuit board.

The major system bus types, which can be identified based on the type of information they carry, are as follows:

**Address bus**—This is a unidirectional pathway, which means that information can only flow one way. The function of the address bus is to carry addresses generated by the CPU to the memory and I/O elements of the computer. The number of conductors in the bus determines the size of the address bus; this, in turn, determines the number of memory locations and I/O elements that the microprocessor can address.

**Data bus**—Unlike the address bus, the data bus is a bidirectional pathway for data flow, which means that information can flow in two directions. Data can flow along the data bus from the CPU to memory during a *write* operation, and data can move from the computer memory to the CPU during a *read* operation. However, should two devices attempt to use the bus at the same time, data errors occur. Any device connected to the data bus must have the capability to temporarily put its output on hold (a floating state) when it is not involved in an operation with the processor. The data bus size, measured in bits, represents the computer's word size. Generally, the larger the bus size, the faster your system. Common data bus sizes are 8 bits or 16 bits (older systems) and 32 bits (new systems). Currently under development are 64-bit data bus systems.

**Control bus**—Carries the control and timing signals needed to coordinate the activities of the entire computer. Control bus signals, unlike information carried by the data and address buses, are not necessarily related to each other. Some are

**Skill Builders**

Make a connection between theory and practice with the aid of skill builders. Clearly marked by icons, skill builders refer to **worksheets** and **lab activities** from the corresponding Lab Companion that reinforce hands-on training. References to the companion CD-ROM for **PhotoZooms** of actual equipment and **instructional videos** on complex topics are also included within chapters.

**Key Terms**

Key terms are clearly introduced within text, then listed at the end of each chapter for quick review, and compiled within a glossary of terms for easy reference.

**Objectives**

Each chapter starts with a succinct list of objectives that should be mastered by the end of the chapter.

**Chapter Summaries**

Appearing at the end of each chapter, chapter summaries provide topic synopses and serve as study aids.

**"Check Your Understanding" Review Questions**

Reinforce concepts and assess knowledge before moving on to subsequent chapters with these review questions presented at the end of each chapter.

## Key Elements of CCNA 3.0 Texts from Cisco Press

**Companion Guides include**

- expanded coverage on complex CCNA topics
- exclusive content that extends the curriculum
- strong textbook pedagogy and learning aids
- clear references to practical activities within Lab Companions

**Expanded CD-ROMs within Companion Guides incorporate**

- more CCNA preparation questions
- new e-Lab Activities
- additional tools such as
  - –PhotoZooms
  - –instructional videos

**Lab Companions contain**

- bonus labs on complex CCNA topics
- a new reduced price

**Engineering Journal and Workbooks have**

- concept and focus questions
- vocabulary exercises

**Overall, CCNA 3.0 textbooks are**

- mapped fully to revised 3.0 curriculum
- written by the curriculum developers
- the only textbooks approved by Cisco Systems

## Instructor Resource Center (IRC) Information

Visit the Cisco Press Networking Academy Instructor Resource Center at www.ciscopress.com/irc for product information, release news, and details on how to sample the classroom textbook companions.

### Networking Academy Newsletter Registration Information

While visiting the Instructor Resource Center, sign up for the Cisco Press Networking Academy e-mail newsletter. This monthly newsletter is filled with upcoming release information and other important new for Networking Academy instructors. Click "newsletter" to learn more.

## How to Request a Cisco Press Review Copy

### U.S. Review Copy Requests

**Option I—Request a review copy**

You may request a review copy of the current and upcoming Networking Academy products by visiting **www.ciscopress. com/networkingacademy** and following these easy steps:

**Step 1** Browse the Academy catalog and select the book you would like to review.

**Step 2** Click on "Request a Review Copy" beneath the "More Information" bar.

**Step 3** Select your customer type and follow the instructions given. Your Prentice Hall representative will be automatically notified to follow up and sample.

**Option II—Contact your Prentice Hall Representative**

Cisco Press is a division of Pearson Education and is represented in the U.S. by the Prentice Hall Education sales force. We have specialized our sales departments to provide the best service to you.

**To locate your U.S. Prentice Hall representative**

Instructors in high schools and vocational/technical schools may reach their sales and service representatives by calling **(866) 466-2539** (toll free).

Instructors in two-year colleges, community colleges, and four-year universities may contact their Prentice Hall sales and service representative by calling **(800) 526-0485** (toll free) or by visiting **www.prenhall.com/replocator** to locate their representative.

### International review copy requests

Cisco Press is represented internationally through a global network of Pearson companies and partners. Visit **www.ciscopress.com/irc** and click on "Review Copies" for instructions on how to request a deskcopy.

## How to Order Cisco Press Resources

### U.S. Orders

To place a book order, call the Pearson Customer Service line at **(800) 922-0579** with your PO number and the ISBN(s) of the title(s) you would like to order. If you do not already have an account with Pearson, your sales representative will be located and an account will be established. You may also fax your order to **(800) 445-6991**.

### International Orders

Please visit **www.ciscopress.com/international** for a complete listing of Pearson contacts for Cisco Networking Academy Program orders outside the United States.

Use the order form on the following page to help prepare your class adoption request for your school bookstore or school administrator.

## Order Form

*Use this form as you prepare the CCNA order for your bookstore.*

School Name ____________________________________________

Instructor ____________________________________________

Department____________________________________________

Course Name/Section Name__________________________________

Expected Enrollment _____________________________________

| Title | ISBN | U.S. Net Price* | Quantity |
|---|---|---|---|
| **CCNA 1 and 2—Third Editions from Cisco Press** | | | |
| **Discounted Value Packs—Order and Save** | | | |
| *CCNA 1 and 2 Complete Pack*<br>Companion Guide, Lab Companion, Engineering Journal and Workbook | 0-13121-711-9 | $80.10 | __________ |
| *CCNA 1 and 2 Lab Pack*<br>Companion Guide, Lab Companion | 0-13113-557-0 | $65.25 | __________ |
| *CCNA 1 and 2 Engineering Pack*<br>Companion Guide, Engineering Journal and Workbook | 0-13113-553-8 | $59.85 | __________ |
| **Individual Titles** | | | |
| CCNA 1 and 2 Companion Guide, Third Edition | 1-58713-110-2 | $50.00 | __________ |
| CCNA 1 and 2 Lab Companion, Third Edition | 1-58713-111-0 | $22.46 | __________ |
| CCNA 1 and 2 Engineering Journal and Workbook, Third Edition | 1-58713-112-9 | $16.46 | __________ |
| **CCNA 3 and 4—Third Editions from Cisco Press** | | | |
| **Discounted Value Packs—Order and Save** | | | |
| *CCNA 3 and 4 Complete Pack*<br>Companion Guide, Lab Companion, Engineering Journal and Workbook | 0-13121-712-7 | $80.10 | __________ |
| *CCNA 3 and 4 Lab Pack*<br>Companion Guide, Lab Companion | 0-13113-556-2 | $65.25 | __________ |
| *CCNA 3 and 4 Engineering Pack*<br>Companion Guide, Engineering Journal and Workbook | 0-13113-554-6 | $59.85 | __________ |
| **Individual Titles** | | | |
| CCNA 3 and 4 Companion Guide, Third Edition | 1-58713-113-7 | $50.00 | __________ |
| CCNA 3 and 4 Lab Companion, Third Edition | 1-58713-114-5 | $22.46 | __________ |
| CCNA 3 and 4 Engineering Journal and Workbook, Third Edition | 1-58713-115-3 | $16.46 | __________ |

***** For pricing outside of the U.S., please contact your local Pearson representative or send an email to international@pearsoned.com.

Cisco Press also has titles and discount value packages available for the other Cisco Networking Academy Program courses. Ask your Prentice Hall representative for more details.

# Bridging CCNA v2.0 and CCNA v3.0

## CCNA1

### Module 3—Networking Media

#### Lesson 3.2: Optical Media

See Chapter 3, "Networking Media," of the Cisco Press Companion Guide, Third Edition, for more information.

Optical fiber is the most frequently used medium for the longer, high-bandwidth, point-to-point transmissions required on LAN backbones and on WANs. Using optical media, light is used to transmit data over a thin glass fiber or plastic. Electrical signals cause a fiber-optic transmitter to generate the light signals sent down the fiber. The receiver produces electrical signals at the far end of the fiber. However, there is no electricity in the fiber-optic cable itself. In fact, the glass used in fiber-optic cable is a very good electrical insulator.

Optical fiber is used in networks because of the following:

- Fiber is not susceptible to lightning, electromagnetic interference (EMI), or radio frequency interference (RFI), and it does not generate EMI or RFI.
- Fiber has much greater bandwidth capabilities than other media.
- Fiber allows significantly greater transmission distances and excellent signal quality because very little signal attenuation occurs.
- Fiber is more secure than other media because it is difficult to tap into a fiber and easy to detect someone placing a tap on the fiber.
- Current fiber transmitter and receiver technologies can be replaced by newer, faster devices as they are developed so that greater transmission speeds can be achieved over existing fiber links with no need to replace the fiber.
- Fiber costs less than copper for long-distance applications.

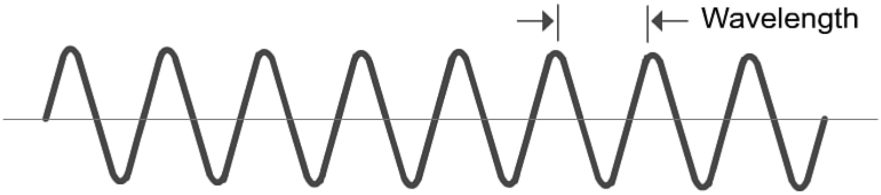
- The raw material that fiber is made from is sand, a very plentiful substance.
- With fiber, there are no grounding concerns as there are when signaling using electricity.
- Fiber is light in weight and easily installed.
- Fiber has better resistance to environmental factors, such as water, than copper wire.
- Lengths of fiber can easily be spliced together for very long cable runs.

For these reasons, when very large numbers of bits need to be sent over distances greater than 100 meters, fiber-optic cable is often used.

This section explains the basics of fiber-optic cable. You learn about how fibers can guide light for long distances. You also learn about the types of cable used, how fiber is installed, the type of connectors and equipment used with fiber-optic cable, and how fiber is tested to ensure that it functions properly.

The light used in optical-fiber networks is one type of electromagnetic energy. When an electric charge moves back and forth, or accelerates, a type of energy called *electromagnetic energy* is produced. This energy in the form of waves can travel through a vacuum, the air, and through some materials such as glass. An important property of any energy wave is the wavelength, as shown in Figure 1.

**Figure 1** Wavelengths



The part of an optical fiber through which light rays travel is called the *core* of the fiber and is shown in Figure 2. Light rays can only enter the core if their angle is inside the numeric aperture of the fiber. Likewise, after the rays have entered the core of the fiber, a light ray can follow only a limited number of optical paths through the fiber. These optical paths are called *modes*. If the diameter of the fiber core is large enough so that there are many paths that light can take through the fiber, the fiber is called *multimode* fiber. Single-mode fiber has a much smaller core that only allows light rays to travel along one mode inside the fiber, as shown in Figure 3.

**Figure 2** Fiber-Optic Cable

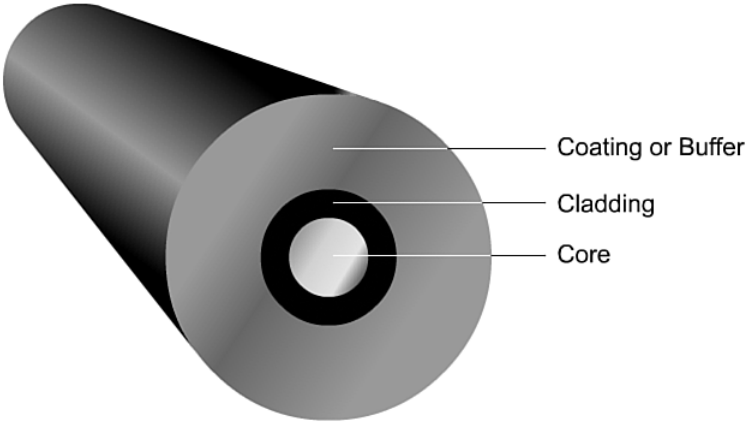
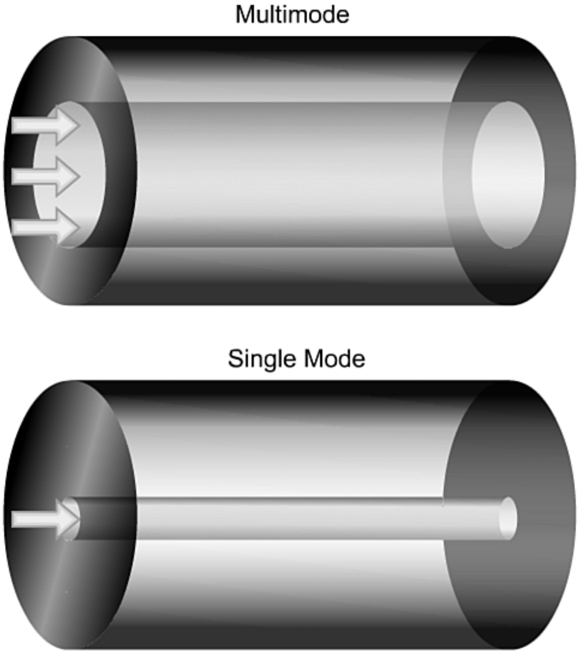


**Figure 3** Multimode and Single-Mode Fiber



## Lesson 3.3: Wireless Media

See Chapter 3, "Networking Media," of the Cisco Press Companion Guide, Third Edition, for more information.

The introduction of wireless technology removes the restraints of cables and brings true portability to the computing world. The current state of wireless technology does not provide the high-speed transfers nor the security and uptime reliability of cabled networks. However, the flexibility has justified the tradeoff.

Administrators often consider wireless when installing a new network or when upgrading an existing network. A simple wireless network could be working just a few minutes after the workstations are turned on. Connectivity to the Internet is provided through a wired connection, router, cable, or digital subscriber line (DSL) modem and a wireless access point that acts as a hub for the wireless nodes. In a residential or small office environment, these devices may be combined into a single unit.

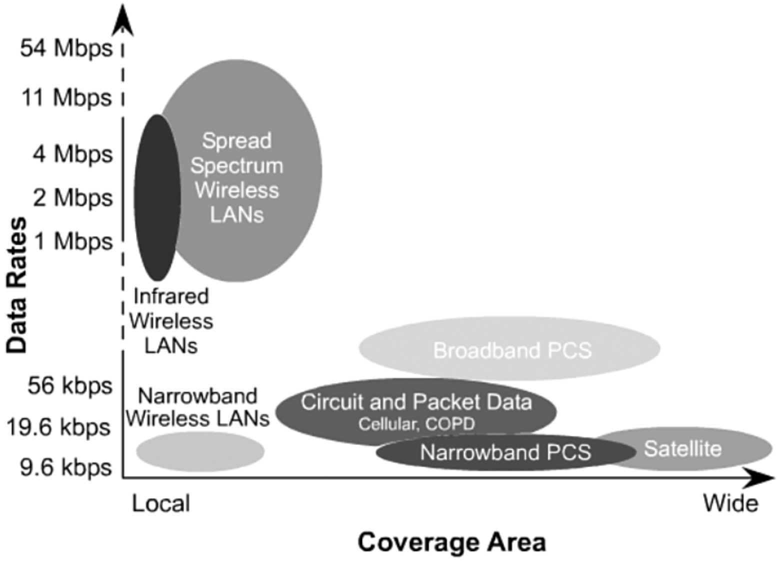
Wireless signals are electromagnetic waves that can travel through the vacuum of outer space or through a medium such as air. No physical copper-based or fiber-optic medium is necessary for wireless signals. This makes utilizing wireless signals a very versatile way to build a network. Wireless transmissions can cover large distances by using high-frequency signals. Each signal uses a difference frequency, measured in hertz (Hz) so that they remain unique from one another.

Wireless technologies have been around for many years. Satellite TV, AM/FM radio, cellular phones, remote-control devices, radar, alarm systems, weather radios, cordless phones, and retail scanners are integrated into everyday life. Today, wireless technologies are a fundamental part of business and personal life.

The radio spectrum is the part of the electromagnetic spectrum used to transmit voice, video, and data. It uses frequencies from 3 kilohertz (kHz) to 300 gigahertz (GHz). This section considers only the part of the radio spectrum that supports wireless data transmission.

Many different types of wireless data communications exist, as Figure 4 shows.

**Figure 4** Wireless Data Networks



Each type of wireless data communication has its advantages and drawbacks, as follows:

- **Infrared (IR)**—Very high data rates and lower cost, but very short distance.
- **Narrowband—**Low data rates and medium cost. Requires a license and covers a limited distance.
- **Spread spectrum—**Medium cost and high data rates. Limited to campus coverage. Cisco Aironet products are spread spectrum.
- **Broadband personal communications service (PCS)—**Low data rates, medium cost, and citywide coverage. Sprint is an exception; Sprint PCS provides nationwide and international coverage.
- **Circuit and packet data (cellular and cellular digital packet data [CDPD])—** Low data rates, high packet fees, and national coverage.
- **Satellite—**Low data rates, high cost, and nationwide or worldwide coverage.

## Module 4—Cable Testing

### Lesson 4.2: Signals and Noise

See Chapter 4, "Cable Testing and Cabling LANs and WANs," of the Cisco Press Companion Guide, Third Edition, for more information.

This lesson describes the issues relating to the testing of media used for physical layer connectivity in LANs. For the LAN to function properly, the physical layer medium must meet the industry standard specifications.

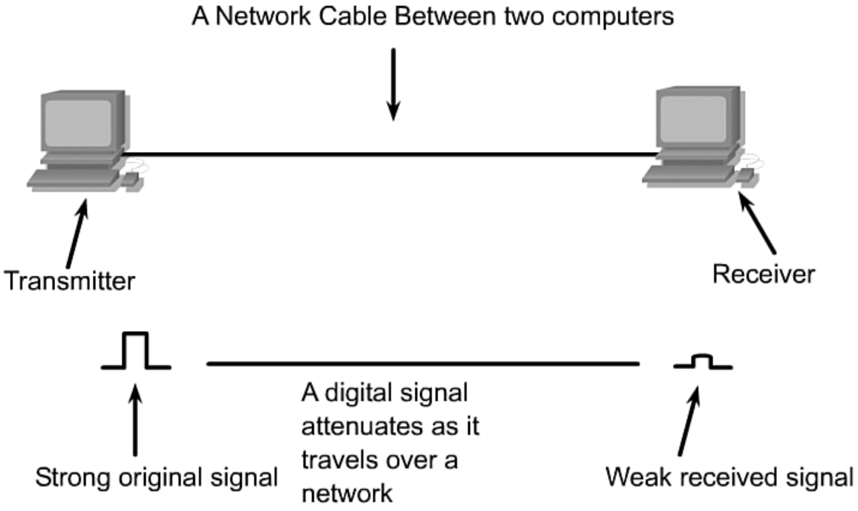
*Noise* refers to any interference on the physical medium that makes it difficult for the receiver to detect the data signal. There are many sources of noise when copper cabling is used, but far fewer sources of noise when optical fiber is used as the transmission medium. Some level of noise on the medium is inevitable, but that acceptable level of noise must be kept as low as possible. Just as it is difficult to carry on a conversation when the background noise of the room is high compared to the volume of the participants' voices, data signals can be overwhelmed by the strength of noise to the point that the desired signal cannot be interpreted.

Proper cable installation techniques and proper attachment of connectors at both ends of a cable are vital. If standards are followed, the data signal experiences less attenuation, and noise levels remain a minimum.

After cable has been installed, it must be tested and meet the specifications of the TIA/EIA-568-B standards. Problems must be identified and corrected prior to further installation of network hardware. Installed cable should also be tested periodically after the installation to determine whether it still meets specifications. Cable and connectors experience wear and deterioration over a period of time and potential problems must be identified and corrected ensure reliable network operation. All cable testing and troubleshooting requires the use of quality cable testers.

*Attenuation* is the decrease in signal amplitude over the length of a link, as shown in Figure 5. Long cable lengths and high signal frequencies contribute to greater signal attenuation. For this reason, attenuation on a cable is measured by a cable tester using the highest frequencies that the cable is rated to support. Attenuation is measured from only one direction on all wire pairs of the cable because the attenuation of a wire pair is the same in either direction.

**Figure 5** Attenuation


A Network Cable Between two computers
Transmitter
Receiver
Strong original signal
A digital signal attenuates as it travels over a network
Weak received signal

*Impedance* is a measurement of the resistance of the cable to an alternating current (AC) and is measured in ohms. The normal (characteristic) impedance of a Category 5 cable is 100 ohms. If a connector is improperly installed on Category 5, it will have a different impedance value than the cable. This is called an *impedance discontinuity* or an *impedance mismatch*.

Impedance discontinuities cause attenuation because a portion of a transmitted signal is reflected back to the transmitting device instead of continuing to the receiver, much like an echo. This effect is compounded if multiple discontinuities cause additional portions of the remaining signal to reflect back to the transmitter. When this returning reflection strikes the first discontinuity, some of the signal rebounds in the direction of the original signal, creating multiple echo effects. The echoes strike the receiver at different intervals making it difficult for the receiver to accurately detect data values on the signal. This effect is called *jitter* and results in data errors.

The combination of the effects of signal attenuation and impedance discontinuities on a communications link is called *insertion loss*. Proper network operation depends on constant characteristic impedance in all cables and connectors, with no impedance discontinuities in the entire cable system.

*Crosstalk* involves the transmission of signals from one wire pair to nearby pairs. When voltages change on one pair of wires, electromagnetic energy is generated. This energy radiates outward from the transmitting wire pair like a radio signal from a transmitter. Adjacent wire pairs in the cable act like antennas generating a weaker but similar electrical signal onto the nearby wire pairs. This causes interference with data that may be present on the adjacent wires. Signals from a completely separate nearby cable can also cause crosstalk. When a signal from outside the cable causes crosstalk, it is called *alien crosstalk*.

The three distinct types of crosstalk are as follows:

- Near-end crosstalk (NEXT), shown in Figure 6
- Far-end crosstalk (FEXT), shown in Figure 7
- Power sum near-end crosstalk (PSNEXT), shown in Figure 8

**Figure 6** Near-End Crosstalk (NEXT)

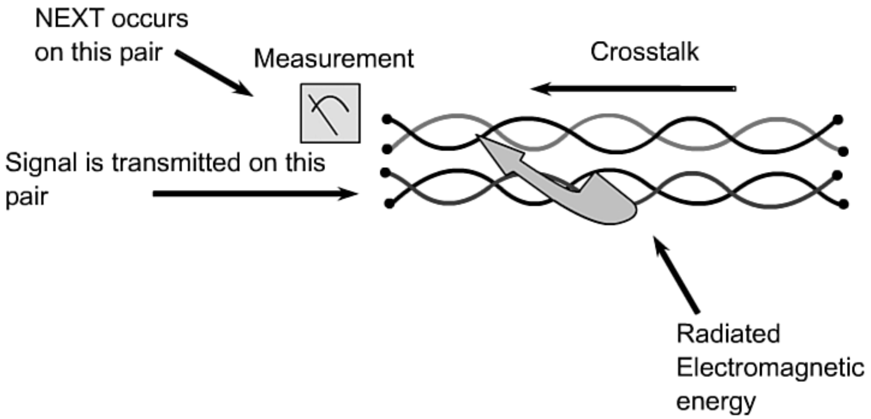

NEXT occurs on this pair
Measurement
Crosstalk
Signal is transmitted on this pair
Radiated Electromagnetic energy

**Figure 7** Far-End Crosstalk (FEXT)

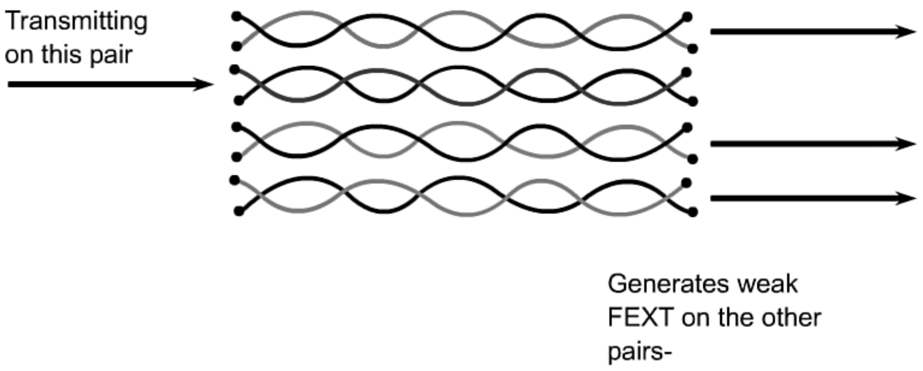
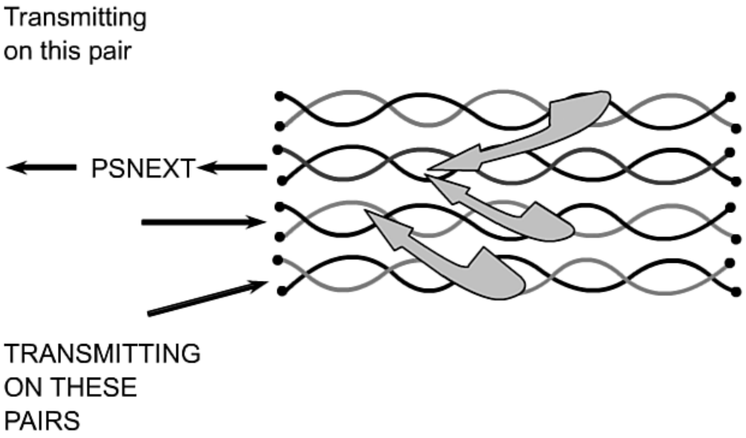

Transmitting on this pair
Generates weak FEXT on the other pairs-

**Figure 8** Power Sum Near-End Crosstalk (PSNEXT)



## Module 6—Ethernet Fundamentals

### Lesson 6.1: Ethernet Fundamentals

See Chapter 5, "Ethernet Fundamentals," of the Cisco Press Companion Guide, Third Edition, for more information.

Ethernet, in its various forms, is the most widely used LAN technology. Ethernet was designed to fill the middle ground between long-distance, low-speed networks and specialized, computer-room networks carrying data at high speeds for very limited distance.

Ethernet is well suited to applications in which a local communication medium must carry sporadic, occasionally heavy traffic at high-pack data rates. It was designed to enable sharing resources on a local workgroup level. Design goals include simplicity, low cost, compatibility, fairness, low delay, and high speed.

In this module, you learn about history of Ethernet and IEEE Ethernet standards. In addition, this module introduces collision domains and broadcast domains. Finally, this module describes segmentation and the devices used to create network segments.

Ethernet is the dominant LAN technology in the world. Most of the traffic on the Internet originates and ends with an Ethernet connection. From its beginning in the 1970s, Ethernet has evolved to meet the increasing demand for high-speed LANs. When a new media, fiber-optic cable, was produced, Ethernet adapted to take advantage of fiber's great bandwidth and low error rate. Now, the same basic protocol that transported data at 3 megabits per second (Mbps) in 1973 is carrying data at 10 gigabits per second (Gbps).

The original technology that today's Ethernet is based on was wireless. This work later formed the basis for the famous Ethernet MAC method known as carrier sense multiple access/collision detect (CSMA/CD). CSMA/CD is discussed in more detail later in this module.

The original idea for Ethernet grew out of the problem of allowing two or more users to use the same medium without each user's signals interfering with the other's.

During the mid-1980s, Ethernet's 10-Mbps bandwidth was more than enough for the PCs of that era. By the early 1990s, PCs had become much faster and people were beginning to complain about the bottleneck caused by the small bandwidth of Ethernet LANs. In 1995, the IEEE announced a standard for a 100-Mbps Ethernet. This was followed by standards for Gigabit (1 billion bits per second) Ethernet in 1998 and 1999. IEEE approved the standards for 10 Gigabit Ethernet in June 2002. These more modern standards are still Ethernet (802.3).

Like the International Organization for Standardization (ISO), the IEEE is a standards-making organization. The manufacturers of networking equipment are not required to fully comply with all the specifications of any standard. The goals of IEEE are as follows:

- To supply the engineering information necessary to build devices that comply with an Ethernet standard
- To not stifle innovation by manufacturers

## Lesson 6.1: Ethernet Operation

See Chapter 5, "Ethernet Fundamentals," of the Cisco Press Companion Guide, Third Edition, for more information.

This section discusses the operation of Ethernet, Ethernet framing, error handling, and the different types of the collisions on Ethernet networks. When multiple stations (nodes) must access physical media and other networking devices, various media access control strategies have been invented. This lesson briefly reviews the access control strategies, and then the discussion focuses on the Ethernet access control method: CSMA/CD.

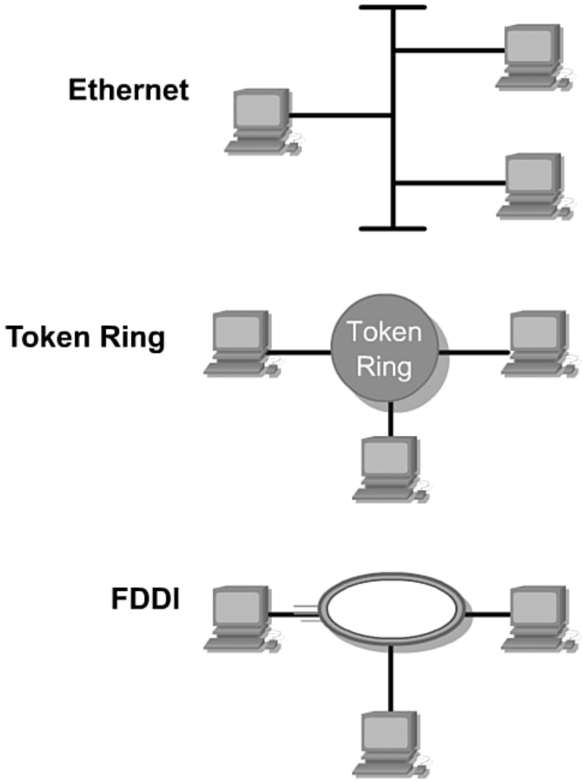
Note that although CSMA/CD has immense historical importance and practical importance in original Ethernet, it is diminishing somewhat in implementation for two reasons:

- When four-pair unshielded twisted-pair (UTP) is used, separate wire pairs for transmission (Tx) and reception (Rx) exist, making copper UTP potentially collisionless and capable of full duplex depending on whether it is deployed in a shared (hub) or switched environment.
- Similar logic applies to optical-fiber links, where separate optical paths—a transmission fiber and an reception fiber—are used.

One new form of Ethernet—1000BASE-TX, Gigabit Ethernet over copper—uses all four wire pairs simultaneously in both directions, resulting in a permanent collision. In older forms of Ethernet, such a permanent collision would preclude the system from working. In 1000BASE-TX, however, sophisticated circuitry can accommodate this permanent collision resulting from an attempt to get as much data as possible over UTP.

Three well-known Layer 2 technologies are Token Ring, FDDI, and Ethernet. Of these, Ethernet is by far the most common; however, they all serve to illustrate a different approach to LAN requirements. All three specify Layer 2 elements (for example, logical link control [LLC], naming, framing, and MAC), as well as Layer 1 signaling components and media issues. Figure 9 shows the specific technologies for each, and the following list describes each element.

**Figure 9** Common LAN Technologies



- **Ethernet—**Logical bus topology (information flow is on a linear bus) and physical star or extended star (wired as a star)
- **Token Ring—**Logical ring topology (in other words, information flow is controlled in a ring) and a physical star topology (wired as a star)
- **FDDI—**Logical ring topology (information flow is controlled in a ring) and physical dual-ring topology (wired as a dual-ring)

Ethernet is a shared-media broadcast technology. The access method CSMA/CD used in Ethernet performs three functions:

- Transmitting and receiving data packets
- Decoding data packets and checking them for valid addresses before passing them to the upper layers of the OSI model
- Detecting errors within data packets or on the network

In the CSMA/CD access method, networking devices with data to transmit over the networking media work in a listen-before-transmit mode (CS standing for carrier sense). With shared Ethernet, this means that when a device wants to send data, it must first check to see whether the networking media is busy—that is, whether there are any signals on the networking media. After the device determines the networking media is not busy, it begins to transmit its data. While transmitting its data in the form of signals, it also listens, to ensure no other stations are transmitting data to the networking media at the same time. If two stations send data at the same time, a collision occurs, as shown in the upper half of Figures 10 and 11. After it completes transmitting its data, the device returns to listening mode. With traditional shared Ethernet, only one device can transmit at a time. This is not true with switched Ethernet.

**Figure 10** CSMA/CD Process

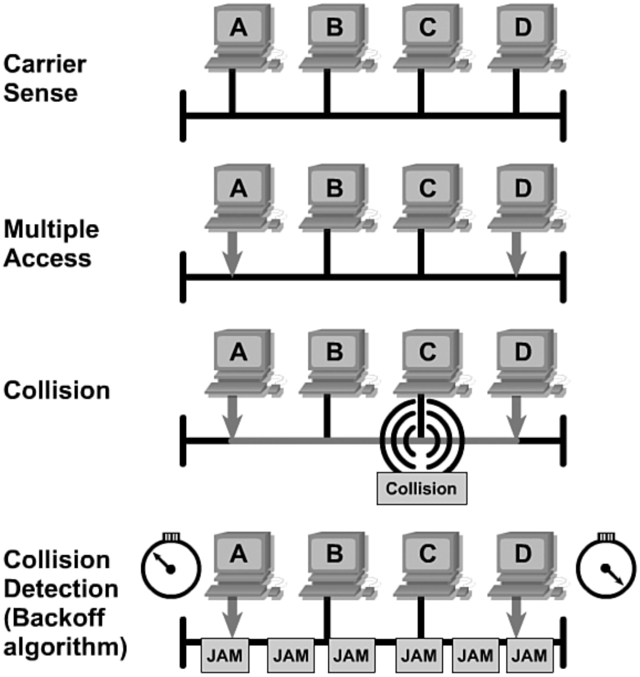
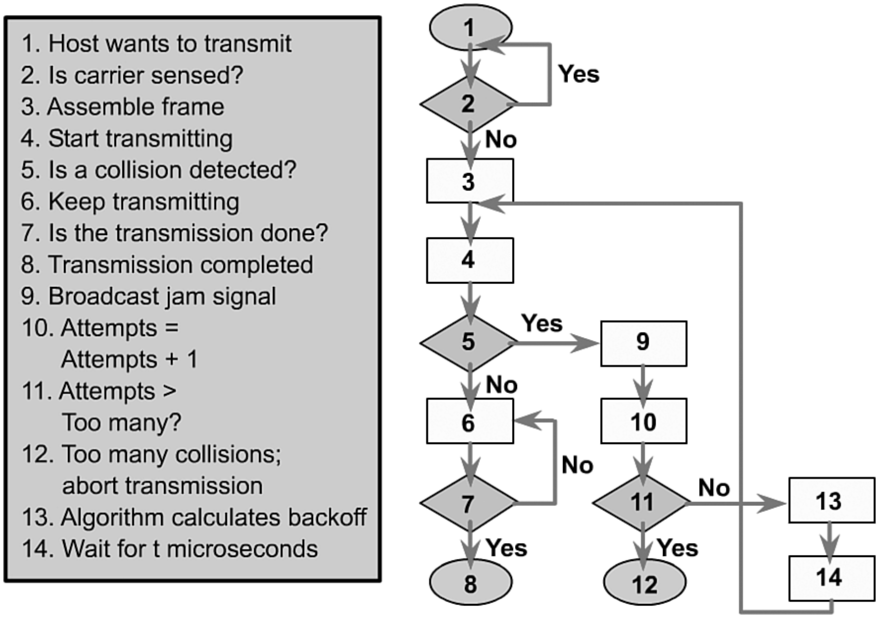


**Figure 11** CSMA/CD Process


1. Host wants to transmit
2. Is carrier sensed?
3. Assemble frame
4. Start transmitting
5. Is a collision detected?
6. Keep transmitting
7. Is the transmission done?
8. Transmission completed
9. Broadcast jam signal
10. Attempts = Attempts + 1
11. Attempts > Too many?
12. Too many collisions; abort transmission
13. Algorithm calculates backoff
14. Wait for t microseconds
1
2
Yes
No
3
4
5
Yes
9
No
6
10
No
7
11
No
13
Yes
Yes
8
12
14

## Module 7—Ethernet Technologies

### Lesson 7.1: 10/100-Mbps Ethernet

See Chapter 6, “Ethernet Technologies and Ethernet Switching,” of the Cisco Press Companion Guide, Third Edition, for more information.

Ethernet has been the most successful LAN technology largely because of its simplicity of implementation compared to other technologies. Ethernet has also been successful because it has been a flexible technology that has evolved to meet changing needs and media capabilities. This lesson introduces the specifics of the most important varieties of Ethernet.

Changes in Ethernet have resulted in major improvements over the 10-Mbps Ethernet of the early 1980s. The 10-Mbps Ethernet standard remained virtually unchanged until 1995 when IEEE announced a standard for a 100-Mbps Fast Ethernet. The power, versatility, and cost effectiveness of 10BASE-T coincided with an explosion in the number of LAN users, the number of Internet users (which also increased LAN traffic), and the complexity of applications. Demand for higher bandwidth grew, and Fast Ethernet was introduced. The copper-cable version of Fast Ethernet that became commercially successful was 100BASE-TX, and many clever features were developed for interoperability with 10BASE-T systems (the emergence of “10/100” interfaces, for example). To compete with the backbone/LAN technology of FDDI, fiber-based 100BASE-FX was introduced. Throughout all of these Ethernet technologies, the MAC addressing concept, the frame format, and CSMA/CD MAC method were maintained.

10BASE-T (originally 802.3i-1990) substituted the cheaper and easier-to-install UTP copper cable for coaxial cable. This cable plugged into a central connection device, a hub or a switch, that contained the shared bus. The type of cable used in 10BASE-T, the distances that the cable could extend from the hub, and the way in which the UTP was installed, interconnected, and tested—all these factors were standardized in a "structured cabling system," which increasingly specified a star or extended star topology. 10BASE-T was originally a half-duplex protocol, but full-duplex features were added later. The explosion in Ethernet's popularity in the 1990s—when Ethernet came to dominate LAN technology—was 10BASE-T running on Category (Cat) 5 UTP.

10BASE-T links generally consist of a connection between the station and a hub or switch. Hubs should be thought of as multiport repeaters and count toward the limit on repeaters between distant stations. Switches can be thought of as multiport bridges and are subject to 100-meter length limitations but no limit on switches between distant stations.

100-Mbps Ethernet, also known as Fast Ethernet (in comparison to the original 10-Mbps Ethernet), was a series of technologies. The two technologies that became commercially important are 100BASE-TX (copper-UTP based) and 100BASE-FX (multimode optical-fiber based). This section examines what these technologies have in common and then examines their individual differences.

100BASE-TX and 100BASE-FX have three things in common:

- The timing parameters
- The frame format
- Parts of the transmission process

Table 1 shows the parameters for 100-Mbps Ethernet operation.

**Table 1** Parameters for 100-Mbps Ethernet Operation

| **Parameter** | **Value** |
|---|---|
| Bit time | 10 ns* |
| Slot time | 512 bit times |
| Interframe spacing | 96 bits |
| Collision attempt limit | 16 |
| Collision backoff limit | 10 |
| Collision jam size | 32 bits |
| Maximum untagged frame size | 1518 octets |
| Minimum frame size | 512 bits (64 octets) |

*ns = nanosecond

100BASE-TX and 100BASE-FX both share timing parameters. Note that 1 bit time in 100-Mbps Ethernet is 10 ns = .01 microseconds = 1 100-millionth of a second.

The 100-Mbps frame format is the same as the 10-Mbps frame. Unlike 10-Mbps Ethernet where the process was the same for all technologies until the signal was applied to the medium, the encoding process differs for each 100-Mbps technology and has multiple steps.

Fast Ethernet represents a 10-fold increase in speed. With this increase in speed comes extra requirements. The bits being sent are getting shorter in duration and occurring more frequently. They require more careful timing, and their transmission requires frequencies closer to medium bandwidth limitations and become more susceptible to noise. In response to these issues of synchronization, bandwidth, and signal-to-noise ratio (SNR), 100-Mbps Ethernet uses two separate encoding steps. The basic idea is to use codes—which can be engineered to have desirable properties—to represent the user data in a way that is efficient to transmit, including achievement of synchronization, efficient usage of bandwidth, and improved SNR characteristics. The first part of the encoding uses a technique called 4-bit/5-bit (4B/5B); the second part of the encoding is the actual line encoding specific to copper or fiber.

The two forms of 100-Mbps Ethernet of consideration in this course, 100BASE-TX and 100BASE-FX, take nibbles (4-bit groupings) from the upper parts of the MAC sublayer and encode them.

The need for faster networks led to the announcement of the 100BASE-T Fast Ethernet and autonegotiation standard in 1995 (originally 802.3u-1995). 100BASE-T increased Ethernet's bit rate to 100 Mbps. 100BASE-TX was the Category 5 UTP version of 100BASE-T that became commercially successful.

Why use 100BASE-FX (introduced as part of the 802.3u-1995 standard)? At the time copper-based Fast Ethernet was introduced, a fiber version was desired for backbone applications, connections between floors and buildings where copper is less desirable and high-noise environments. 100BASE-FX was also positioned as an alternative to the then-popular FDDI (100-Mbps token-passing, dual-ring LAN using fiber-optic cable). However, the vast majority of Fast Ethernet installations today are 100BASE-TX. One reason for the relative lack of adoption of 100BASE-FX was the rapidity of the introduction of Gigabit Ethernet copper and fiber standards, which are now the dominant technology for backbone installations, high-speed cross-connects, and general infrastructure needs.

## Lesson 7.2: 1000-Mbps/10-Gbps Ethernet

See Chapter 6, "Ethernet Technologies and Ethernet Switching," of the Cisco Press Companion Guide, Third Edition, for more information.

Fast Ethernet (100 Mbps) represented a major improvement over Legacy Ethernet (10 Mbps). Yet the even more rapid progression from Fast to Gigabit Ethernet is testimony to the power of IEEE standards, engineering advances, and market forces. Gigabit Ethernet, 1000 Mbps, is a 100-fold increase in network speed over the wildly popular 10BASE-T. Although MAC addressing, CSMA/CD, and most importantly the frame format from earlier versions of Ethernet are preserved, many other aspects of the MAC sublayer, the physical layer, and the medium have been changed.

Copper interfaces capable of “10/100/1000” operation are now common. Gigabit switch and router ports and blades are becoming routine in wiring closets. More multimode and single-mode optical fiber is being installed. A major emphasis of Gigabit Ethernet is fiber-optic technology, but the need for a copper version led to a very clever scheme to get 1000 Mbps down the same Category 5 UTP used so successfully in 10-Mbps and 100-Mbps Ethernet. (The copper version is necessary take advantage of existing cable plants and to utilize the ruggedness of copper in user environments.) All the Gigabit technologies are intrinsically full duplex. The inexorable forward march of technology continues as standards and technologies for 40 Gbps, 100 Gbps, and 160 Gbps are currently being implemented. Most dramatic is the evolution of Ethernet from LAN applications only to an end-to-end LAN, metropolitan-area network (MAN), and WAN technology.

### 1000-Mbps Versions of Ethernet (Gigabit)

In 1998, the 1000BASE-X standard was adapted by the IEEE 802.3z committee. This standard raised the data transmission rate to 1 Gbps full duplex over optical fiber, a 100-fold increase in speed over 10BASE-T. The 1000BASE-T standard, specifying 1 Gbps full duplex over Category 5 or higher UTP was adopted in 1999.

Table 2 shows the parameters for 1000-Mbps Ethernet operation.

**Table 2** Parameters for Gigabit Ethernet Operation

| Parameter | Value |
|---|---|
| Bit time | 1 ns |
| Slot time | 4096 bit times |
| Interframe spacing | 96 bits* |
| Collision attempt limit | 16 |
| Collision backoff limit | 10 |
| Collision jam size | 32 bits |
| Maximum untagged frame size | 1518 octets |
| Minimum frame size | 512 bits (64 octets) |
| Burst limit | 65,536 bits |

*The value listed is the official interframe spacing.

1000BASE-T, 1000BASE-SX, and 1000BASE-LX all share the same timing parameters. Note that bit time at 1000 Mbps = 1 ns = .001 microseconds = 1 billionth of a second. Also note that some differences in timing relative to Legacy and Fast Ethernet are now appearing because of the special issues that arise with such short bit and slot times.

The 1000-Mbps (Gigabit) Ethernet frame has the same format as is used for 10- and 100-Mbps Ethernet. 1000-Mbps Ethernet has different paths for the process of converting frames to bits on the cable, depending on which implementation is used.

Gigabit Ethernet is a 10-fold increase in speed over Fast Ethernet. Just as with Fast Ethernet, with this increase in speed comes extra requirements—the bits being sent are getting shorter in duration (1 ns). The bits are occurring more frequently, they require more careful timing, their transmission requires frequencies closer to medium bandwidth limitations, and they become more susceptible to noise. In response to these issues of synchronization, bandwidth, and SNR, Gigabit Ethernet uses two separate encoding steps. The basic idea is to use codes—which can be engineered to have desirable properties—to represent the user data in a way that is efficient to transmit, including achievement of synchronization, efficient usage of bandwidth, and improved SNR characteristics.

### 1000BASE-T

Goals for 1000BASE-T (introduced as 802.3ab-1999 1000BASE-T Gigabit Ethernet over twisted-pair) included the following:

- Functioning over existing Category 5 copper-cable plants
- Ensuring this cable would work by passing a Category 5e test, which most cable can pass after a careful determination
- Interoperability with 10BASE-T and 100BASE-TX
- Applications such as building backbones, inter-switch links, wiring-closet applications, server farms, and high-end desktop workstations
- Providing 10x bandwidth of Fast Ethernet, which became very widely installed by end users helping to necessitate more speed upstream in the network

To achieve this speed running over Category 5e copper cable, 1000BASE-T needed to use all four pairs of wires. Category 5e cable can reliably carry up to 125 Mbps of traffic. Using sophisticated circuitry, full-duplex transmissions on the same wire pair allow 250 Mbps per pair, multiplied by four wire pairs gives a total of 1000 Mbps (1 Gbps). For some purposes, it is helpful to think of these four wire pairs as "lanes" over which the data travels simultaneously (to be carefully reassembled at the receiver).

Gigabit Ethernet over fiber is one of the better recommended backbone technologies. Its benefits are tremendous:

- 1000-Mbps data transfer can aggregate groupings of widely deployed Fast Ethernet devices.
- Noise immunity.

- Lack of any ground potential problems between floors or buildings.
- An explosion in 1000BASE-X device options.
- Excellent distance characteristics.

Gigabit Ethernet over fiber was originally introduced in the IEEE 802.3 supplement titled 802.3z-1998 1000BASE-X Gigabit Ethernet. The only application for which 1000BASE-SX and 1000BASE-LX has not caught on as rapidly is to the office desktop—1000BASE-TX is considered more “user proof” in terms of day-to-day wear and 10/100/1000-Mbps copper interfaces are common.

### 10-Gbps Versions of Ethernet

Most recently, in 2002, IEEE 802.3ae was adopted. This standard specifies 10-Gbps full-duplex transmission over fiber-optic cable. Taken as a whole, the similarities between 802.3ae and 802.3 (the original Ethernet) and all of the other varieties of Ethernet are remarkable. Metcalfe’s original design has evolved, but it is still very apparent in the modern Ethernet. Recently 10 Gigabit Ethernet (10GbE) has emerged as the latest example of the extensibility of the Ethernet system. Usable for LANs, storage-area networks (SANs), MANs, and WANs, 10GbE offers exciting new networking possibilities. What is 10GbE and why should it be used?

Legacy Ethernet, Fast Ethernet, and Gigabit Ethernet now dominate the LAN market. The next step in the evolution of Ethernet is to move to 10GbE, operating at 10,000,000,000 bps. By maintaining the frame format and other Ethernet Layer 2 specifications, increasing bandwidth needs can be accommodated with the low-cost, easily implementable, and easily interoperable 10GbE. 10GbE will only run over optical-fiber media. End-to-end Ethernet networks become possible.

Because of massive growth in Internet and intranet-based traffic, and the rapidly increasing use of Gigabit Ethernet, even higher-bandwidth interconnections are needed. Internet service providers (ISPs) and network service providers (NSPs) can use 10GbE to create high-speed, low-cost, easily interoperable connections between co-located carrier switches and routers. Points of presence (POPs), intranet server farms comprised of Gigabit Ethernet servers, digital video studios, SANs, and backbones are already envisaged applications.

Perhaps most significantly, a major conceptual change comes with 10GbE. Ethernet is traditionally thought of as a LAN technology. But 10GbE physical layer standards allow both an extension in distance (to 40 kilometers [km] over single-mode fiber) and compatibility with Synchronous Optical Network (SONET)/Synchronous Digital Hierarchy (SDH) networks. Operation at a 40-km distance makes 10GbE a viable MAN technology. Compatibility with SONET/SDH networks operating up to OC-192 speeds (9.584640 Gbps) make 10GbE a viable WAN technology. 10GbE might also compete with Asynchronous Transfer Mode (ATM) for certain applications.

The following summarizes how 10GbE compares to other varieties of Ethernet:

- Frame format is the same, allowing interoperability between all varieties of Legacy, Fast, Gigabit, and 10GbE, with no reframing or protocol conversions.
- Bit time is now 0.1 ns; all other time variables scale accordingly.
- Because only full-duplex fiber connections are used, CSMA/CD is not necessary.
- The IEEE 802.3 sublayers within OSI Layers 1 and 2 are mostly preserved, with a few additions to accommodate 40-km fiber links and interoperability with SONET/SDH technologies.
- Flexible, efficient, reliable, relatively low-cost, end-to-end Ethernet networks become possible.
- TCP/IP can run over LANs, MANs, and WANs with one Layer 2 transport method.

# CCNA2

## Module 8—TCP/IP Messages

### Lesson 8.1: Overview of TCP/IP Error Messages

See Chapter 17, “TCP/IP Error and Control Messages,” of the Cisco Press Companion Guide, Third Edition, for more information.

IP is limited in that it is a best-effort delivery system and an unreliable method for delivery of network data (the reason it is known as a “best-effort“ delivery mechanism). It has no built-in processes to ensure that data is delivered in the event that problems exist with network communication. If an intermediary device such as another router fails or if a destination device is disconnected from the network, delivery will not happen. Additionally, nothing in its basic design allows IP to notify the sender that a data transmission has failed. Internet Control Message Protocol (ICMP), shown in Figure 12, is the component of the TCP/IP protocol stack that addresses this basic limitation of IP. ICMP does not overcome the unreliability issues in IP. Upper-layer protocols must provide reliability if needed. This lesson describes the various types of ICMP error messages and some of the ways they are used.

ICMP is an error-reporting protocol for IP. When datagram delivery errors occur, ICMP is used to report these errors back to the sender of the datagram. If Workstation 1 in Figure 13 sends a datagram to Workstation 6, but the corresponding interface on Router C goes down, for example, Router C uses ICMP to send a message back to Workstation 1 indicating that the datagram could not be delivered. ICMP does not correct the encountered network problem. In the example from Figure 13, ICMP does not attempt to correct the problem with the interface on Router C that is preventing datagram delivery. The only capability of ICMP is to report the errors back to Workstation 1.

**Figure 12** ICMP

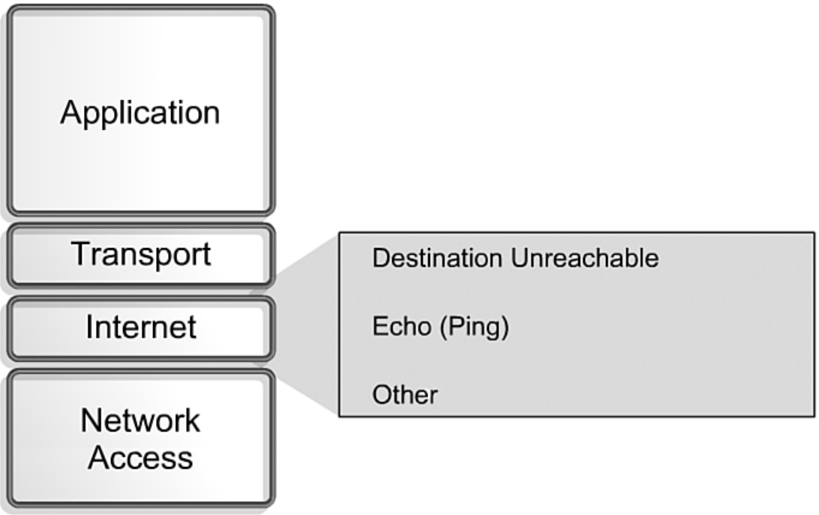
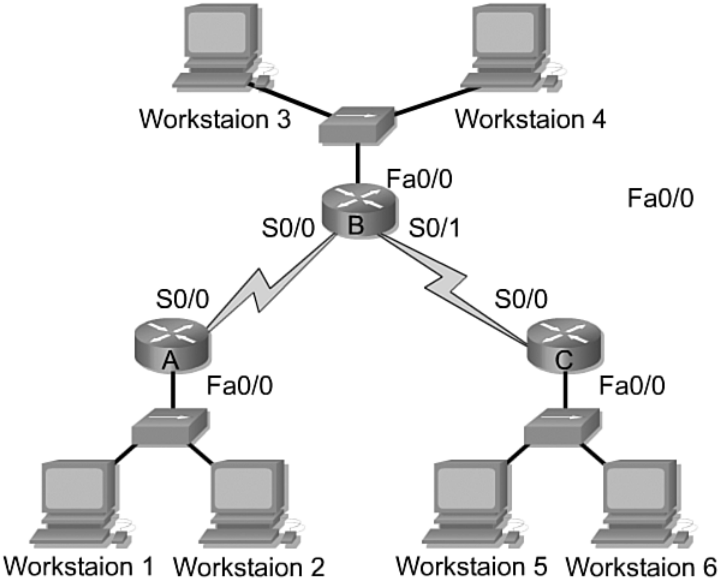


**Figure 13** Error Reporting and Error Correction



**NOTE**

Router C does not notify the intermediary devices of the delivery failure. That is, in this example, Router C does not send ICMP messages to Router A and Router B; Router C just sends the message to the originating device. Neither does Router C know the path the datagram has taken to arrive there. Datagrams contain only source and destination IP addresses. They do not contain information about all the intermediary devices. Therefore, the reporting device has only the sender's IP address with which to communicate. This is not to say that Routers A and B will never become aware of the down interface on Router C, but the dissemination of this information to neighbor routers is not the function of ICMP. ICMP reports on the status of the delivered packet to the sender. Its function is not to propagate information about network changes.

Note the following key points:

- IP is a best-effort delivery method that uses ICMP messages to alert the sender that the data did not reach its destination.
- ICMP echo request and echo reply messages allow the network administrator to test IP connectivity to aid in the troubleshooting process.
- ICMP messages are transmitted using the IP protocol, so their delivery is unreliable.
- ICMP packets have their own special header information starting with a type field and a code field.

## Lesson 8.2: Overview of TCP/IP Control Messages

See Chapter 17, "TCP/IP Error and Control Messages," of the Cisco Press Companion Guide, Third Edition, for more information.

Because IP does not have a built-in mechanism for sending error and control messages, it uses ICMP to send and receive error and control messages to hosts on a network. This lesson focuses on control messages, which are messages that provide information or configuration parameters to hosts. Knowledge of ICMP control messages is an essential part of network troubleshooting and is a key to a full understanding of IP networks.

Students completing this lesson should be able to

- Identify potential causes of specific ICMP error messages.
- Describe ICMP control messages.
- Identify a variety of ICMP control messages used in networks today.
- Determine the causes for ICMP control messages.

The Internet Control Message Protocol (ICMP) is an integral part of the TCP/IP protocol suite. In fact, all IP implementations must include ICMP support. The reasons for this are simple. First, because IP does not guarantee delivery, it has no inherent method to inform hosts when errors occur. Second, IP has no built-in method to provide informational or control messages to hosts. For this reason, ICMP performs these functions for IP.

Unlike error messages, control messages are not the results of lost packets or error conditions that occur during packet transmission. Instead, they are used to inform hosts of conditions such as network congestion or the existence of a better gateway to a remote network. Like all ICMP messages, ICMP control messages are encapsulated within an IP datagram, as shown in Figure 14. ICMP uses IP datagrams to traverse multiple networks.

**Figure 14** Control Messages

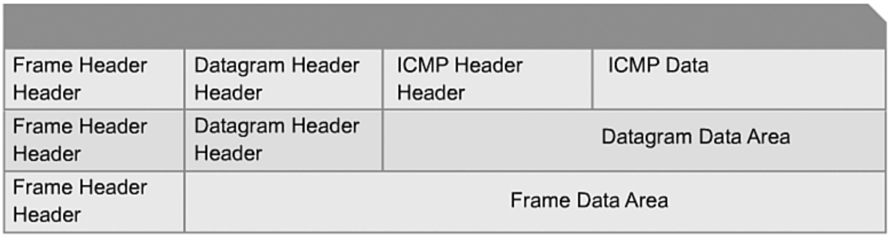
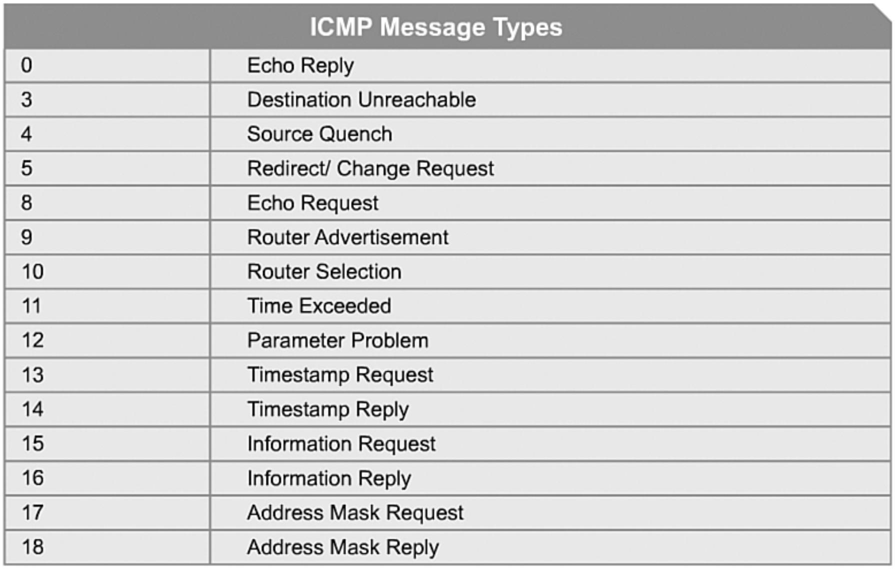


**Figure 15** ICMP Message Types



| ICMP Message Types | |
|---|---|
| 0 | Echo Reply |
| 3 | Destination Unreachable |
| 4 | Source Quench |
| 5 | Redirect/ Change Request |
| 8 | Echo Request |
| 9 | Router Advertisement |
| 10 | Router Selection |
| 11 | Time Exceeded |
| 12 | Parameter Problem |
| 13 | Timestamp Request |
| 14 | Timestamp Reply |
| 15 | Information Request |
| 16 | Information Reply |
| 17 | Address Mask Request |
| 18 | Address Mask Reply |

## Module 9—Basic Router Troubleshooting

### Lesson 9.1: Examining the Routing Table

See Chapter 18, "Basic Router Troubleshooting," of the Cisco Press Companion Guide, Third Edition, for more information.

One of a router's primary functions is to determine the best path to a given destination. A router learns paths, also called *routes*, from an administrator's configuration or from other routers via routing protocols. They store this routing information in "routing tables" using onboard random-access memory (RAM). A routing table contains a list of the best available routes and routers use this table to make packet-forwarding decisions.

The **show ip route** command displays the contents of the IP routing table. This table contains entries for all known networks and subnetworks (and a code that indicates how that information was learned). You can use the following additional commands with the **show ip route** command:

- **show ip route connected**
- **show ip route network**
- **show ip route rip**
- **show ip route igrp**
- **show ip route static**

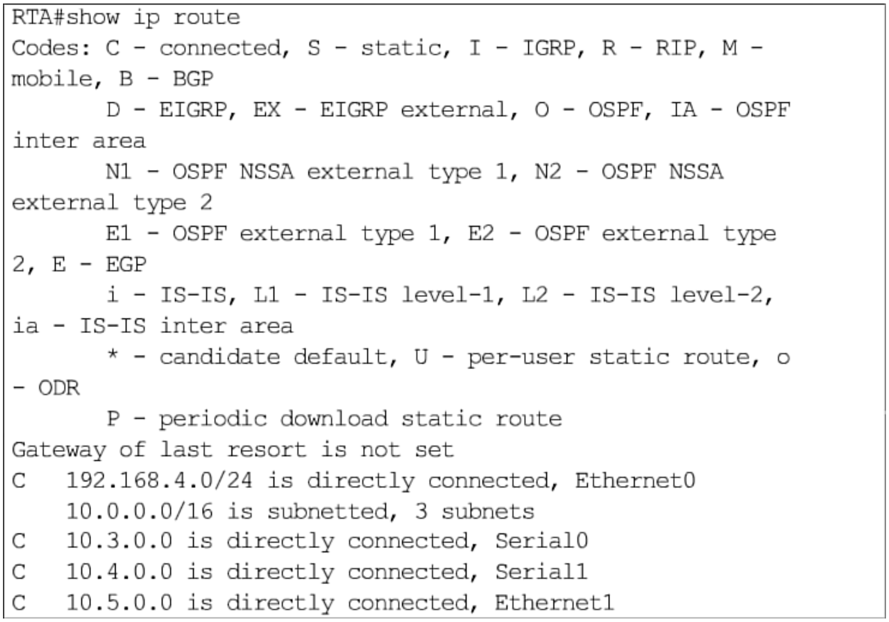
A routing table maps network prefixes to an outbound interface. When RTA receives a packet destined for 192.168.4.46, it looks for the prefix 192.168.4.0/24 in its table. RTA then forwards the packet out an interface (Ethernet0) based on the routing table entry. If RTA receives a packet destined for 10.3.21.5, it sends that packet out Serial 0/0.

The example routing table, shown in Figure 16, shows four routes for directly connected networks. They are labeled with a C, and RTA drops any packet destined for a network that is not listed in the routing table. To forward to other destinations, the routing table for RTA must include more routes. These new routes may be added in one of two ways:

- **Static routing—**An administrator manually defines routes to one or more destination networks.
- **Dynamic routing—**Routers follow rules defined by a routing protocol to exchange routing information and independently select the best path.

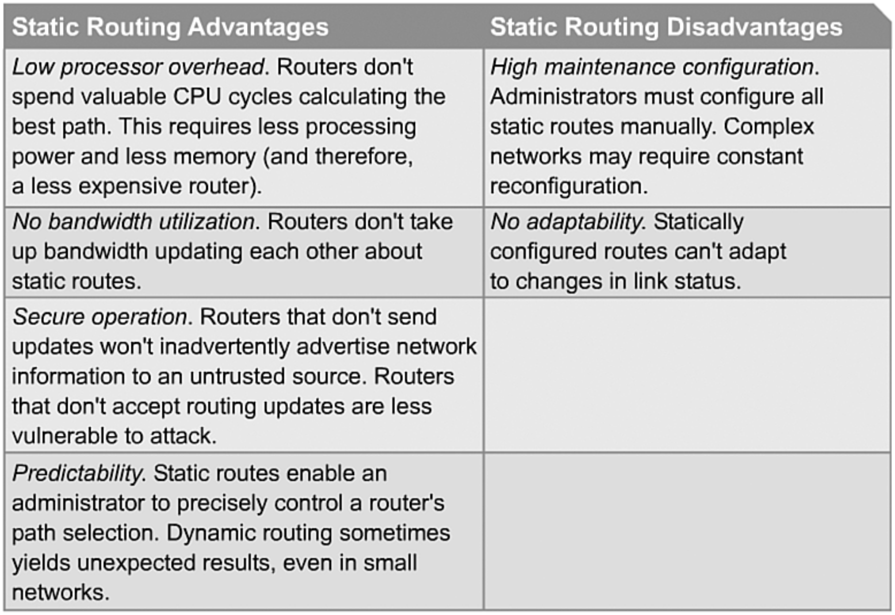
Administratively defined routes are said to be static because they do not change until a network administrator manually programs the changes. Routes learned from other routers are dynamic because they can change automatically as neighboring routers update each other with new information. Each method has fundamental advantages and disadvantages (see Figures 17 and 18).

**Figure 16** The **show ip route** Command



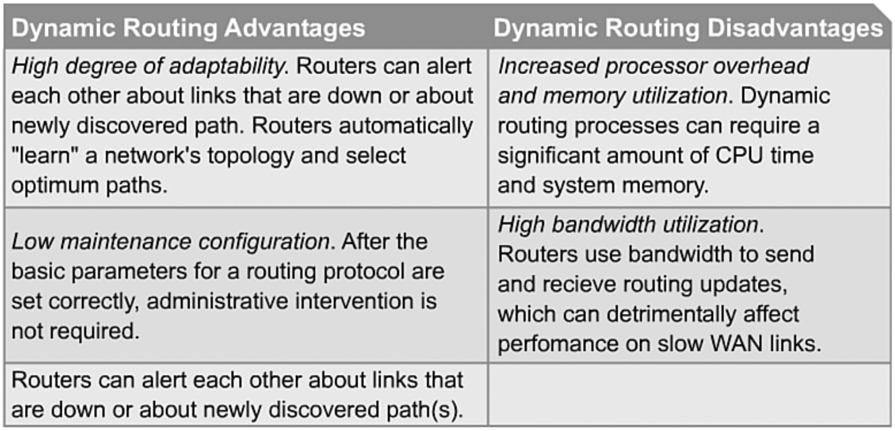
```
RTA#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M -
mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF
inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA
external type 2
       E1 - OSPF external type 1, E2 - OSPF external type
2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2,
ia - IS-IS inter area
       * - candidate default, U - per-user static route, o
- ODR
       P - periodic download static route
Gateway of last resort is not set
C   192.168.4.0/24 is directly connected, Ethernet0
    10.0.0.0/16 is subnetted, 3 subnets
C   10.3.0.0 is directly connected, Serial0
C   10.4.0.0 is directly connected, Serial1
C   10.5.0.0 is directly connected, Ethernet1
```

**Figure 17** Static Routing Advantages and Disadvantages



| Static Routing Advantages | Static Routing Disadvantages |
|---|---|
| *Low processor overhead*. Routers don't spend valuable CPU cycles calculating the best path. This requires less processing power and less memory (and therefore, a less expensive router). | *High maintenance configuration*. Administrators must configure all static routes manually. Complex networks may require constant reconfiguration. |
| *No bandwidth utilization*. Routers don't take up bandwidth updating each other about static routes. | *No adaptability*. Statically configured routes can't adapt to changes in link status. |
| *Secure operation*. Routers that don't send updates won't inadvertently advertise network information to an untrusted source. Routers that don't accept routing updates are less vulnerable to attack. | |
| *Predictability*. Static routes enable an administrator to precisely control a router's path selection. Dynamic routing sometimes yields unexpected results, even in small networks. | |

**Figure 18** Dynamic Routing Advantages and Disadvantages



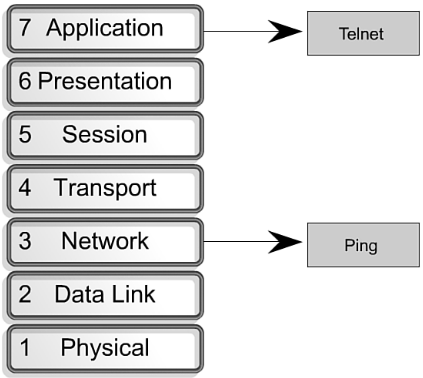
| Dynamic Routing Advantages | Dynamic Routing Disadvantages |
|---|---|
| *High degree of adaptability*. Routers can alert each other about links that are down or about newly discovered path. Routers automatically "learn" a network's topology and select optimum paths. | *Increased processor overhead and memory utilization*. Dynamic routing processes can require a significant amount of CPU time and system memory. |
| *Low maintenance configuration*. After the basic parameters for a routing protocol are set correctly, administrative intervention is not required. | *High bandwidth utilization*. Routers use bandwidth to send and recieve routing updates, which can detrimentally affect perfomance on slow WAN links. |
| Routers can alert each other about links that are down or about newly discovered path(s). | |

## Lesson 9.2: Network Testing

See Chapter 18, “Basic Router Troubleshooting,” of the Cisco Press Companion Guide, Third Edition, for more information.

Basic testing of a network should proceed in sequence from one OSI reference model layer to the next, as shown in Figure 19. It is best to begin with Layer 1 and work to Layer 7, if necessary. Beginning with Layer 1, look for simple problems such as whether power cords are plugged into the wall. The most common problems that occur on IP networks result from errors in the addressing scheme. It is important to test the address configuration before continuing with further configuration steps.

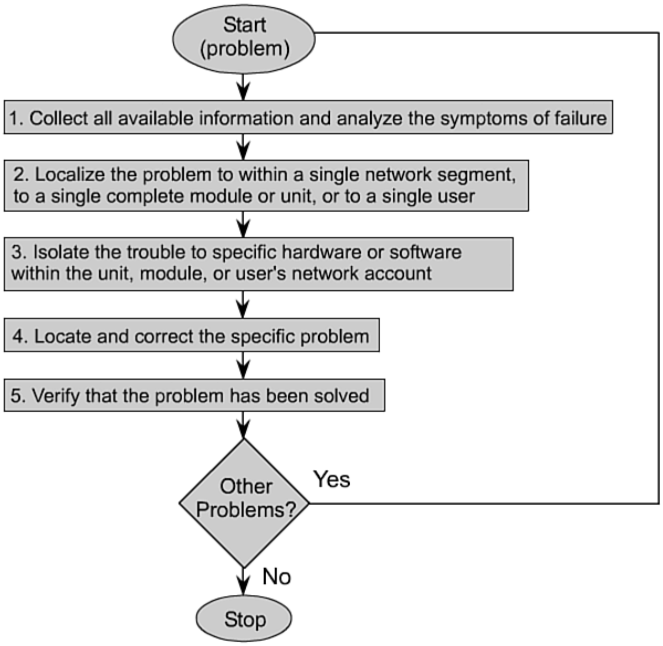
**Figure 19** Testing Process Overview



Each test presented in this section focuses on network operations at a specific layer of the OSI model. **telnet** and **ping** are just two of the commands that enable you to test of a network.

Troubleshooting is a process that enables a user to find problems on a network. Troubleshooting should follow an orderly process based on the networking standards set in place by an administration. Documentation is a very important part of the troubleshooting process, as shown in Figure 20.

**Figure 20** Troubleshooting Steps


Start (problem)
1. Collect all available information and analyze the symptoms of failure
2. Localize the problem to within a single network segment, to a single complete module or unit, or to a single user
3. Isolate the trouble to specific hardware or software within the unit, module, or user's network account
4. Locate and correct the specific problem
5. Verify that the problem has been solved
Other Problems?
Yes
No
Stop

This troubleshooting model follows these steps:

**Step 1** Collect all available information and analyze the symptoms of failure.

**Step 2** Localize the problem to within a single network segment, to a single complete module or unit, or to a single user.

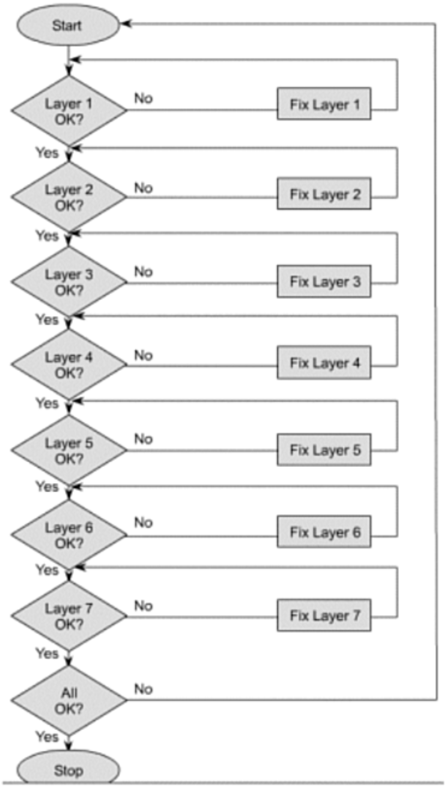
**Step 3** Isolate the trouble to specific hardware or software within the unit, module, or user's network account.

**Step 4** Locate and correct the specific problem.

**Step 5** Verify that the problem has been solved.

Figure 21 shows one approach to troubleshooting. These two concepts are not the only ways to troubleshoot. To keep a network running smoothly and efficiently, however, an orderly troubleshooting process is of utmost importance.

**Figure 21** OSI Layer Troubleshooting



With a structured approach, members of the network know what each member has done in the attempt to solve a problem. A variety of ideas used without any organization results in a chaotic nature to the problem solving. In such cases, very few problems are usually solved.

Testing should begin with Layer 1 of the OSI model and work to Layer 7, if necessary.

Figure 22 shows Layer 1 errors, which may include the following:

- Broken cables
- Disconnected cables
- Cables connected to the wrong ports
- Intermittent cable connection
- Wrong cables used for the task at hand (must use rollovers, crossover cables, and straight-through cables correctly)
- Transceiver problems
- DCE cable problems
- DTE cable problems
- Devices turned off

**Figure 22** Troubleshooting Layer 1

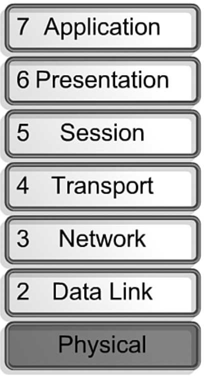


Figure 23 shows Layer 2 errors, which may include the following:

- Improperly configured serial interfaces
- Improperly configured Ethernet interfaces
- Improper encapsulation set (High-Level Data Link Control [HDLC] is the default for serial interfaces.)
- Improper clock rate settings on serial interfaces
- Network interface card (NIC) problems

**Figure 23** Troubleshooting Layer 2

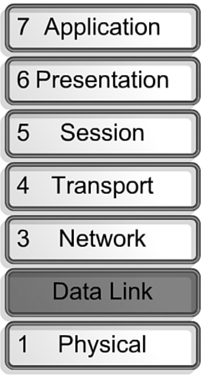
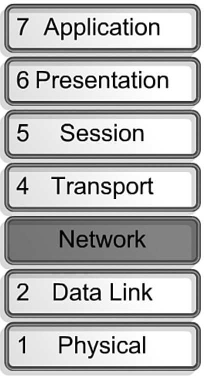


Figure 24 shows Layer 3 errors, which may include the following:

- Routing protocol not enabled
- Wrong routing protocol enabled
- Incorrect IP addresses
- Incorrect subnet masks
- Incorrect DNS-to-IP bindings

**Figure 24** Troubleshooting Layer 3



If errors appear on the network, the process of testing through the OSI layers should begin. **ping** is a command at Layer 3 that may be used to test connectivity. At Layer 7, the **telnet** command enables you to verify the application layer software between source and destination stations. Both of these commands are discussed in detail in a later section.

## Lesson 9.3: Troubleshooting Router Issues Overview

See Chapter 18, “Basic Router Troubleshooting,” of the Cisco Press Companion Guide, Third Edition, for more information.

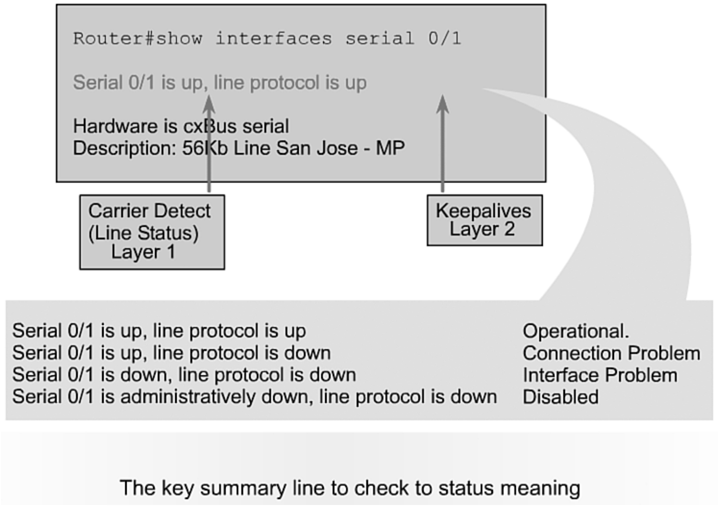
The Cisco IOS contains a rich set of commands for troubleshooting. Among the more widely used are the **show** commands. You can view every aspect of the router with one or more of the **show** commands. The **show** command used to check the status and statistics of the interfaces is the **show interfaces** command. You can use variations of this command to check the status of the different types of interfaces. To view the status of the Fast Ethernet interfaces, use **show interfaces FastEthernet**. You can also use the command to view the status of one particular interface. To view the status of Serial 0/0, for instance, use **show interface serial0/0**.

The **show interfaces** command enables you to view the status of two important portions of the interfaces: the physical (hardware) portion and logical (software) portion. These can be related to the Layer 1 and the Layer 2 functions.

The hardware includes cables, connectors, and interfaces showing the condition of the physical connection between the devices. The software status shows the state of messages that are passed between adjacent devices (messages such as keepalives, control information, and user information). This messaging relates to the condition of a data link layer protocol passed between two connected, neighboring router interfaces.

These important elements of the **show interfaces serial** command output are displayed as the line and data-link protocol status, as shown in Figure 25.

**Figure 25** Interpreting **show interfaces serial** Output

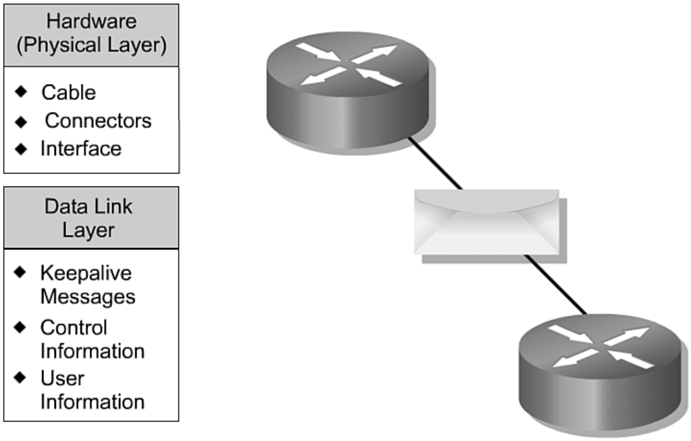


```
Router#show interfaces serial 0/1

Serial 0/1 is up, line protocol is up

Hardware is cxBus serial
Description: 56Kb Line San Jose - MP
```

```
Serial 0/1 is up, line protocol is up                          Operational.
Serial 0/1 is up, line protocol is down                        Connection Problem
Serial 0/1 is down, line protocol is down                      Interface Problem
Serial 0/1 is administratively down, line protocol is down     Disabled
```

The **show interfaces** command is perhaps the single most important tool to discover Layer 1 and Layer 2 problems with the router. The first parameter (**line**) refers to the physical layer. The second parameter (**protocol**) indicates whether the IOS processes that control the line protocol consider the interface usable. This usability is determined by whether keepalives are successfully received. If the interface misses three consecutive keepalives, the line protocol is marked as down, as shown in Figure 26.

**Figure 26** Is the Link Operational?



Cisco Discovery Protocol (CDP) advertises device information to its direct neighbors, including MAC and IP addresses and outgoing interfaces.

The output from the **show cdp neighbors** command displays information about directly connected neighbors. This information is useful for debugging connectivity issues. If you suspect a cabling problem, enable the interfaces with the **no shutdown** command and then execute the **show cdp neighbor detail** command before any other configuration. The command displays specific device detail, such as the active interfaces, the port ID, and the device. The version of Cisco IOS that is running on the remote devices also displays.

The **traceroute** command enables you to discover the routes that packets take when traveling to their destination. You can also use **traceroute** to test the network layer (Layer 3) on a hop-by-hop basis and to provide performance benchmarks.

The output of the **traceroute** command generates a list of hops that were successfully reached. If the data successfully reaches the intended destination, the output indicates every router that the datagram passes through. You can capture this output and use it for future troubleshooting of the internetwork.

**traceroute** output also indicates the specific hop at which the failure occurs. For each router in the path, a line of output is generated on the terminal indicating the IP address of the interface that the data entered. If an asterisk (*) appears, the packet failed. By obtaining the last good hop from the **traceroute** output and comparing it to a diagram of the internetwork, you can isolate the problem area.

**traceroute** also provides information indicating the relative performance of links. The round-trip time (RTT) is the time required to send an echo packet and get a response. This information enables you to approximate the length of the delay on the link. These figures are not precise enough to be used for an accurate performance evaluation. However, you can capture this output and use it for future performance troubleshooting of the internetwork.

The **show ip protocols** and **show ip route** commands display information about routing protocols and the routing table. You can use the output from these commands to verify the routing protocol configuration.

The **show ip route** command is perhaps the single most important command for troubleshooting routing issues. This command displays the contents of the IP routing table. Its output shows the entries for all known networks and subnetworks and how that information was learned.

Very often routers are remotely configured or troubleshot, and it is not possible to physically inspect the router connections. The **show controllers serial** command enables you to determine the type of cable connected without inspecting the cables.

By examining the **show controllers serial** command output, you can determine the type of cable that the controller detects. This information proves useful for finding a serial interface with no cable, the wrong type of cable, or a defective cable.

The **show controllers serial** command queries the integrated circuit (chip) that controls the serial interfaces and displays information about the physical interface. This output varies from controller chip to controller chip. Even within a router type, different controller chips may be used.

## Module 11—Access Lists

### Lesson 11.1: Access Control List Fundamentals

See Chapter 19, "Intermediate TCP," of the Cisco Press Companion Guide, Third Edition, for more information.

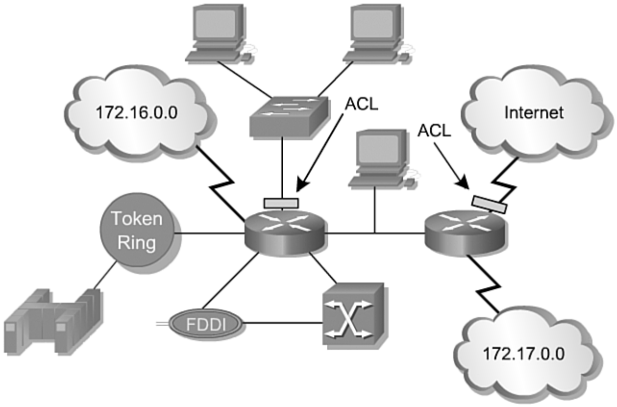
Network administrators must figure out how to deny unwanted access to the network while allowing internal users appropriate access to necessary services. Although security tools, such as passwords, callback equipment, and physical security devices are helpful, they often lack the flexibility of basic traffic filtering and the specific controls most administrators prefer. For example, a network administrator might want to allow users access to the Internet but might not want external users to use telnet to access the LAN.

Routers provide basic traffic-filtering capabilities, such as blocking Internet traffic, with access control lists (ACLs). An ACL is a sequential list of **permit** or **deny** statements that apply to addresses or upper-layer protocols. This lesson explains how to use standard and extended ACLs as a means to control network traffic and how ACLs are used as part of a security solution.

In addition, this lesson includes tips, considerations, recommendations, and general guidelines on how to use ACLs, including the commands and configurations needed to create ACLs. This lesson also provides examples of standard and extended ACLs and discusses how to apply ACLs to router interfaces.

ACLs are lists of conditions that are applied to traffic traveling across a router's interface, as shown in Figure 27. These lists tell the router what types of packets to accept or deny. Acceptance and denial can be based on specified conditions. ACLs enable management of traffic and secure access to and from a network.

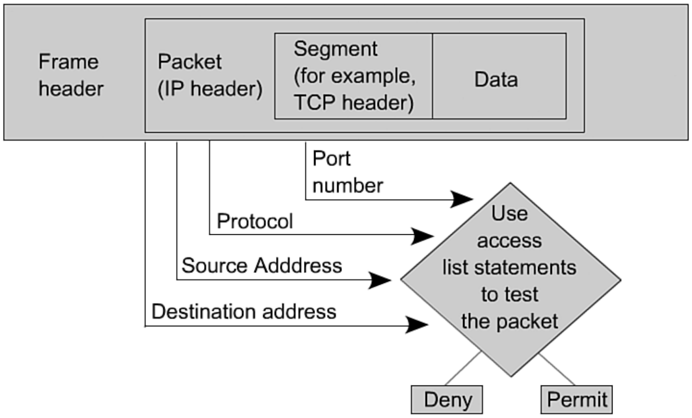
**Figure 27** ACL



ACLs can be created for all routed network protocols, such as Internet Protocol (IP) and Internetwork Packet Exchange (IPX). ACLs can be configured at the router to control access to a network or subnet.

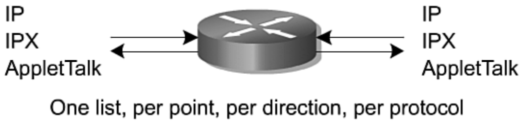
ACLs filter network traffic by controlling whether routed packets are forwarded or blocked at the router's interfaces, as shown in Figure 28. The router examines each packet to determine whether to forward or drop it, based on the conditions specified in the ACL. Some ACL decision points are source and destination addresses, protocols, and upper-layer port numbers.

**Figure 28** ACLs Checking Packet Headers



ACLs must be defined on a per-protocol, per-direction, per-port basis, as shown in Figure 29. To control traffic flow on an interface, an ACL must be defined for each protocol enabled on the interface. ACLs control traffic in only one direction on an interface; so for every protocol, two access lists need to be created (inbound and outbound). Finally, every interface can have multiple protocols and directions defined. If the router has two interfaces configured for IP, AppleTalk, and IPX, at least 12 separate ACLs are needed: one ACL for each protocol, times two, for direction in and out, times two for the number of ports.

**Figure 29** Access List Groupings in a Router



With two interfaces and three protocols running, this router could have a total of 12 separate ACLs.

The following are some of the primary reasons to create ACLs:

- Limit network traffic and increase network performance. By restricting video traffic, for instance, ACLs could greatly reduce the network load and consequently increase network performance.

- Provide traffic flow control. ACLs can restrict the delivery of routing updates. If updates are not required, because of network conditions, bandwidth is preserved.
- Provide a basic level of security for network access. ACLs can allow one host to access a part of the network and prevent another host from accessing the same area. Host A is allowed to access the Human Resources network, for example, and Host B is prevented from accessing it.
- Decide which types of traffic are forwarded or blocked at the router interfaces. Permit e-mail traffic to be routed but at the same time block all telnet traffic.
- Allow an administrator to control which areas a client can access on a network.
- Screen certain hosts either to allow or deny access to part of a network.
- Grant or deny user permission to access only certain types of files, such as FTP or HTTP.

If ACLs are not configured on the router, all packets passing through the router are allowed onto all parts of the network.

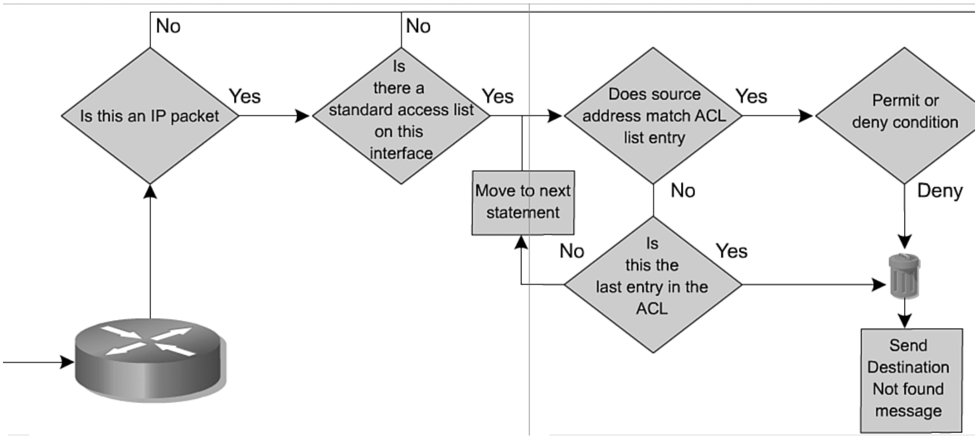
## Lesson 11.2: Access Control Lists

See Chapter 19, "Intermediate TCP," of the Cisco Press Companion Guide, Third Edition, for more information.

Access control lists (ACLs) can be as simple as a single line intended to permit packets from a specific host, or they can be extremely complex sets of rules and conditions that can precisely define traffic and shape the performance of router processes. Many of the advanced uses of ACLs are beyond the scope of this course, but this lesson does cover standard and extended ACLs, the proper placement of ACLs, and some special applications of ACLs.

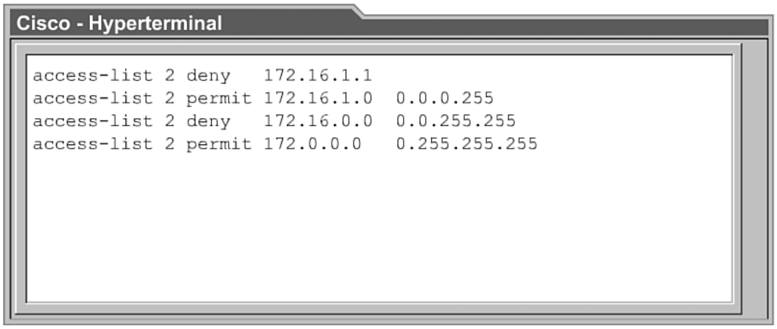
Standard ACLs check the source address of IP packets that are routed, as shown in Figure 30. The comparison results in either permit or deny access for an entire protocol suite, based on the network, subnet, and host addresses. For example, packets coming in Fa0/0 are checked for source address and protocol. If they are permitted, the packets are routed through the router to an output interface. If they are not permitted, they are dropped at the incoming interface.

**Figure 30** Standard ACL


No
No
Is this an IP packet
Yes
Is there a standard access list on this interface
Yes
Does source address match ACL list entry
Yes
Permit or deny condition
Move to next statement
No
Deny
No
Is this the last entry in the ACL
Yes
Send Destination Not found message

The standard version of the **access-list** global configuration enables you to define a standard ACL with a number in the range of 1 to 99, as shown in Figure 31. In the first ACL statement, notice that there is no wildcard mask. In this case where no list is shown, the default mask is used: 0.0.0.0.

**Figure 31** Standard ACL Statements

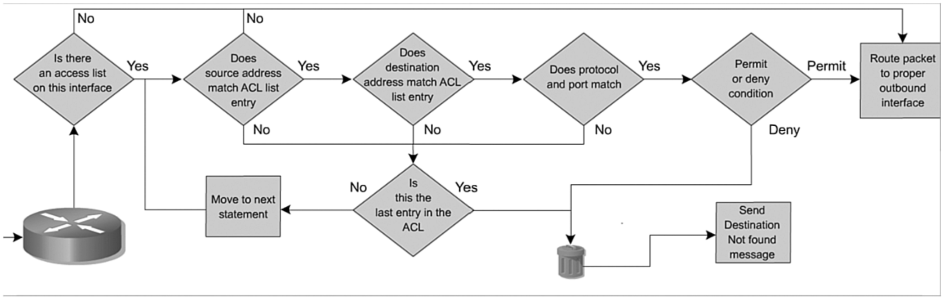


```
access-list 2 deny   172.16.1.1
access-list 2 permit 172.16.1.0  0.0.0.255
access-list 2 deny   172.16.0.0  0.0.255.255
access-list 2 permit 172.0.0.0   0.255.255.255
```

- Access list number range of 1-99
- Filter only on source IP address
- Wildcard masks
- Applied to port closest to destination

Extended ACLs are used more often than standard ACLs because they provide a greater range of control, as shown in Figure 32. Extended ACLs check the source and destination packet addresses and can check for protocols and port numbers (giving you greater flexibility to describe what the ACL will check). Packets can be permitted or denied access based on where the packet originated and its destination as well as protocol type and port addresses. An extended ACL can allow e-mail traffic from Fa0/0 to specific S0/0 destinations, while denying file transfers and web browsing. When packets are discarded, some protocols send an echo packet to the sender, stating that the destination was unreachable.

**Figure 32** Extended ACL


No
No
Is there an access list on this interface
Yes
Does source address match ACL list entry
Yes
Does destination address match ACL list entry
Yes
Does protocol and port match
Yes
Permit or deny condition
Permit
Route packet to proper outbound interface
No
No
No
Deny
No
Is this the last entry in the ACL
Yes
Move to next statement
Send Destination Not found message

IP named ACLs were introduced in Cisco IOS Software Release 11.2, allowing standard and extended ACLs to be given names rather than numbers. A named access list provides the following advantages:

- Intuitively identify an ACL using an alphanumeric name.
- Eliminate the limit of 99 simple and 100 extended ACLs.
- Modify ACLs without deleting and then reconfiguring them. (Note that a named access list will allow the deletion of statements but will only allow for statements to be inserted at the end of a list.)

# CCNA3

## Module 1—Introduction to Classless Routing

### Lesson 1.1: Variable-Length Subnet Masks (VLSM)

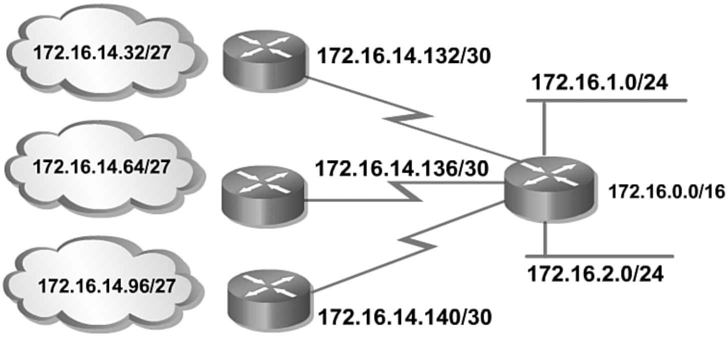
See Chapter 2, "Introduction to Classless Routing," of the Cisco Press Companion Guide, Third Edition, for more information.

A network administrator must anticipate and manage the physical growth of a network, perhaps by buying or leasing another floor of the building to house new networking equipment such as racks, patch panels, switches, and routers. The network designer must choose an addressing scheme that allows for growth. Variable-length subnet masking (VLSM) is a technique that allows for the creation of efficient, scalable addressing schemes.

Variable-length subnet masks (VLSMs) were developed to allow multiple levels of subnetworked IP addresses within a single network. You can use this strategy only when it is supported by the routing protocol in use, such as Open Shortest Path First (OSPF) and Enhanced Interior Gateway Routing Protocol (EIGRP). RIP version 1 is older than VLSM and cannot support it. RIP version 2, however, can support VLSM.

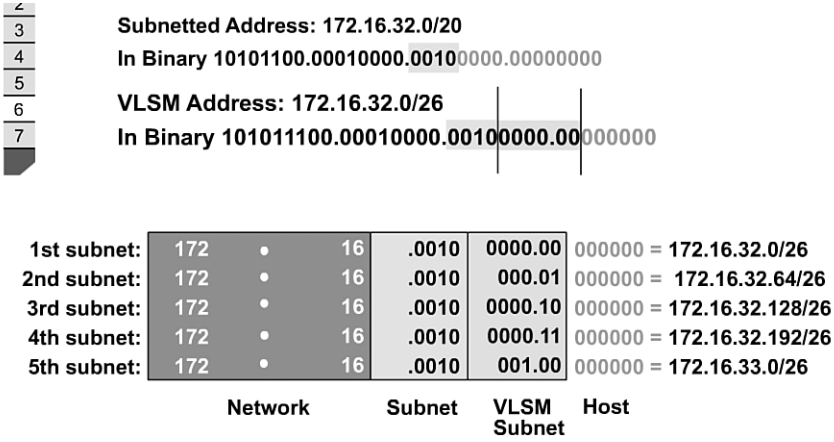
As IP subnets have grown, administrators have looked for ways to use their address space more efficiently. One technique is called variable-length subnet masks (VLSMs). VLSM allows an organization to use more than one subnet mask within the same network address space. VLSM enables an administrator to "subnet a subnet," and it can be used to maximize addressing efficiency, as shown in Figures 33 and 34.

**Figure 33** What Is a Variable-Length Subnet Mask?



- Subnet 172.16.14/024 is divided into smaller subnets:
- Subnet with one mask (/27)
- Then further subnet one of the unused /27 subnets into mutiple /30 subnets

**Figure 34** Calculating VLSMs



Subnetted Address: 172.16.32.0/20

In Binary 10101100.00010000.00100000.00000000

VLSM Address: 172.16.32.0/26

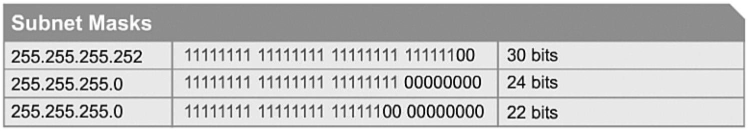
In Binary 101011100.00010000.00100000.00000000

| | Network | | | Subnet | VLSM Subnet | Host |
|---|---|---|---|---|---|---|
| 1st subnet: | 172 | • | 16 | .0010 | 0000.00 | 000000 = 172.16.32.0/26 |
| 2nd subnet: | 172 | • | 16 | .0010 | 000.01 | 000000 = 172.16.32.64/26 |
| 3rd subnet: | 172 | • | 16 | .0010 | 0000.10 | 000000 = 172.16.32.128/26 |
| 4th subnet: | 172 | • | 16 | .0010 | 0000.11 | 000000 = 172.16.32.192/26 |
| 5th subnet: | 172 | • | 16 | .0010 | 001.00 | 000000 = 172.16.33.0/26 |

Within an autonomous system, most routing protocols insist that every network use the same subnet mask. Therefore, if 192.168.187.0, 192.168.188.0, and 192.168.200.0 are all in IGRP autonomous system number 2, these networks must all agree upon *one* subnet mask, such as 255.255.255.0.

VLSM is simply a feature that allows a single autonomous system to have networks with different subnet masks. If a routing protocol allows VLSM, use a 30-bit subnet mask on network connections, 255.255.255.252; a 24-bit mask for user networks, 255.255.255.0; or even a 22-bit mask, 255.255.252.0, for networks with up to 1000 users, as shown in Figure 35.

**Figure 35** Subnet Masks



| Subnet Masks | | |
|---|---|---|
| 255.255.255.252 | 11111111 11111111 11111111 11111100 | 30 bits |
| 255.255.255.0 | 11111111 11111111 11111111 00000000 | 24 bits |
| 255.255.255.0 | 11111111 11111111 11111100 00000000 | 22 bits |

## Lesson 1.2: RIP Version 2

See Chapter 2, “Introduction to Classless Routing,” of the Cisco Press Companion Guide, Third Edition, for more information.

Networks must be scalable to meet the changing needs of users. When a network is scalable, it can grow in a logical, efficient, and cost-effective way. Which routing protocol is used in a network does much to determine the scalability of the network. Therefore, it is important that the routing protocol be chosen wisely. The Routing Information Protocol (RIP) is still considered suitable for very small networks but is not scalable to large networks because of many inherent limitations. To overcome these limitations yet maintain the simplicity of RIP version 1 (RIPv1), RIP version 2 (RIPv2) was developed.

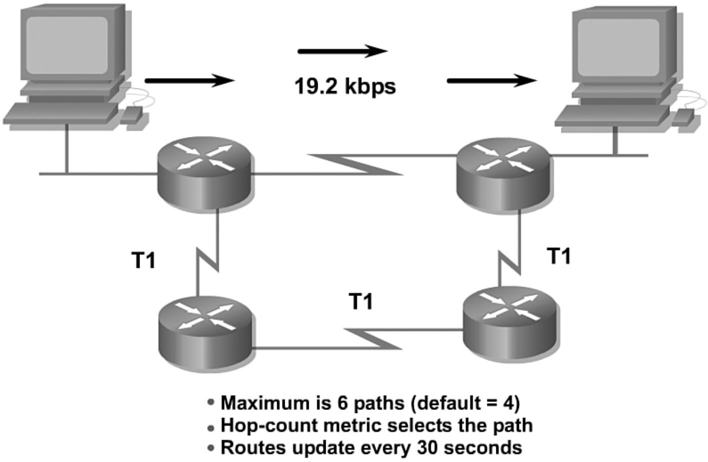
Students completing this lesson should be able to

- Identify the key features of RIPv1 and RIPv2.
- Identify the important differences between RIPv1 and RIPv2.
- Configure RIPv2.
- Verify and troubleshoot RIPv2 operation.

The Internet is a collection of autonomous systems. Each autonomous system is generally administered by a single entity. Each autonomous system has its own routing technology, which may differ from other autonomous systems. The routing protocol used within an autonomous system is referred to as an Interior Gateway Protocol (IGP). A separate protocol, called an Exterior Gateway Protocol (EGP), is used to transfer routing information among autonomous systems. RIP was designed to work as an IGP in a moderate-sized autonomous system and is not intended for use in more complex environments.

RIPv1, shown in Figure 36, is considered an IGP that is classful. RIPv1 is a distance vector protocol that broadcasts its entire routing table to each neighbor router at predetermined intervals, such as 30-second intervals. RIP uses hop count as a metric, with 15 as the maximum number of hops.

**Figure 36** History of RIP


19.2 kbps
T1
T1
T1
• Maximum is 6 paths (default = 4)
• Hop-count metric selects the path
• Routes update every 30 seconds

If the router receives information about a network, and the receiving interface belongs to the same network but is on a different subnet, the router applies the one subnet mask that is configured on the receiving interface.

For Class A addresses, the default classful mask is 255.0.0.0.

For Class B addresses, the default classful mask is 255.255.0.0.

For Class C addresses, the default classful mask is 255.255.255.0.

RIPv1 is a popular routing protocol because virtually all IP routers support it. The popularity of RIPv1 is based on the simplicity and the universal compatibility it demonstrates. RIPv1 is capable of load balancing over as many as six equal-cost paths; the default is four paths.

RIPv1 has the following limitations:

- It does not send subnet masks information in its updates.
- It sends updates as broadcasts on 255.255.255.255.
- It does not support authentication.
- It is not able to support VLSM or classless interdomain routing (CIDR).

RIPv2, an improved version of RIPv1, shares the following features with RIPv1:

- It is a distance vector protocol that uses a hop-count metric.
- It uses hold-down timers to prevent routing loops; the default is 180 seconds.

- It uses split horizon to prevent routing loops.
- It uses 16 hops as a metric for infinite distance.

RIPv2 provides prefix routing, which allows it to send out subnet mask information with the route update. Therefore, RIPv2 supports the use of classless routing in which different subnets within the same network can use different subnet masks and VLSM.

RIPv2 provides for authentication in its updates. A set of keys can be used on an interface as an authentication check. RIPv2 allows for a choice of the type of authentication to be used in RIPv2 packets. The choice can be either clear text or MD5 encryption. Clear text is the default. MD5 can be used to authenticate the source of a routing update. MD5 is typically used to encrypt enable secret passwords, and it has no known reversal.

RIPv2 multicasts routing updates using the Class D address 224.0.0.9, which provides for better efficiency.

## Module 2—Single-Area OSPF

### Lesson 2.2: Single-Area OSPF Concepts

See Chapter 3, "Single-Area OSPF," of the Cisco Press Companion Guide, Third Edition, for more information.

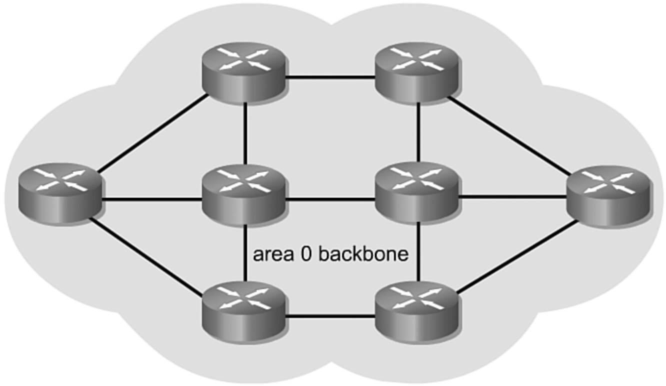
Link-state routing protocols differ from distance vector protocols. Link-state protocols flood link-state information and so allow every router to have a complete view of the network topology. Triggered updates allow efficient use of bandwidth and faster convergence because the news of the change in the state of a link is sent to all routers in the network as soon as the change happens.

One of the most important link-state protocols is Open Shortest Path First (OSPF). As should be apparent from its name, OSPF is based on open standards, which means it can be developed and improved by multiple vendors. Although it is a complex protocol that can be quite challenging to implement in a large network, the basics of OSPF are fairly straightforward and are the subject of this lesson.

Open Shortest Path First (OSPF) is a link-state routing protocol based on open standards. It is described in several standards of the Internet Engineering Task Force (IETF). The most recent description is RFC 2328. The "Open" in OSPF means that it is open to the public and is nonproprietary.

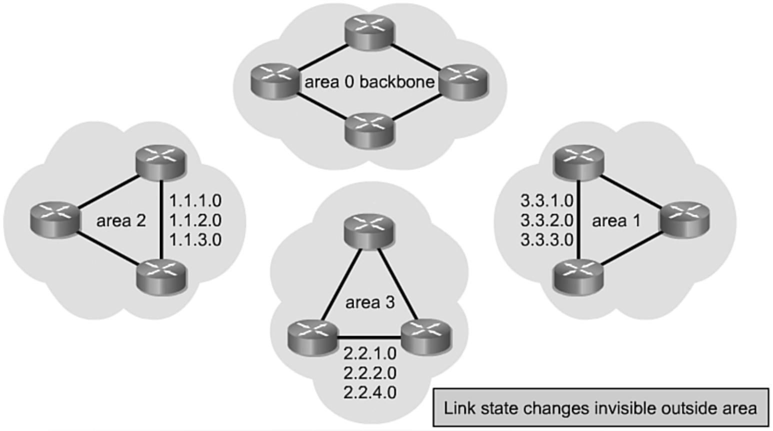
OSPF is becoming the preferred IGP when compared with RIPv1 and RIPv2 because it is scalable. RIP cannot scale beyond 15 hops, it converges slowly, and it can choose slow routes as it ignores critical factors such as bandwidth in route determination. OSPF deals with these limitations and has been proven to be a robust and scalable routing protocol suitable for the networks of today. OSPF can be used and configured as a single area, as shown in Figure 37, for small networks. It can also be used for large networks. OSPF routing scales to large networks if hierarchical network design principles are used, as shown in Figure 38.

**Figure 37** Single-Area OSPF Network



Large OSPF networks are hierarchical and divided into multiple areas.

**Figure 38** Single-Area OSPF Network



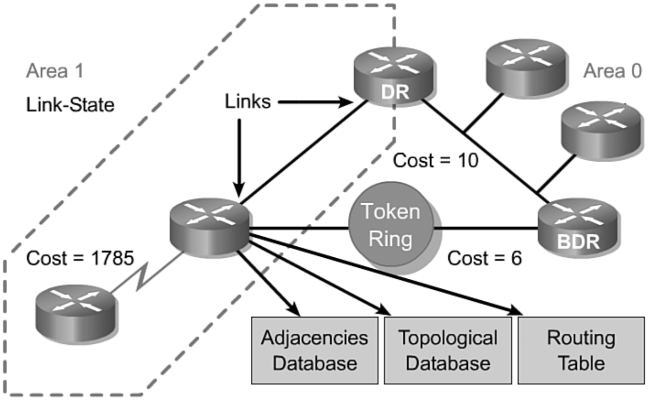
Large OSPF networks are hierarchical and divided into multiple areas.

Large OSPF networks use hierarchical design. Multiple areas connect to a distribution area, area 0, also called the *backbone*. This design approach allows for extensive control of routing updates. Defining areas reduces routing overhead, speeds up convergence, confines network instability to an area, and improves performance.

## OSPF Terminology

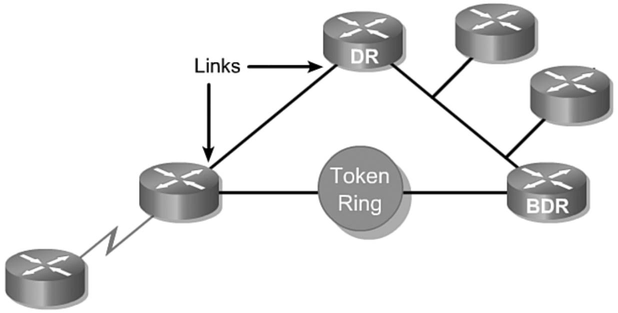
As a link-state protocol, OSPF operates differently than distance vector routing protocols. Link-state routers identify neighboring routers and then communicate with the identified neighbors. OSPF comes with a new set of terms. Figure 39 lists these new terms.

**Figure 39** OSPF Terminology



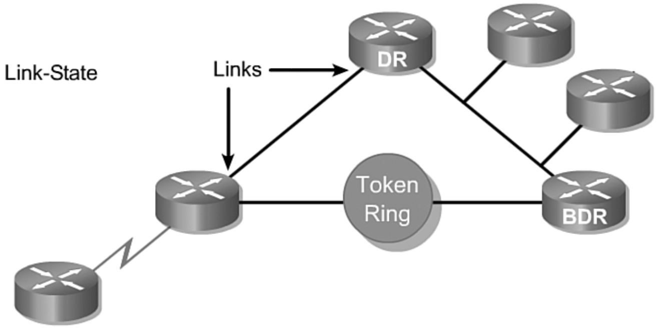
Information is gathered from OSPF neighbors about the status, or links, of each OSPF router, as shown in Figure 40. This information is flooded to all its neighbors. Flooding is a process that sends information out all ports, with the exception of the port on which the information was received. An OSPF router advertises its own link states, as shown in Figure 41, and passes on received link states.

**Figure 40** OSPF Terminology



**Link:** An interface on a router.

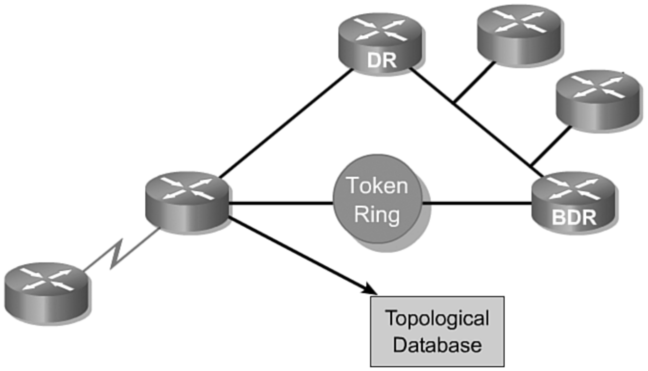
**Figure 41** OSPF Terminology



**Link-State:** The status of a link between two routers. Also a router's interface and its relationship to its neighboring routers.

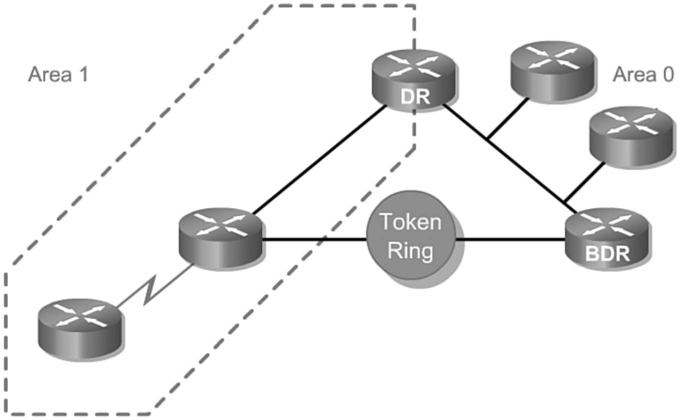
The routers process the information about link states and build a link-state database, as shown in Figure 42. Every router in the OSPF area has the same link-state database, as shown in Figure 43. Every router has the same information about the state of the links and the neighbors of every other router.

**Figure 42** OSPF Terminology



**Link-state database (or topological database):** A list of information about all other routers in the internetwork. It shows the internetwork topology.

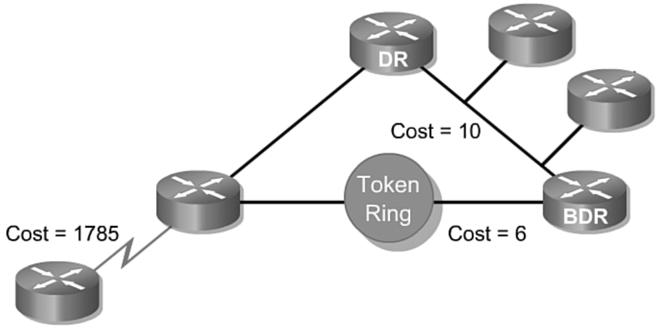
**Figure 43** OSPF Terminology



**Area:** A collection of networks and routers that has the same area identification. Each router within an area has the same link-state information. A router within an area is called an internal router.

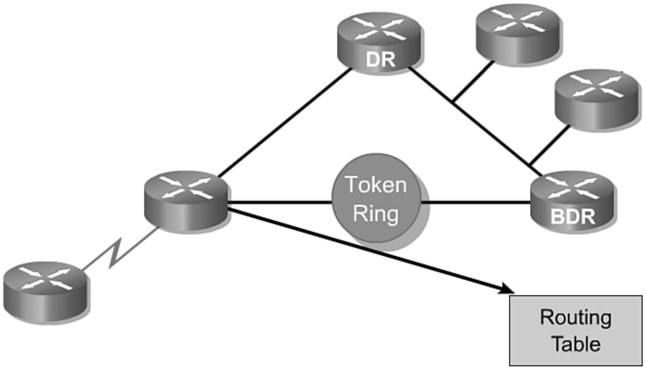
Each router then runs the SPF algorithm on its own copy of the database. This calculation determines the best route to a destination. The SPF algorithm adds up the cost, which is a value that is usually based on bandwidth, as shown in Figure 44. The lowest-cost path is added to the routing table, which is also known as the *forwarding database*, as shown in Figure 45.

**Figure 44** OSPF Terminology



**Cost:** The value assigned to a link. Rather than hops, link-state protocols assign a cost to a link, which is based on the speed of the media.

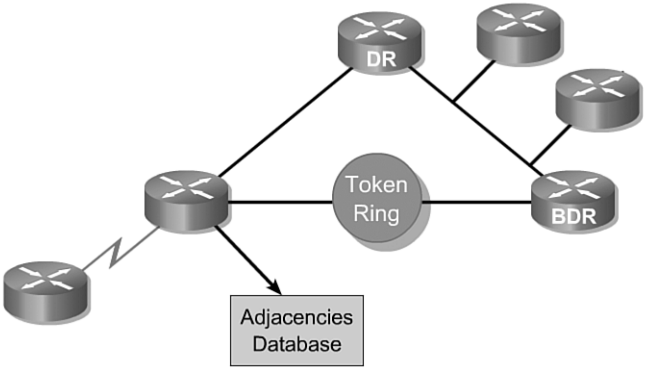
**Figure 45** OSPF Terminology



**Routing table:** The routing table (also known as forwarding database) generated when an algorithm is run on the link-state database. Each router's routing table is unique.

OSPF routers record information about their neighbors in the *adjacency database*, as shown in Figure 46.

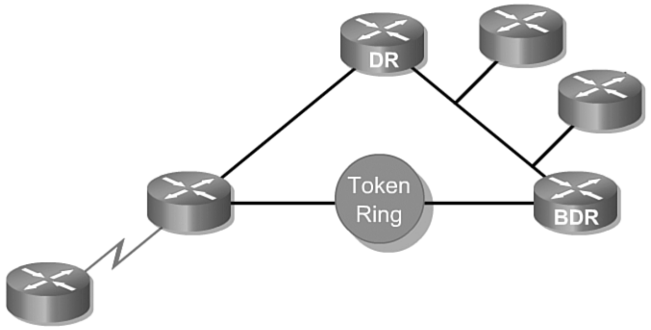
**Figure 46** OSPF Terminology



**Adjacencies database:** A listing of all the neighbors to which a router has established bidirectional communication.

To reduce the number of exchanges of routing information among several neighbors on the same network, OSPF routers elect a designated router (DR) and a backup designated router (BDR) that serve as focal points for routing information exchange, as shown in Figure 47.

**Figure 47** OSPF Terminology



**Designated router (DR) and backup designated router (BDR):** A router that is elected by all other routers on the same LAN to represent all the routers. Each network has a DR and BDR.

## Lesson 2.3: Single-Area OSPF Configuration

See Chapter 3, "Single-Area OSPF," of the Cisco Press Companion Guide, Third Edition, for more information.

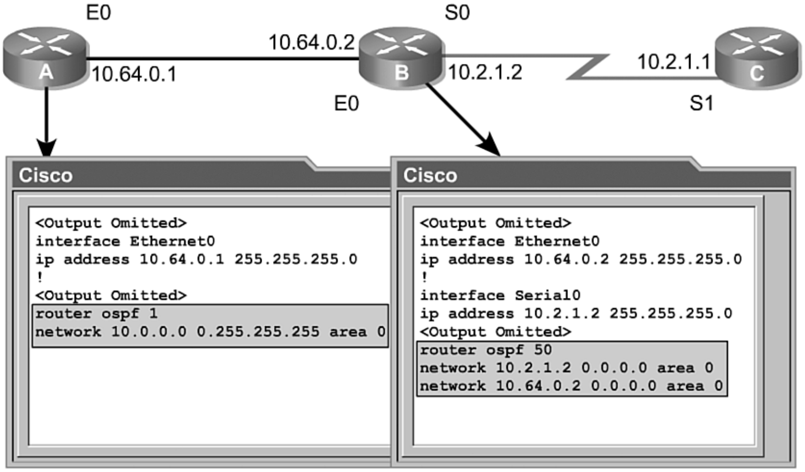
OSPF configuration on a Cisco router is in many ways much like the configuration of other routing protocols. As with other routing protocols, the OSPF routing process must be enabled and networks must be identified that will be announced by OSPF. However, OSPF has a number of features and configuration procedures that are unique to it. These features make OSPF a powerful choice for a routing protocol, but they can also make OSPF configuration a very challenging proposition.

In large, complex networks, OSPF can be configured to span many areas and several different area types. The ability to design and implement large OSPF networks begins with the ability to configure OSPF in a single area. This lesson focuses on just that: configuration of single-area OSPF.

OSPF routing uses the concept of areas. Each router contains a complete database of link states in a specific area. If the OSPF network has only one area, that area is numbered 0 and known as *area 0*. In multi-area OSPF networks, all areas are required to connect to area 0. Area 0 is also called the *backbone area*.

To use OSPF, you must configure it on the router and include network addresses and area information, as shown in Figure 48. Network addresses are configured with a wildcard mask and not a subnet mask. The wildcard mask represents the links or host addresses that can be present in this segment. You can write area IDs as a whole number or in dotted-decimal notation.

**Figure 48** Basic OSPF Configuration



```
<Output Omitted>
interface Ethernet0
ip address 10.64.0.1 255.255.255.0
!
<Output Omitted>
router ospf 1
network 10.0.0.0 0.255.255.255 area 0
```

```
<Output Omitted>
interface Ethernet0
ip address 10.64.0.2 255.255.255.0
!
interface Serial0
ip address 10.2.1.2 255.255.255.0
<Output Omitted>
router ospf 50
network 10.2.1.2 0.0.0.0 area 0
network 10.64.0.2 0.0.0.0 area 0
```

To enable OSPF routing, use the following global configuration command syntax:

```
Router(config)#router ospf process-id
```

The *process-id* refers to a number that is used to identify an OSPF routing process on the router. Multiple OSPF processes can be started on the same router. The number can be any value between 1 and 65,535. Most network administrators keep the same process ID throughout an autonomous system, but this is not a requirement. It is rarely necessary to run more than one OSPF process on a router. IP networks are advertised as follows in OSPF:

```
Router(config-router)#network address wildcard-mask area area-id
```

Each network must be identified with the area to which it belongs. The network address can be a whole network, a subnet, or the address of the interface. *wildcard mask* represents the set of host addresses that the segment supports. This differs from a subnet mask, which is used when configuring IP addresses on interfaces.

## Module 3—EIGRP

### Lesson 3.1: EIGRP Concepts

See Chapter 4, "Enhanced Interior Gateway Routing Protocol," of the Cisco Press Companion Guide, Third Edition, for more information.

Enhanced Interior Gateway Routing Protocol (EIGRP) is a Cisco proprietary routing protocol based on Interior Gateway Routing Protocol (IGRP).

Unlike IGRP, which is a classful routing protocol, EIGRP supports classless interdomain routing (CIDR), enabling network designers to maximize address space by using CIDR and variable-length subnet masking (VLSM). Compared to IGRP, EIGRP boasts faster convergence times, improved scalability, and superior handling of routing loops.

Furthermore, EIGRP can replace Novell Routing Information Protocol (RIP) and AppleTalk Routing Table Maintenance Protocol (RTMP), serving both IPX and AppleTalk networks with powerful efficiency.

EIGRP is often described as a hybrid routing protocol offering the best of distance vector and link-state algorithms. Technically, EIGRP is an advanced distance vector routing protocol that relies on features commonly associated with link-state protocols. Some of the best features of OSPF, such as partial updates and neighbor discovery, are similarly put to use by EIGRP. However, EIGRP is easier to configure than OSPF.

### Comparing EIGRP with IGRP

Cisco released EIGRP in 1994 as a scalable, improved version of its proprietary distance vector routing protocol, IGRP. The same distance vector technology found in IGRP is used in EIGRP, and the underlying distance information remains the same.

The convergence properties and the operating efficiency have improved significantly, resulting in an improved architecture while retaining the existing investment in IGRP.

Comparisons between EIGRP and IGRP fall into the following major categories:

- Compatibility mode
- Metric calculation
- Hop count
- Automatic protocol redistribution
- Route tagging

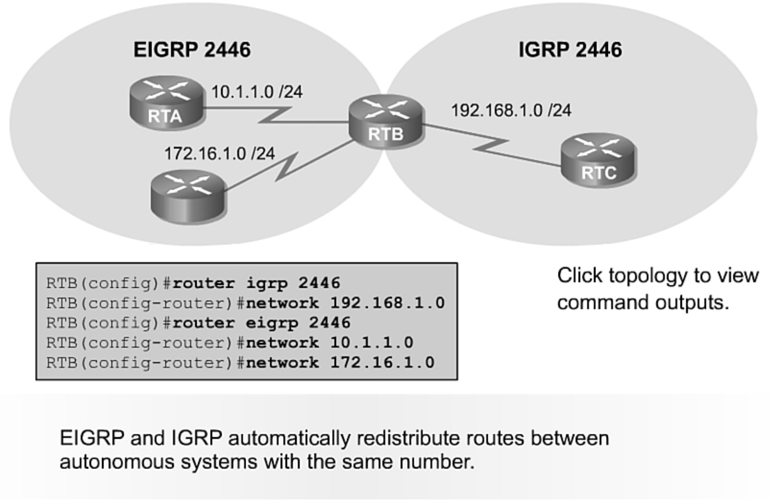
IGRP and EIGRP are compatible with each other. This compatibility provides seamless interoperability with IGRP routers. This interoperability is important because it enables users to take advantage of the benefits of both protocols. EIGRP offers multiprotocol support, but IGRP does not.

EIGRP and IGRP use different metric calculations. EIGRP scales the metric of IGRP by a factor of 256 (because EIGRP uses a metric that is 32 bits long, and IGRP uses a 24-bit metric). By multiplying or dividing by 256, EIGRP can easily exchange information with IGRP.

EIGRP also imposes a maximum hop limit of 224. This is more than adequate to support the largest, properly designed internetworks. IGRP has a higher hop-count limit: 255.

Enabling dissimilar routing protocols such as OSPF and RIP to share information requires advanced configuration. However, sharing, or redistribution, is automatic between IGRP and EIGRP as long as both processes use the same autonomous system number. In Figure 49, RTB automatically redistributes EIGRP-learned routes to the IGRP autonomous system and vice versa.

**Figure 49** Using EIGRP with IGRP



```
RTB(config)#router igrp 2446
RTB(config-router)#network 192.168.1.0
RTB(config)#router eigrp 2446
RTB(config-router)#network 10.1.1.0
RTB(config-router)#network 172.16.1.0
```

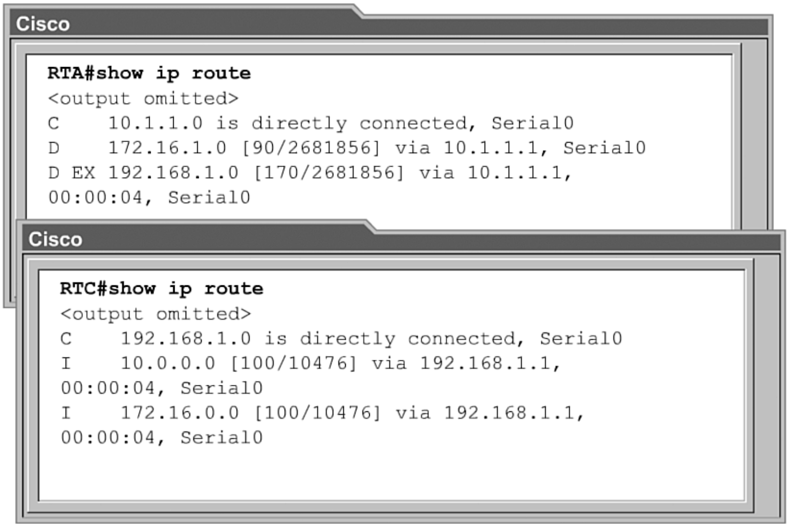
Click topology to view command outputs.

EIGRP and IGRP automatically redistribute routes between autonomous systems with the same number.

EIGRP will tag routes learned from IGRP or any outside source as external because they did not originate from EIGRP routers. IGRP cannot differentiate between internal and external routes.

Notice that in the **show ip route** command output for the routers in Figure 50, EIGRP routes are flagged with D, and external routes are denoted by EX. RTA identifies the difference between the network learned via EIGRP (172.16.0.0) and the network that was redistributed from IGRP (192.168.1.0). In the RTC table, the IGRP protocol makes no such distinction. RTC, which is running IGRP only, just sees IGRP routes, despite the fact that both 10.1.1.0 and 172.16.0.0 were redistributed from EIGRP.

**Figure 50 show ip route** Command Output



```
RTA#show ip route
<output omitted>
C    10.1.1.0 is directly connected, Serial0
D    172.16.1.0 [90/2681856] via 10.1.1.1, Serial0
D EX 192.168.1.0 [170/2681856] via 10.1.1.1,
00:00:04, Serial0
```

```
RTC#show ip route
<output omitted>
C    192.168.1.0 is directly connected, Serial0
I    10.0.0.0 [100/10476] via 192.168.1.1,
00:00:04, Serial0
I    172.16.0.0 [100/10476] via 192.168.1.1,
00:00:04, Serial0
```

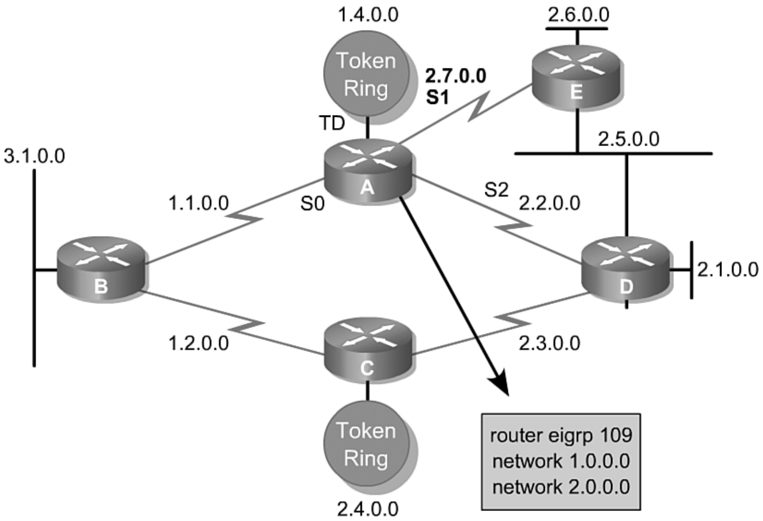
## Lesson 3.2: EIGRP Configuration

See Chapter 4, "Enhanced Interior Gateway Routing Protocol," of the Cisco Press Companion Guide, Third Edition, for more information.

Enhanced Interior Gateway Routing Protocol (EIGRP), the Cisco proprietary routing protocol based on IGRP, has much of the functionality of OSPF but is much easier to configure. In a networking environment that is primarily composed of Cisco routers, EIGRP is an ideal choice for a dynamic routing protocol.

This lesson covers common EIGRP configuration tasks; particularly the ways in which EIGRP establishes relationships with adjacent routers, calculates primary and backup routes, and, when necessary, responds to failures in known routes to a particular destination, as shown in Figure 51.

**Figure 51** Configuring EIGRP



Despite the complexity of the Distributed Update Algorithm (DUAL), configuring EIGRP can be relatively simple. EIGRP configuration commands vary depending on the protocol that is to be routed. Some examples of these protocols are IP, IPX, and AppleTalk. This section covers EIGRP configuration for the IP protocol.

Perform the following steps to configure EIGRP for IP:

**Step 1** Use the following to enable EIGRP and define the autonomous system:

```
router(config)# router eigrp autonomous-system-number
```

The autonomous system number is the number that identifies the autonomous system. It is used to indicate all routers that belong within the internetwork. This value must match all routers within the internetwork.

**Step 2** Indicate which networks belong to the EIGRP autonomous system on the local router by using the following command:

```
router(config-router)# network network-number
```

The network number is the network number that determines which interfaces of the router are participating in EIGRP and which networks are advertised by the router.

The **network** command configures only connected networks. For example, network 3.1.0.0, which is on the far left of the main figure, is not directly connected to Router A. Consequently, that network is not part of the configuration of Router A.

**Step 3** When you are configuring serial links using EIGRP, it is important to configure the bandwidth setting on the interface. If the bandwidth for these interfaces is not changed, EIGRP assumes the default bandwidth on the link rather than the true bandwidth. If the link is slower, the router may not be able to converge, routing updates might become lost, or suboptimal path selection may result. To set the interface bandwidth, use the following syntax:

```
router(config-if)# bandwidth kilobits
```

The value, *kilobits*, indicates the intended bandwidth in kilobits per second. For generic serial interfaces, such as PPP or HDLC, set the bandwidth to the line speed.

**Step 4** Cisco also recommends adding the following command to all EIGRP configurations:

```
router(config-if)# eigrp log-neighbor-changes
```

This command enables the logging of neighbor adjacency changes to monitor the stability of the routing system and to help detect problems.

## Lesson 3.3: Troubleshooting Routing Protocols

See Chapter 4, “Enhanced Interior Gateway Routing Protocol,” of the Cisco Press Companion Guide, Third Edition, for more information.

A network is made up of many devices, protocols, and media that allow data communication to happen. When one piece of the network doesn’t work properly, one or two users may be unable to communicate, or the entire network may fail. In either case, the network administrator must quickly identify and troubleshoot problems when they arise.

A network administrator should approach troubleshooting in a methodical manner using a general problem-solving model. It is often useful to check for physical layer problems first and then move up the layers in an organized manner. Although this lesson focuses on troubleshooting the operation of routing protocols, which work at Layer 3, it is important to eliminate any problems that may exist at lower layers.

All routing protocol troubleshooting should begin with a logical sequence, or process flow. This process flow is not a rigid outline for troubleshooting an internetwork. However, it is a foundation from which a network administrator can build a problem-solving process to suit a particular environment.

1. When analyzing a network failure, make a clear problem statement.
2. Gather the facts needed to help isolate possible causes.
3. Consider possible problems based on the facts that have been gathered.
4. Create an action plan based on the potential problems.
5. Implement the action plan, carefully troubleshooting each problem, one at a time, while testing to see whether the symptom disappears.
6. Analyze the results to determine whether the problem has been resolved. If it has, the process is complete.
7. If the problem has not been resolved, create an action plan based on the next most likely problem in the list. Return to Step 4, change one variable at a time, and repeat the process until you have solved the problem.
8. When the actual cause of the problem is identified, try to solve it.

Cisco routers provide numerous integrated commands to assist in monitoring and troubleshooting an internetwork:

- **show** commands help monitor installation behavior and normal network behavior, as well as isolate problem areas.
- **debug** commands assist in the isolation of protocol and configuration problems.
- TCP/IP network tools such as **ping**, **traceroute**, and **telnet**.

Cisco IOS **show** commands are among the most important tools for understanding the status of a router, detecting neighboring routers, monitoring the network in general, and isolating problems in the network.

Exec **debug** commands can provide a wealth of information about interface traffic, internal error messages, protocol-specific diagnostic packets, and other useful troubleshooting data. Use **debug** commands to isolate problems, not to monitor normal network operation. Only use **debug** commands to look for specific types of traffic or problems. Before using the **debug** command, narrow the problems to a likely subset of causes. Use the **show debugging** command to view which debugging features are enabled.

## Module 6—Switch Configuration

### Lesson 6.1: Starting the Switch

See Chapter 7, "Switch Configuration," of the Cisco Press Companion Guide, Third Edition, for more information.

A *switch* is a Layer 2 network device that acts as the concentration point for the connection of workstations, servers, routers, hubs, and other switches.

A *hub* is an earlier type of concentration device that, like a switch, provides multiple ports. Hubs are inferior to switches because all devices connected to a hub reside in the same bandwidth domain, and collisions will occur. In addition, hubs operate only in half-duplex mode. Half-duplex mode means the hubs can either send or receive data, but not both, at any given time. Switches can operate in full-duplex mode, which means they can send and receive data simultaneously.

Switches are multiport bridges. Switches are the standard technology for today's Ethernet LANs that utilize a star topology. A switch provides many dedicated, point-to-point virtual circuits between connected networking devices, so collisions are virtually impossible.

The ability to understand and configure switches is essential for network support because of the dominant role they play in modern networks.

A new switch has a preset configuration with factory defaults. This configuration is rarely what a network administrator needs. Switches can be configured and managed from a command-line interface (CLI). Increasingly, networking devices can also be configured and managed using a web-based interface and a browser.

Switches are dedicated, specialized computers, which contain a CPU, RAM, and an OS. Switches usually have several ports for connecting hosts and specialized ports for management. You can manage a switch by connecting it to the console port to view and make changes to the configuration.

Switches typically have no power switch to turn them on and off, but just connect or disconnect from a power source.

### Lesson 6.2: Configuring the Switch

See Chapter 7, "Switch Configuration," of the Cisco Press Companion Guide, Third Edition, for more information.

A new switch has a preset configuration with factory defaults. This configuration is rarely what a network administrator needs. Switches can be configured and managed from a command-line interface (CLI). Increasingly, networking devices can also be configured and managed using a web-based interface and a browser.

To effectively manage a network with switches, a network administrator must be familiar with many tasks. Some tasks are associated with maintaining the switch and its Internetworking Operating System (IOS), whereas others involve managing the switch's interfaces and tables for optimal, reliable, and secure operation. Essential network administrator skills include basic switch configuration, upgrading the IOS, and performing password recovery.

A switch may already be configured and only passwords may need to be entered for the user EXEC, enable, or privileged EXEC modes. Switch configuration mode is entered from privileged EXEC mode.

In the CLI, the default privileged EXEC mode is Switch#. In user EXEC mode, the prompt is Switch>.

To ensure that a new configuration completely overwrites any existing configuration, follow these steps:

**Step 1** Remove any existing VLAN information by deleting the VLAN database file vlan.dat from the Flash memory directory.

**Step 2** Erase the backup configuration file startup-config.

**Step 3** Reload the switch.

Security, documentation, and management are important for every internetworking device.

A switch should be given a hostname, and passwords should be set on the console and vty lines.

To allow the switch to be accessible by telnet and other TCP/IP applications, IP addresses and a default gateway should be set. VLAN 1 is, by default, the management VLAN. In a switch-based network, all internetworking devices should be in the management VLAN. This setup allows a single management workstation to access, configure, and manage all the internetworking devices.

The Fast Ethernet switch ports default to auto-speed and auto-duplex. This allows the interfaces to negotiate these settings. If a network administrator needs to ensure an interface has particular speed and duplex values, the administrator can set those values manually.

Intelligent networking devices can provide a web-based interface for configuration and management purposes. When a switch is configured with an IP address and gateway, it can be accessed in this way. A browser can be set to point at the IP address and port (default 80) for a web service. The HTTP service can be turned on or off and the port address for the service can be chosen.

Any additional software, such as an applet, can be downloaded to the browser from the switch and the network devices managed by a browser-based graphical user interface (GUI).

## Module 7—Spanning Tree Protocol (STP)

### Lesson 7.1: Redundant Topologies

See Chapter 8, “Spanning Tree Protocol,” of the Cisco Press Companion Guide, Third Edition, for more information.

Redundancy in a network is extremely important because redundancy allows networks to be fault tolerant. Redundant topologies protect against network downtime due to a failure of a single link, port, or networking device. Network engineers are often required to make difficult decisions balancing the cost of redundancy with the need for network availability.

Redundant topologies based on switches and bridges are susceptible to broadcast storms, multiple frame transmissions, and MAC address database instability. Therefore, network redundancy requires careful planning and monitoring to function properly.

Switched networks provide the benefits of smaller collision domains, microsegmentation, and full-duplex operation. Put simply, switched networks provide better performance.

Redundancy in a network is required to protect against loss of connectivity due to the failure of an individual component. Providing this redundancy, however, often results in physical topologies with loops. Physical layer loops can cause serious problems in switched networks. Broadcast storms, multiple frame transmissions, and MAC database instability can make such networks unusable.

Many companies and organizations increasingly rely on computer networks for their operations. Access to file servers, databases, the Internet, intranets, and extranets is critical for successful businesses. If the network is down, productivity is lost and customers are dissatisfied.

Companies are increasingly looking for 24-hour, 7-days-a-week uptime for their computer networks. Achieving 100-percent uptime is perhaps impossible, but securing a 99.999-percent (or “five nines”) uptime is a goal that organizations set. This is interpreted to mean 1 day of downtime, on average, for every 30 years, or 1 hour of downtime, on average, for every 4000 days, or 5.25 minutes of downtime per year.

Achieving such a goal requires extremely reliable networks. Reliability in networks is achieved by installing reliable equipment and by designing networks that are tolerant to failures and faults. The network is designed to reconverge rapidly so that the fault is bypassed.

Fault tolerance is achieved by redundancy. Redundancy means to be in excess or exceeding what is usual and natural. How does redundancy help achieve reliability?

Assume that the only way to get to work is by a car. If the car develops a fault that makes it unusable, going to work is impossible until the car is repaired and returned.

If the car fails and is unavailable on average 1 day in 10, there is 90-percent usage. Going to work is possible 9 days in every 10. Reliability is therefore 90 percent.

Buying another car will improve matters. There is no need for two cars just to get to work; however, the extra car does provide redundancy (backup) in case the primary vehicle fails. The ability to get to work is no longer dependent on a single car.

Both cars may become unusable simultaneously, 1 day in every 100. Purchasing a second redundant car improves reliability to 99 percent.

A goal of redundant topologies is to eliminate network outages caused by a single point of failure. All networks need redundancy for enhanced reliability.

## Lesson 7.2: Spanning Tree Protocol (STP) Overview

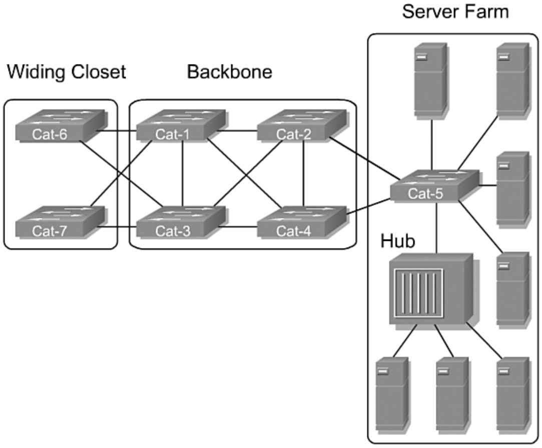
See Chapter 8, "Spanning Tree Protocol," of the Cisco Press Companion Guide, Third Edition, for more information.

The Spanning Tree Protocol is used in switched networks to create a loop-free logical topology from a physical topology that has loops. Links, ports, and switches that are not part of the active loop-free topology do not participate in the forwarding of data frames. STP is a powerful tool that gives network administrators the security of a redundant topology without the risk of problems caused by switching loops.

Networking topologies are designed to ensure that networks continue to function in the presence of single points of failure. Users have less chance of interruption to their work because the network continues to function. Any interruptions that are caused by a failure should be as short as possible.

Reliability is increased by redundancy. A network based on switches or bridges introduces redundant links between the switches or bridges to overcome the failure of a single link. These connections introduce physical loops into the network, as shown in Figure 52. These bridging loops are created so that if one link fails another can take over the function of forwarding traffic.

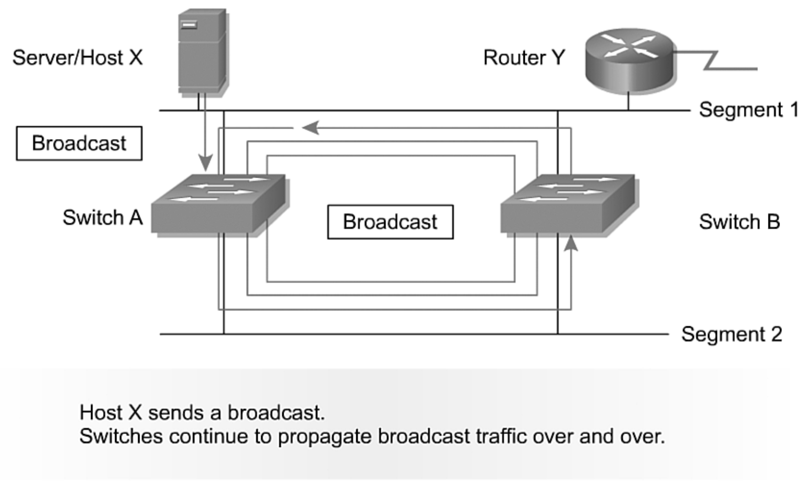
**Figure 52** Using Bridging Loops for Redundancy



Switches operate at Layer 2 of the OSI model, and forwarding decisions are made at this layer. As a result of this process, switched networks must not have loops.

Switches flood traffic out all ports when it is for a destination that is not yet known. Broadcast and multicast traffic is forwarded out every port other than the port on which the traffic arrived. This traffic can be caught in a loop, as shown in Figure 53.

**Figure 53** Broadcast Storm



Host X sends a broadcast.
Switches continue to propagate broadcast traffic over and over.

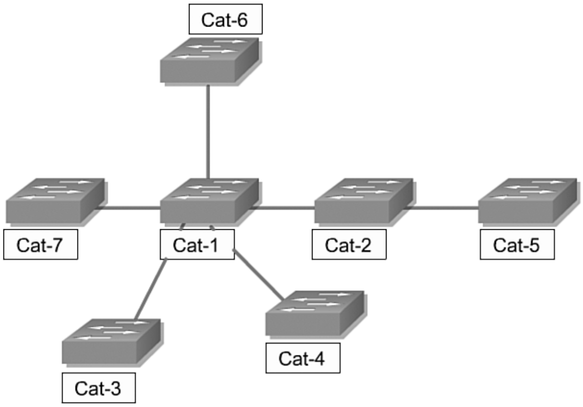
The Layer 2 header does not contain a Time-To-Live (TTL). If a frame is sent into a Layer 2-looped topology of switches, it can loop forever. This wastes bandwidth and makes the network unusable.

At Layer 3, the TTL is decremented and the packet discarded when the TTL reaches zero. This creates a dilemma. A physical topology that contains switching or bridging loops is necessary for reliability, but a switched network cannot have loops.

The solution is to allow physical loops but create a loop-free logical topology, as shown in Figure 54. With this logical topology, traffic destined for the server farm attached to Category 5 from any user workstation attached to Category 4 travels through Category 1 and Category 2. This travel happens even though a direct physical connection exists between Category 5 and Category 4.

The loop-free logical topology created is called a *tree*. This topology is a star or extended star logical topology, the spanning tree of the network. It is a spanning tree because all devices in the network are reachable or spanned.

**Figure 54** A Logical Loop-Free Topology Created by the Spanning-Tree Algorithm



The algorithm used to create this loop-free logical topology is the spanning-tree algorithm. This algorithm can take a relatively long time to converge. A new algorithm called the *rapid spanning-tree algorithm* is being introduced to reduce the time for a network to compute a loop-free logical topology.

## Module 8—VLANS

### Lesson 8.1: VLAN Concepts

See Chapter 9, "Virtual LANs," of the Cisco Press Companion Guide, Third Edition, for more information.

An important feature of Ethernet switching is the virtual local-area network (VLAN). A *VLAN* may be defined as a group of ports or LANs that have different physical connections but which communicate as if they are connected on a single network segment. Devices on a VLAN are restricted to contacting other devices on their own VLAN unless a router is used to route traffic between VLANs. It is often difficult to get an exact definition for a VLAN because vendors take varied approaches to creating them.

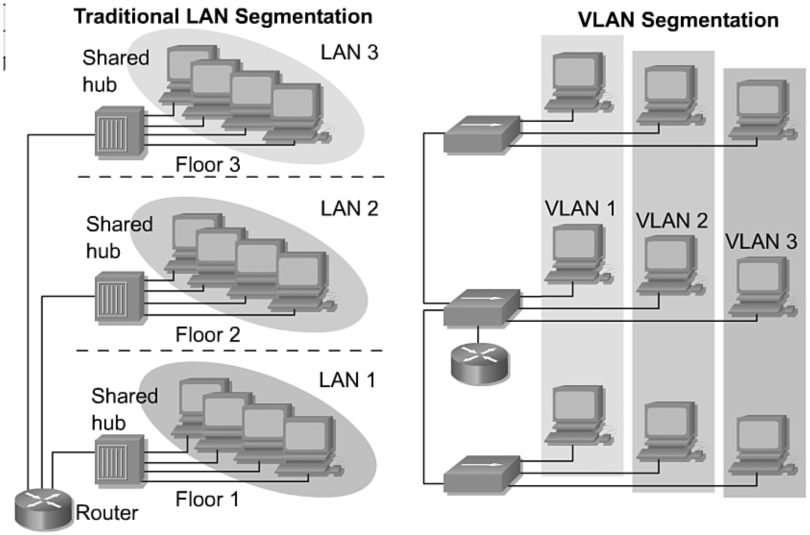
VLANs increase overall network performance by grouping users and resources that communicate most frequently with each other. Businesses often use VLANs as a way to ensure that a particular set of users is logically grouped even if the users are geographically separated. People who work in the marketing section of the business are placed in the Marketing VLAN, for example, and people who work in the Engineering section are placed in the Engineering VLAN.

VLANs can enhance scalability, security, and network management. Routers in VLAN topologies provide broadcast filtering, security, and traffic-flow management.

VLANs are potentially powerful tools for network administrators. Properly designed and configured, VLANs can simplify the tasks of adds, moves, and changes. VLANs can also enhance network security and help with the control of Layer 3 broadcasts. However, improperly configured VLANs can make a network function badly or not at all. It is extremely important to carefully design a network that uses VLANs and to understand the different ways that VLANs are implemented on different switches.

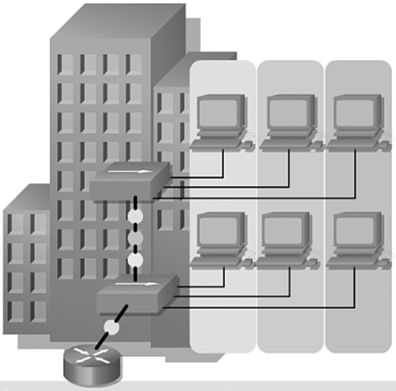
A VLAN is a group of network services that is not restricted to a physical segment or switch, as shown in Figure 55.

**Figure 55** VLANs and Physical Boundaries



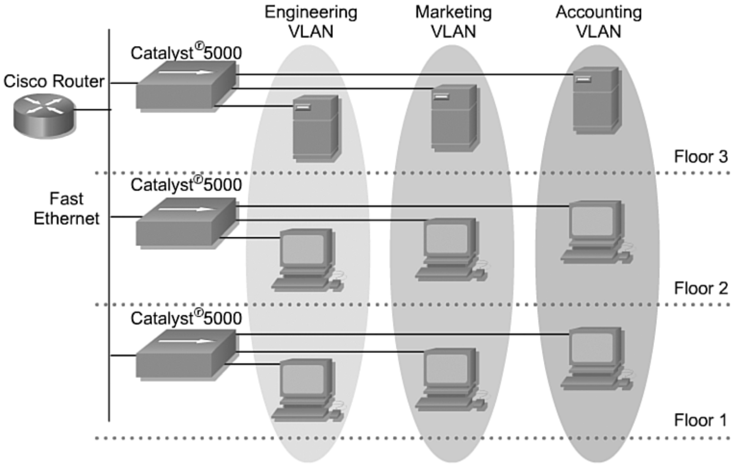
VLANs logically segment switched networks based on an organization's functions, project teams, or applications as opposed to a physical or geographical basis. For example, all the workstations and servers used by a particular workgroup team could be connected to the same VLAN, regardless of their physical connections to the network or location. Reconfiguration of the network can be done through software instead of by physically unplugging and moving devices or cables, as shown in Figures 56 and 57.

**Figure 56** Introduction to VLANs



- A group of ports or users in same broadcast domain
- Can be based on port ID, MAC address, protocol, or application
- LAN switches and network management software provide a mechanism to create VLANs
- Frame tagged with VLAN ID

**Figure 57** Multiple VLANs



A client workstation on a VLAN is generally restricted to contacting only file servers on the same VLAN. A VLAN may be thought of as a broadcast domain that exists within a defined set of switches. VLANs consist of a number of end systems. These are either hosts or network equipment, such as bridges and routers, connected by a single bridging domain. The bridging domain is supported on various pieces of network equipment, such as LAN switches that operate bridging protocols, with a separate bridge group for each VLAN.

VLANs are created to provide the segmentation services traditionally provided by routers in LAN configurations. VLANs address scalability, security, and network management. Routers in VLAN topologies provide broadcast filtering, security, and traffic-flow management. Switches may not bridge any traffic between VLANs because this would violate the integrity of the VLAN broadcast domain. Traffic should only be routed between VLANs.

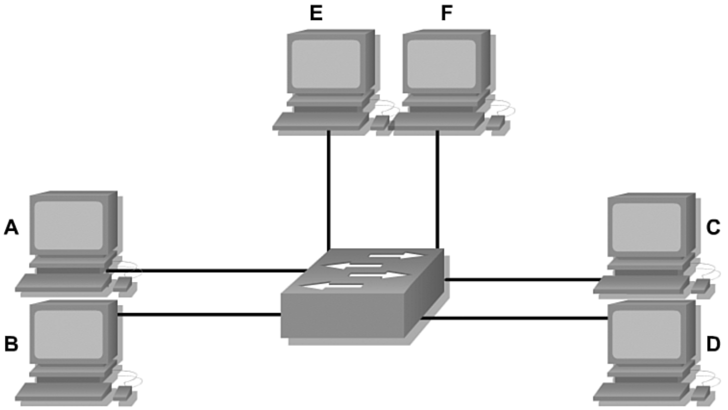
## Lesson 8.2: VLAN Concepts

See Chapter 9, "Virtual LANs," of the Cisco Press Companion Guide, Third Edition, for more information.

Remember that each interface on a switch behaves like a port on a legacy bridge. Bridges filter traffic that does not need to go to segments other than the source. If a frame needs to cross the bridge, the bridge forwards the frame to the correct interface and to no others. If the bridge or switch does not know where the destination resides, it floods the frame to all ports in the broadcast domain VLAN, except the source port.

In a switched environment, a station usually sees only traffic destined specifically for it. The switch filters most of the other background traffic in the network. This allows the workstation to have full, dedicated bandwidth for sending or receiving interesting traffic. Unlike a shared-hub system where only one station can transmit at a time, the switched network allows many concurrent transmissions within a broadcast domain. The switched network does this without directly affecting other stations inside or outside of the broadcast domain, as shown in Figure 58. Station pairs A/B, C/D, and E/F can all communicate without affecting the other station pairs.

**Figure 58** Concurrent Transmissions in a Catalyst



Each VLAN must have a unique Layer 3 network address assigned. This address enables switching of packets between VLANs with routers.

VLANs can exist either as end-to-end networks, which span the entire switch fabric, or they can exist inside of geographic boundaries.

An end-to-end VLAN network has the following characteristics:

- Users are grouped into VLANs independent of physical location, but according to group or job function.
- All users in a VLAN should have the same 80/20 traffic flow patterns.
- As a user moves around the campus, VLAN membership for that user should not change.

Each VLAN has a common set of security requirements for all members.

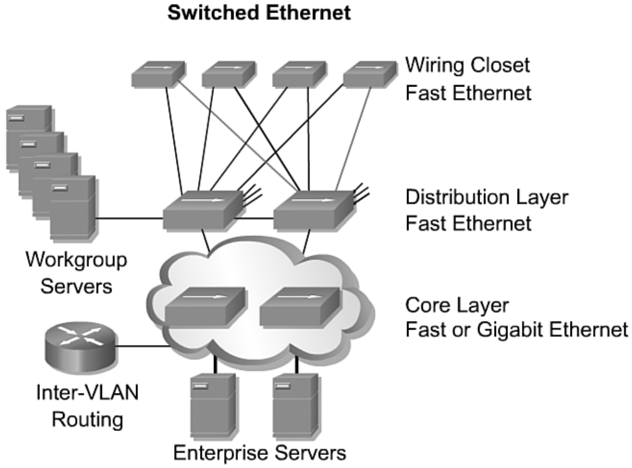
Starting in the wiring closet, 10-Mbps dedicated Ethernet ports are provisioned for each user. Each color represents a subnet. Because people have moved around over time, each switch eventually becomes a member of all VLANs. Fast Ethernet Inter-Switch Link (ISL) or IEEE 802.1Q is used to carry multiple VLAN information between the wiring closets and the distribution layer switches.

ISL is a Cisco proprietary protocol that maintains VLAN information as traffic flows between switches and routers. IEEE 802.1Q is an open-standard (IEEE) VLAN tagging mechanism that predominates in modern switching installations. Catalyst 2950 switches do not support ISL trunking.

Workgroup servers operate in a client/server model. For this reason, attempts have been made to keep users in the same VLAN as their server to maximize the performance of Layer 2 switching and keep traffic localized.

In the core, a router allows communication between subnets. The network is engineered, based on traffic-flow patterns, to have 80 percent of the traffic contained within a VLAN. The remaining 20 percent crosses the router to the enterprise servers and to the Internet and WAN, as shown in Figure 59.

**Figure 59** End-to-End VLANs



## Lesson 8.3: Troubleshooting VLANs

See Chapter 9, "Virtual LANs," of the Cisco Press Companion Guide, Third Edition, for more information.

VLANs are now commonplace in campus networks. VLANs give network engineers flexibility in designing and implementing networks. VLANs also enable broadcast containment, security, and geographically disparate communities of interest. As with basic LAN switching, however, problems can occur when VLANs are implemented. This lesson covers some of the more common problems that can occur with VLANs and examines several tools and techniques for troubleshooting.

Students completing this lesson should be able to:

- Utilize a systematic approach to VLAN troubleshooting.
- Demonstrate the steps for general troubleshooting in switched networks.
- Describe how spanning-tree problems can lead to broadcast storms.
- Use **show** and **debug** commands to troubleshoot VLANs.

It is important to develop a systematic approach to troubleshooting switch-related problems. Figure 60 lists steps that can assist in isolating a problem on a switched network.

**Step 1** Check the physical indications, such as LED status.

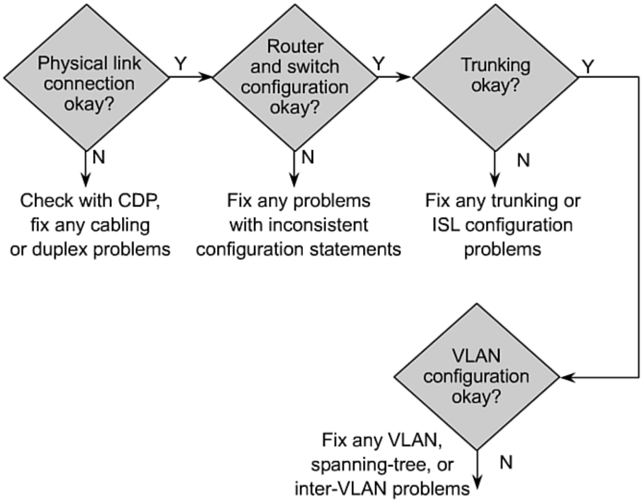
**Step 2** Start with a single configuration on a switch and work outward.

**Step 3** Check the Layer 1 link.

**Step 4** Check the Layer 2 link.

**Step 5** Troubleshoot VLANs that span several switches.

**Figure 60** Problem Isolation in Catalyst Networks


Physical link connection okay?
Y
Router and switch configuration okay?
Y
Trunking okay?
Y
N
Check with CDP, fix any cabling or duplex problems
N
Fix any problems with inconsistent configuration statements
N
Fix any trunking or ISL configuration problems
VLAN configuration okay?
Fix any VLAN, spanning-tree, or inter-VLAN problems
N

When troubleshooting, check to see whether the problem is a recurring one rather than an isolated fault. Some recurring problems result from growth in demand for services by workstation ports outpacing the configuration, trunking, or capacity to access server resources. For example, the use of web technologies and traditional applications, such as file transfer and e-mail, is causing network traffic growth that enterprise networks must handle.

Many campus LANs face unpredictable network traffic patterns that result from the combination of intranet traffic, fewer centralized campus server locations, and the increasing use of multicast applications. The old 80/20 rule, which stated that only 20 percent of network traffic went over the backbone, is obsolete. Internal web browsing now enables users to locate and access information anywhere on the corporate intranet. Traffic patterns are dictated by where the servers are located and not by the physical workgroup configurations with which they happen to be grouped.

If a network frequently experiences bottleneck symptoms, such as excessive overflows, dropped frames, and retransmissions, there may be too many ports riding on a single trunk or too many requests for global resources and access to intranet servers.

Bottleneck symptoms may also occur because a majority of the traffic is being forced to traverse the backbone. Another cause may be that any-to-any access is common, as users draw upon corporate web-based resources and multimedia applications. In this case, it may be necessary to consider increasing the network resources to meet the growing demand.

## Module 9—Virtual Trunking Protocol (VTP)

### Lesson 9.1: Trunking

See Chapter 10, "VLAN Trunking Protocol," of the Cisco Press Companion Guide, Third Edition, for more information.

Early VLANs were difficult to implement across large networks. Most VLANs were defined on a per-switch basis, which meant that defining VLANs over an entire network was a complicated task. Further complicating things, every switch manufacturer had a different idea of the best ways to make their switches VLAN capable. VLAN trunking solves many of the problems of early VLANs.

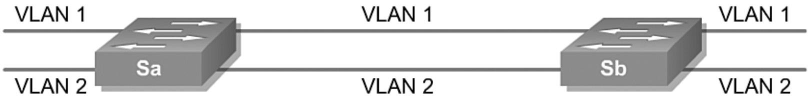
VLAN trunking allows many VLANs to be defined throughout an organization by adding special tags to frames to identify the VLAN to which they belong. This tagging allows many VLANs to be carried across a common backbone, or trunk. VLAN trunking is standards based, with the IEEE 802.1Q trunking protocol now widely implemented. Cisco's Inter-Switch Link (ISL) is a proprietary trunking protocol that can be implemented in all-Cisco networks.

VLAN trunking using specially tagged frames allows multiple VLANs to be carried throughout large switched networks over common backbones. Even with the use of trunks, however, manually configuring and maintaining VLANs on numerous switches can be difficult. VLAN Trunking Protocol (VTP) helps the network administrator by making many of the VLAN configuration tasks automatic.

As mentioned before, a trunk is a physical and logical connection between two switches across which network traffic travels. In few words, a trunk is a single transmission channel between two points that are usually switching centers.

In the context of a VLAN switching environment, a trunk is a point-to-point link that supports several VLANs. The purpose of a trunk is to save ports when creating a link between two devices implementing VLANs, typically two switches. Figure 61 illustrates two VLANs made available on two switches (Sa and Sb) using two physical links between the devices, each carrying the traffic for a separate VLAN. This is the simplest form of implementation, but it does not scale well.

**Figure 61** VLANs



Adding a third VLAN would require two additional ports to be given up. This design is also inefficient in terms of load sharing, and the traffic on some VLANs may not justify a dedicated link. Trunking will bundle multiple virtual links over one physical link, as shown in Figure 62.

**Figure 62** Trunking

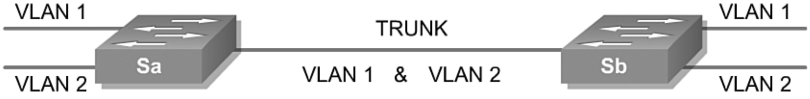
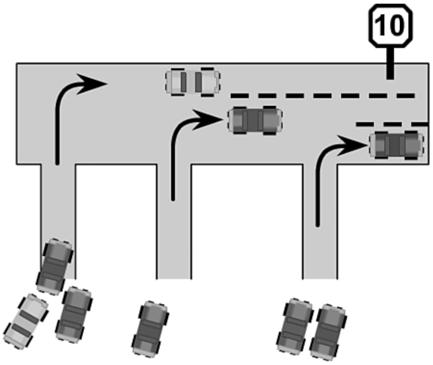


Figure 63 uses the metaphor of a highway distributor to describe trunking. The roads with different starting and ending points share a main national highway for a few kilometers and then divide again to reach their particular destinations. This method is more cost effective than building an entire road from start to end for every, existing or new destination.

**Figure 63** Highway Distributor



## Lesson 9.2: Virtual Trunking Protocol (VTP)

See Chapter 10, "VLAN Trunking Protocol," of the Cisco Press Companion Guide, Third Edition, for more information.

VLAN trunking using specially tagged frames allows multiple VLANs to be carried throughout large switched networks over common backbones. Even with the use of trunks, however, manually configuring and maintaining VLANs on numerous switches can be difficult. VLAN Trunking Protocol (VTP) helps the network administrator by making many of the VLAN configuration tasks automatic.

This lesson explains the concept and operation of VTP as well as its implementation in a VLAN-switched LAN environment.

VLAN Trunking Protocol (VTP) was created to solve potential operational problems in a VLAN's network-switched environment.

Consider, for example, a domain with several interconnected switches that support several VLANs. To maintain connectivity within VLANs, each VLAN must be manually configured on each switch. As the organization grows and additional switches are added to the network, each new switch must be manually configured with VLAN information. A single incorrect VLAN assignment could cause two potential problems:

- Cross-connected VLANs due to VLAN configuration inconsistencies
- VLAN configuration reconciliations across mixed-media environments such as Ethernet and Fiber Distributed Data Interface (FDDI)

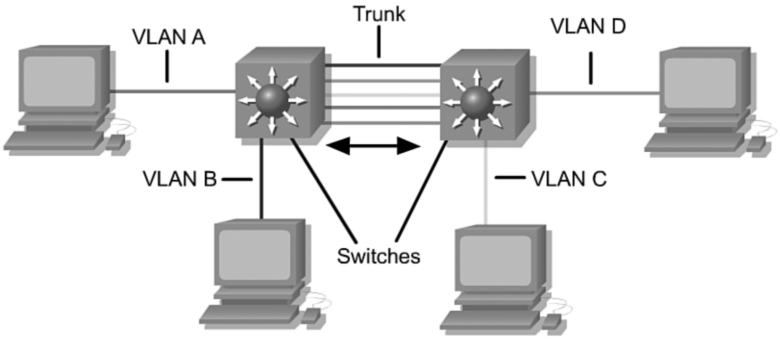
With VTP, VLAN configuration consistency is maintained across a common administration domain. Additionally, VTP reduces the complexity of managing and monitoring VLAN networks.

The role of VTP is to maintain VLAN configuration consistency across a common network administration domain. VTP is a messaging protocol that uses OSI Layer 2 trunk frames to manage the addition, deletion, and renaming of VLANs on a single domain. Further, VTP allows for centralized changes that are communicated to all other switches in the network.

VTP messages are encapsulated in either Cisco proprietary Inter-Switch Link (ISL) or IEEE 802.1Q protocol frames, and then passed across trunk links to other devices. In IEEE 802.1Q frames, a 4-byte field is added that tags the frame. Both formats carry the VLAN ID.

Whereas switch ports are normally assigned to only a single VLAN, trunk ports by default carry frames from all VLANs, as shown in Figure 64.

**Figure 64** Highway Distributor



## Lesson 9.3: Inter-VLAN Routing

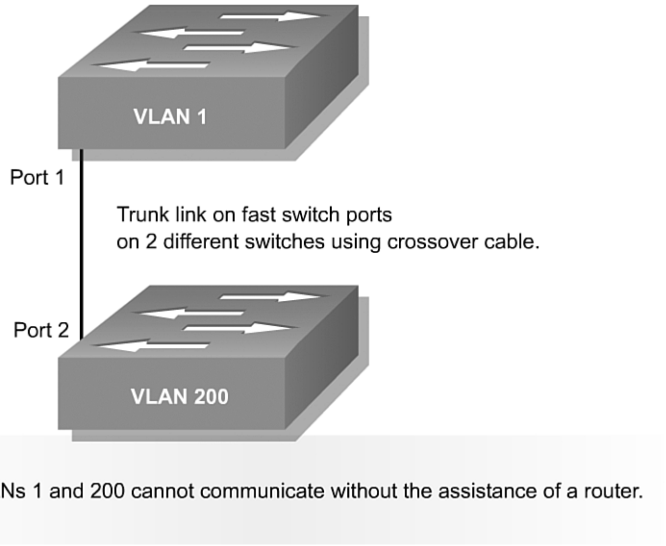
See Chapter 10, “VLAN Trunking Protocol,” of the Cisco Press Companion Guide, Third Edition, for more information.

VLAN technology provides network administrators with many advantages. Among other things, VLANs help control Layer 3 broadcasts, they improve network security, and they can help logically group network users. However, VLANs have an important limitation. They operate at Layer 2, which means that devices on one VLAN cannot communicate with users on another VLAN without the use of routers and network layer addresses.

When a host in one broadcast domain wants to communicate with another host, a router must be involved. The same situation exists with VLANs.

Port 1 on a switch is part of VLAN 1, and port 2 is part of VLAN 200, as shown in Figure 65. If all the switch ports were part of VLAN 1, the hosts connected to these ports could communicate. In this case, however, the ports are part of different VLANs, VLAN 1 and VLAN 200. A router must be involved if hosts from the different VLANs need to communicate, as shown in Figure 66.

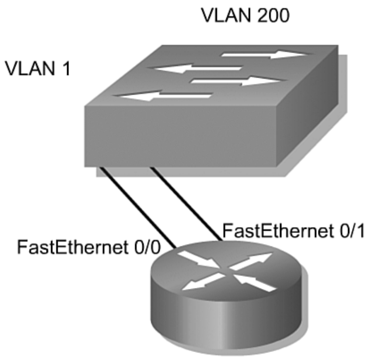
**Figure 65** Multiple VLANs


VLAN 1
Port 1
Trunk link on fast switch ports
on 2 different switches using crossover cable.
Port 2
VLAN 200

VLANs 1 and 200 cannot communicate without the assistance of a router.

The most important benefit of routing is its proven history of facilitating networks, particularly large networks. Although the Internet serves as the obvious example, this point is true for any type of network, such as a large campus backbone. Because routers prevent broadcast propagation and use more intelligent forwarding algorithms than bridges and switches, routers provide more efficient use of bandwidth. This simultaneously results in flexible and optimal path selection. For example, it is very easy to implement load balancing across multiple paths in most networks when routing. On the other hand, Layer 2 load balancing can be very difficult to design, implement, and maintain.

**Figure 66** Multiple VLANs

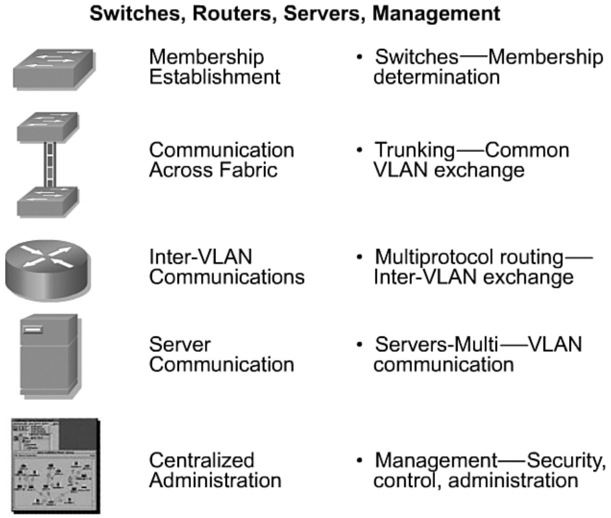


To route traffic between VLAN 1 and VLAN 200 in a non-ISL environment, a router must be connected to a port in VLAN1 and a port in VLAN 200.

If a VLAN spans across multiple devices, a trunk is used to interconnect the devices. A trunk carries traffic for multiple VLANs. A trunk can connect a switch to another switch, for instance, a switch to the inter-VLAN router, or a switch to a server with a special network interface card installed that supports trunking.

Remember that when a host on one VLAN wants to communicate with a host on another, a router must somehow be involved, as shown in Figure 67.

**Figure 67** VLAN Components



**Switches, Routers, Servers, Management**

| | |
|---|---|
| Membership Establishment | • Switches—Membership determination |
| Communication Across Fabric | • Trunking—Common VLAN exchange |
| Inter-VLAN Communications | • Multiprotocol routing—Inter-VLAN exchange |
| Server Communication | • Servers-Multi—VLAN communication |
| Centralized Administration | • Management—Security, control, administration |

# CCNA4

## Module 1—Scaling IP Addresses

### Lesson 1.1: Scaling Networks with NAT and PAT

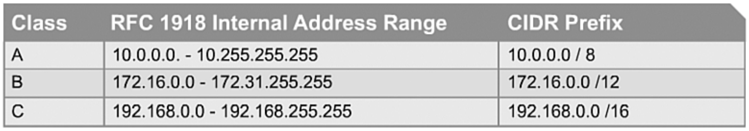
See Chapter 11, “Scaling IP Addresses,” of the Cisco Press Companion Guide, Third Edition, for more information.

The rapid growth of the Internet has astonished most observers. One reason that the Internet has grown so quickly is the flexibility of the original design. This design has not remained static, and if it had, the supply of IP addresses would have been exhausted long ago. To cope with a potential shortage of addresses, several solutions have been proposed. Two of the solutions that have been widely implemented are classless interdomain routing (CIDR) and Network Address Translation (NAT).

NAT is a mechanism for conserving registered IP addresses in large networks and simplifying IP addressing management tasks. As a packet is routed across a NAT-capable device, which is usually a firewall or router, the source IP address on the packet from a private internal network address is translated to a legal, external IP address. This translation allows the packet to be transported over public external networks, such as the Internet. The reply traffic is then translated back to the private internal address for delivery within the internal network. A variation of NAT, called Port Address Translation (PAT), allows many addresses to be translated using a single, globally routable address.

RFC 1918 sets aside three blocks of IP addresses: 1 Class A address, 16 Class B addresses, and 256 Class C addresses, as shown in Figure 68. These addresses are for private, internal network usage only, providing more than 17 million private addresses.

**Figure 68** Private IP Addresses



| Class | RFC 1918 Internal Address Range | CIDR Prefix |
|---|---|---|
| A | 10.0.0.0. - 10.255.255.255 | 10.0.0.0 / 8 |
| B | 172.16.0.0 - 172.31.255.255 | 172.16.0.0 /12 |
| C | 192.168.0.0 - 192.168.255.255 | 192.168.0.0 /16 |

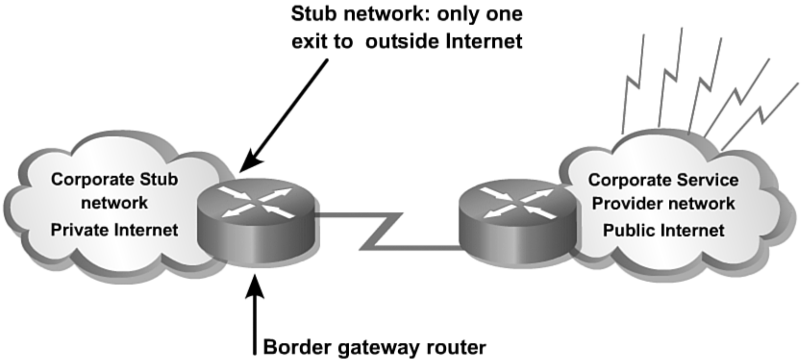
Public Internet addresses must be registered by a company with an Internet authority (for example, American Registry for Internet Numbers [ARIN] or Réseaux IP Européens [RIPE]). These public Internet addresses can also be leased from an ISP. Private IP addresses are reserved and can be used by anyone. That means two networks, or two million networks, can each use the same private address. RFC 1918 addresses should never be seen on the public Internet. A router should never route RFC 1918 addresses because ISPs typically configure the border routers to prevent privately addressed traffic from being forwarded.

NAT provides great benefits to individual companies and the Internet. Before NAT, a host with a private address could not access the Internet. Using NAT, individual companies can address some or all of their hosts with private addresses and use NAT to provide access the Internet.

NAT is the process of altering the IP header of a packet. NAT changes the header so that the destination address, the source address, or both addresses are replaced in the header. A device that runs specialized NAT software or hardware performs this process. NAT is designed to conserve IP addresses and enable networks using private IP addresses to connect to the Internet. This is accomplished by translating those nonregistered addresses into globally registered IP addresses. NAT also increases network privacy by hiding internal IP addresses from external networks.

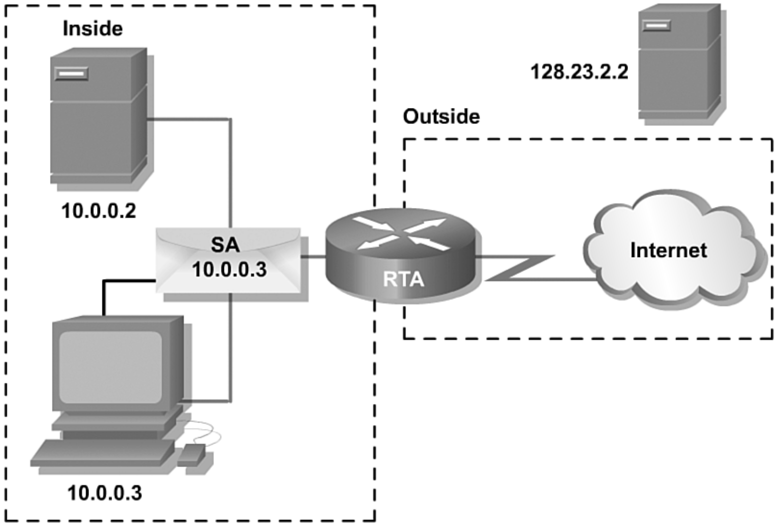
A NAT-enabled device typically operates at the border of a stub network. A stub network is a network that has a single connection to its neighbor network, as shown in Figure 69. When a host inside the stub network wants to transmit to a host on the outside, it forwards the packet to the border gateway router. The border gateway router for the host performs the NAT process, translating the internal private address to a public, external routable address, as shown in Figure 70. In NAT terminology, the internal network is the set of networks that are subject to translation. The external network refers to all other addresses.

**Figure 69** Introducing NAT and PAT



NAT can be configured to use only one address for the entire network. This function, static Port Address Translation (PAT) or “overload,” effectively hides the internal network, providing additional security.

**Figure 70** Introducing NAT and PAT



## Lesson 1.2: DHCP

See Chapter 11, "Scaling IP Addresses," of the Cisco Press Companion Guide, Third Edition, for more information.

Routers, servers, and other key nodes usually require a static IP configuration, which is entered manually. However, desktop clients do not require a specific address but rather any one in a range of addresses. This range is typically within an IP subnet. A desktop client within a specific subnet can have any address within a range, and the other values are defaults, including subnet mask, gateway, and DNS server.

The Dynamic Host Configuration Protocol (DHCP) was designed to assign IP addresses and other important network configuration information dynamically. Because desktop clients typically make up the bulk of network nodes, DHCP is an extremely useful time-saving tool for network administrators.

DHCP works in a client/server mode. DHCP enables DHCP clients on an IP network to obtain their configurations from a DHCP server. Less work is involved in administrating an IP network when DHCP is used. The most significant configuration option the client receives from the server is its IP address. RFC 2131 describes DHCP.

The DHCP client is part of most modern operating systems, including Windows 2000, Windows NT, Solaris, Linux, and Mac OS. With DHCP, the client requests the configuration values from the network. There must be a DHCP server on the network. This server manages the allocation of the IP configuration values and answers configuration requests from clients. The DHCP server can be responsible for answering requests for many subnets. DHCP is not intended for use in configuring routers, switches, and servers. These hosts all need to have static IP addresses.

DHCP works by configuring a server to give out IP information to clients. Clients lease the information from the server for an administratively defined period. When the lease is up, the host must ask for another address, although the host is typically reassigned the same one.

Administrators typically prefer to use a Microsoft NT server or a UNIX computer to offer DHCP services because these solutions are scalable and relatively easy to manage. Even so, a Cisco IOS feature set, Easy IP, offers an optional, fully featured DHCP server. Easy IP leases configurations for 24 hours by default—a convenience for small offices and home offices, which can take advantage of DHCP and NAT without having a Windows NT or UNIX server.

Administrators set up DHCP servers to assign addresses from predefined pools. DHCP servers can also offer other information, such as DNS server addresses, WINS server addresses, and domain names. Most DHCP servers also allow the administrator to define specifically what client MAC addresses can be serviced and automatically assign them the same IP address each time.

DHCP uses User Datagram Protocol (UDP) as its transport protocol. The client sends messages to the server on port 67. The server sends messages to the client on port 68.

## Module 2—WAN Technologies

### Lesson 2.2: WAN Technologies

See Chapter 12, “WAN Technologies,” of the Cisco Press Companion Guide, Third Edition, for more information.

As the enterprise grows beyond a single location, it is necessary to interconnect the LANs in the various branches to form a WAN. This lesson examines some of the options available for these interconnections, the hardware needed to implement them, and the terminology used to discuss them.

Many options are currently available for implementing WAN solutions. They differ in technology, speed, and cost. Familiarity with these technologies is an important part of network design and evaluation.

If all data traffic in an enterprise is within a single building, a LAN meets the needs of the organization. If data must flow between buildings on a single campus, the buildings can be interconnected with high-speed data links to form a campus LAN. If data must be transferred between geographically disparate locations, however, a WAN is needed to carry the data. Individual remote access to the LAN and connection of the LAN to the Internet are separate study topics and are not considered here.

Most students will not have the opportunity to design a new WAN but many will be involved in designing additions and upgrades to existing WANs and will be able to apply the techniques learned in this lesson.

A WAN is a data communications network that operates beyond the geographic scope of a LAN. One primary difference between a WAN and a LAN is that a company or organization must subscribe to an outside WAN service provider to use WAN carrier network services. A WAN uses data links provided by carrier services to access the Internet and connect the locations of an organization to each other, to locations of other organizations, to external services, and to remote users. WANs generally carry a variety of traffic types, such as voice, data, and video. Telephone and data services are the most commonly used WAN services.

WAN links are provided at various speeds measured in bits per second (bps), kilobits per second (kbps or 1000 bps), megabits per second (Mbps or 1000 kbps), or gigabits per second (Gbps or 1000 Mbps). The bps values are generally full duplex. This means that an E1 line can carry 2 Mbps, or a T1 can carry 1.5 Mbps, in each direction simultaneously.

Devices on the subscriber premises are called customer premises equipment (CPE), as shown in Figure 71. The CPE may be owned by the subscriber or leased from the service provider. A copper cable connects the CPE to the service provider's nearest exchange or central office (CO). The copper cabling is often called the local loop, or "last-mile." A dialed call is connected locally to other local loops, or nonlocally through a trunk to a primary center. It then goes to a sectional center and on to a regional or international carrier center as the call travels to its destination, as shown in Figure 72.

**Figure 71** WAN Technology

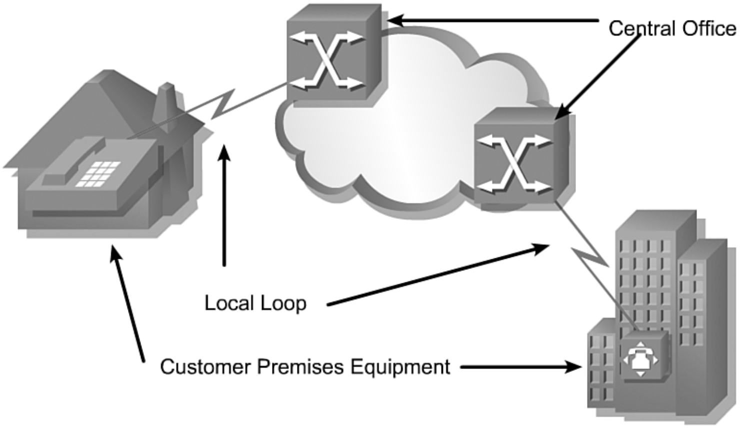
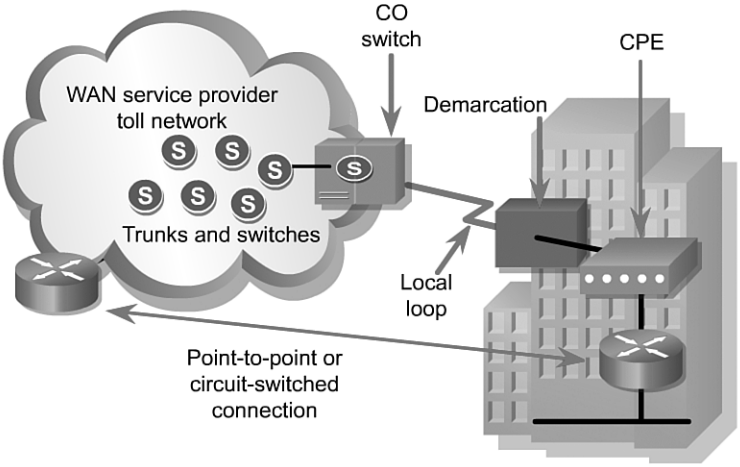


**Figure 72** WAN Service Providers



For the local loop to carry data, a device such as a modem is needed to prepare the data for transmission. Devices that put data on the local loop are called data circuit-terminating equipment or data communications equipment (DCE). The customer devices that pass the data to the DCE are called data terminal equipment (DTE), as shown in Figure 73. The DCE primarily provides an interface for the DTE into the communication link on the WAN cloud. The DTE/DCE interface uses various physical layer protocols such as High-Speed Serial Interface (HSSI) and V.35 that establish the codes the devices use to communicate with each other, as shown in Figure 74.

**Figure 73** DCE and DTE

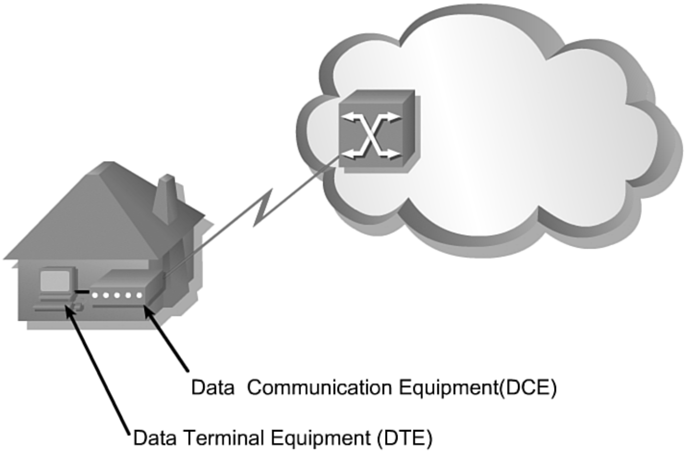
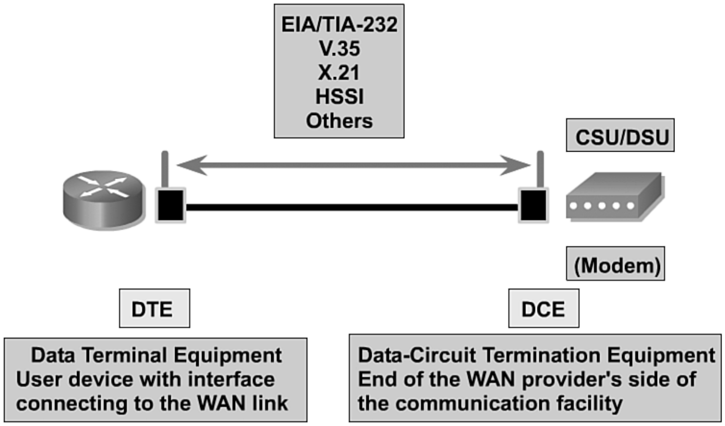

Data Communication Equipment(DCE)
Data Terminal Equipment (DTE)

**Figure 74** Physical Layer: WANs


EIA/TIA-232
V.35
X.21
HSSI
Others
CSU/DSU
(Modem)
DTE
DCE
Data Terminal Equipment
User device with interface
connecting to the WAN link
Data-Circuit Termination Equipment
End of the WAN provider's side of
the communication facility

## Module 4—ISDN and DDR

### Lesson 4.1: ISDN Concepts

See Chapter 14, "ISDN and DDR," of the Cisco Press Companion Guide, Third Edition, for more information.

Integrated Services Digital Network (ISDN) is a network that provides end-to-end digital connectivity to support a wide range of services, including voice and data services.

ISDN allows multiple digital channels to be operated simultaneously through the same regular phone wiring used for analog lines, but ISDN transmits a digital signal rather than an analog one. Latency is much lower on an ISDN line than on an analog line.

Several WAN technologies are used to provide network access from remote locations. One of these technologies is ISDN. ISDN is specifically designed to solve the low-bandwidth problems that small offices or dial-in users have with traditional telephone dial-in services.

The traditional Public Switched Telephone Network (PSTN) was based on an analog connection between the customer's premises and the local exchange, also called the *local loop*, as shown in Figure 75. This analog signaling introduces limitations on the bandwidth that can be obtained on the local loop. Bandwidth restrictions do not permit analog data to travel faster than 3000 Hz. Removal of the bandwidth restriction has permitted the use of digital signaling on the local loop and hence better access speeds for the remote users, as shown in Figure 76.

**Figure 75** Physical Layer: WANs

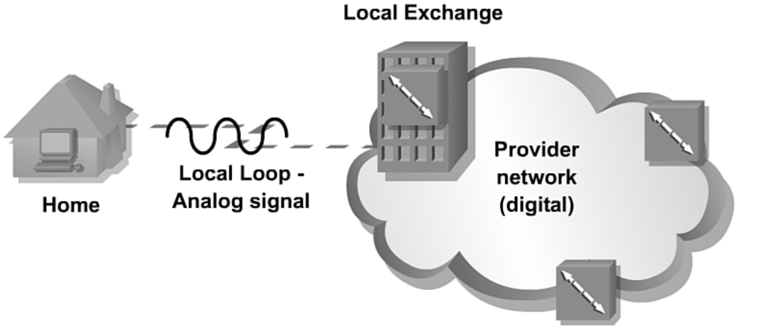
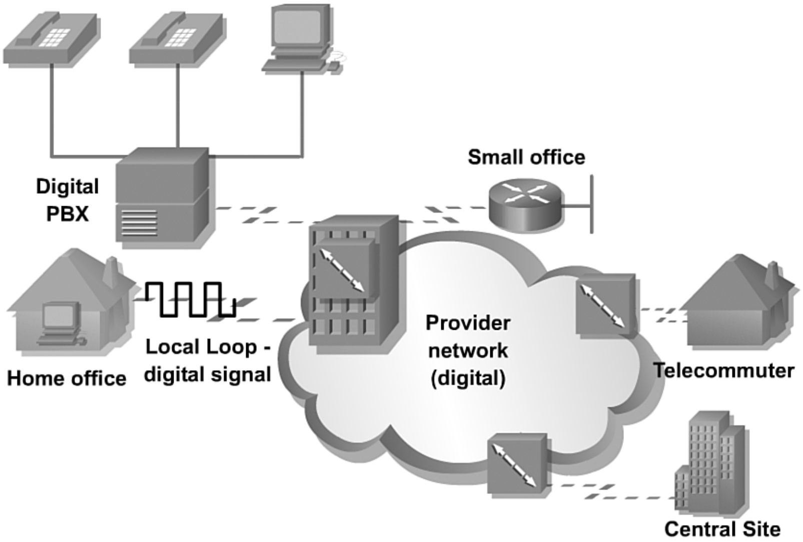


**Figure 76** Physical Layer: WANs



Telephone companies developed ISDN with the intention of creating a totally digital network. ISDN allows digital signals to be transmitted over existing telephone wiring. This became possible when the telephone company switches were upgraded to handle digital signals. ISDN is generally used for telecommuting and networking small and remote offices into the corporate LAN.

Telephone companies developed ISDN as part of an effort to standardize subscriber services. This standardization included the User-Network Interface (UNI), better known as the local loop. The ISDN standards define the hardware and call setup schemes for end-to-end digital connectivity. These standards help achieve the goal of worldwide connectivity by ensuring that ISDN networks easily communicate with one another. In an ISDN network, the digitizing function is done at the user site rather than the telephone company.

ISDN brings digital connectivity to local sites, and the benefits include the following:

- Carrying a variety of user traffic signals, including data, voice, and video.
- Offering much faster call setup than modem connections.
- Bearer channels (B channels) provide a faster data transfer rate than modems.
- B channels are suitable for negotiated Point-to-Point Protocol (PPP) links.

ISDN is a versatile service able to carry voice, video, and data traffic. It is possible to use multiple channels to carry different types of traffic over a single connection.

Unlike PSTN connections, ISDN uses out-of-band signaling, the delta (D channel), for call setup and signaling. To make a normal telephone call, the user dials the number one digit at a time. When all the numbers are received, the call can be placed to the remote user. ISDN allows all the numbers to be signaled to the switch simultaneously, thus reducing the time it takes to set up the call.

ISDN also provides more bandwidth than a traditional 56-kbps dialup connection. ISDN uses bearer channels, also called B channels, as clear data paths. Each B channel provides 64 kbps of bandwidth. With multiple B channels, ISDN offers more bandwidth for WAN connections than some leased services. An ISDN connection with two B channels provides a total usable bandwidth of 128 kbps.

Each ISDN B channel can make a separate serial connection to any other site in the ISDN network. Because PPP operates over both synchronous and asynchronous serial links, ISDN lines can be used in conjunction with PPP encapsulation.

## Lesson 4.2: ISDN Configuration

See Chapter 14, "ISDN and DDR," of the Cisco Press Companion Guide, Third Edition, for more information.

The command **isdn switch-type** *switch-type* can be configured at the global or interface command mode to specify the provider ISDN switch.

Configuring the **isdn switch-type** command in the global configuration mode sets the ISDN switch type identically for all ISDN interfaces. Individual interfaces may be configured, after the global configuration command, to reflect an alternate switch type.

When the ISDN service is installed, the service provider issues information about the switch type and service profile identifiers (SPIDs). SPIDs are used to define the services available to individual ISDN subscribers. Depending on the switch type, these SPIDs may have to be added to the configuration. National ISDN-1 and DMS-100 ISDN switches require SPIDs to be configured, but the AT&T 5ESS switch does not. SPIDs must be specified when using the Adtran ISDN simulator.

The format of the SPIDs can vary depending on the ISDN switch type and specific provider requirements. Use the **isdn spid1** and **isdn spid2** interface configuration mode commands to specify the SPID required by the ISDN network when the router initiates a call to the local ISDN exchange.

Configuration of ISDN BRI is a mix of global and interface commands. To configure the ISDN switch type, use the **isdn switch-type** command in global configuration mode, as follows:

```
Router(config)#isdn switch-type switch-type
```

The argument *switch-type* indicates the service provider switch type. To disable the switch on the ISDN interface, specify **isdn switch-type none**. The following example configures the National ISDN-1 switch type in the global configuration mode:

```
Router(config)#isdn switch-type basic-ni
```

To define SPIDs, use the **isdn spid#** command in interface configuration mode. This command is used to define the SPID numbers that have been assigned for the B channels:

```
Router(config-if)#isdn spid1 spid-number [ldn]
Router(config-if)#isdn spid2 spid-number [ldn]
```

## Lesson 4.3: DDR Configuration

See Chapter 14, "ISDN and DDR," of the Cisco Press Companion Guide, Third Edition, for more information.

Dial-on-demand routing (DDR) is a technique developed by Cisco that allows the use of existing telephone lines to form a WAN, instead of using separate, dedicated lines. Public Switched Telephone Networks (PSTNs) are involved in this process.

DDR is used when a constant connection is not needed, thus reducing costs. DDR defines the process of a router connecting via a dialup network when there is traffic to send, and then disconnecting when the transfer is complete.

This flowchart shows how a router decides whether to initiate a DDR connection.

DDR is triggered when traffic that matches a predefined set of criteria is queued to be sent out a DDR-enabled interface. The traffic that causes a DDR call to be placed is referred to as *interesting traffic*. After the router has transmitted the interesting traffic, the call is terminated.

The key to efficient DDR operation is in the definition of interesting traffic. Interesting traffic is defined with a dialer list. Dialer lists can allow all traffic from a specific protocol to bring up a DDR link, or they can query an access list to see which types of traffic should bring up the link. Dialer lists do not filter traffic on an interface. Even traffic that is not interesting is forwarded if the connection to the destination is active.

DDR is implemented in Cisco routers as follows:

1. The router receives traffic, performs a routing table lookup to determine whether there is a route to the destination, and identifies the outbound interface.
2. If the outbound interface is configured for DDR, the router does a lookup to determine whether the traffic is interesting.
3. The router identifies the dialing information necessary to make the call using a dialer map to access the next-hop router.
4. The router then checks to see whether the dialer map is in use. If the interface is currently connected to the desired remote destination, the traffic is sent. If the interface is not currently connected to the remote destination, the router sends call-setup information via the Basic Rate Interface (BRI) using the D channel.
5. After the link is enabled, the router transmits both interesting and uninteresting traffic. Uninteresting traffic can include data and routing updates.
6. The idle timer starts when no interesting traffic is seen during the idle timeout period and disconnects the call based on the idler timer configuration.

The idle timer setting specifies the length of time the router should remain connected if no interesting traffic has been sent. When a DDR connection is established, any traffic to that destination is permitted. However, only interesting traffic resets the idle timer.

Legacy DDR is a term used to define basic DDR configurations in which a single set of dialer parameters is applied to an interface. If multiple unique dialer configurations are needed on one interface, dialer profiles should be used.

To configure Legacy DDR, perform the following steps:

**Step 1** Define static routes.

**Step 2** Specify interesting traffic.

**Step 3** Configure the dialer information.

## Module 5—Frame Relay

### Lesson 5.1: Frame Relay Concepts

See Chapter 15, “Frame Relay,” of the Cisco Press Companion Guide, Third Edition, for more information.

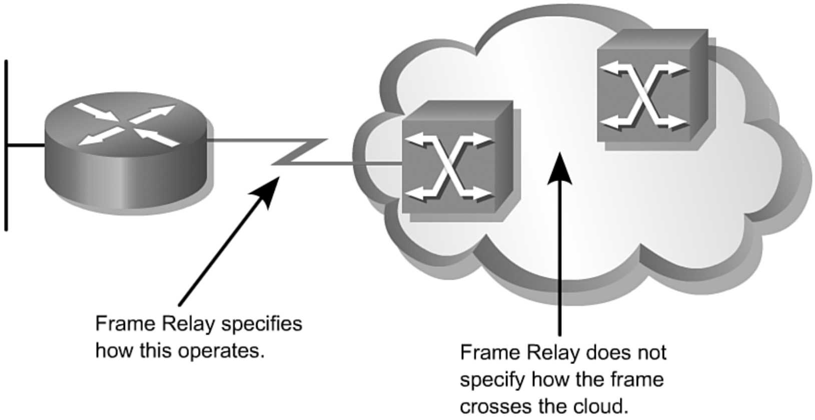
Frame Relay was originally developed as an extension of ISDN to enable the circuit-switched technology to be transported on a packet-switched network. The technology has become a standalone and cost-effective means of creating a WAN.

Frame Relay switches create virtual circuits to connect remote LANs to a WAN. The Frame Relay exists between a LAN border device, usually a router, and the carrier switch. The technology used by the carrier to transport the data between the switches is irrelevant to Frame Relay.

The sophistication of the technology requires a thorough understanding of the terms used to describe how Frame Relay works. Without a firm understanding of Frame Relay, it is difficult to troubleshoot its performance.

Frame Relay is an International Telephony Union (ITU-T) and American National Standards Institute (ANSI) standard. Frame Relay is a packet-switched, connection-oriented, WAN service. It operates at the data link layer of the OSI reference model. Frame Relay does this by using a subset of the High-Level Data Link Control (HDLC) protocol called Link Access Protocol Frame (LAPF). Frames carry data between user devices, referred to as data terminal equipment (DTE), and the data communications equipment (DCE) at the edge of the WAN, as shown in Figure 77.

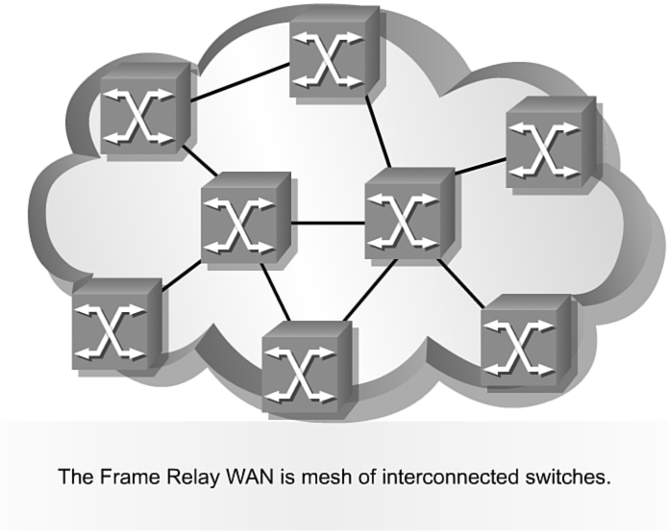
**Figure 77** Frame Relay Operation



Originally Frame Relay was designed to allow Integrated Services Digital Network (ISDN) equipment to have access to a packet-switched service on a B channel. However, Frame Relay is now a standalone technology.

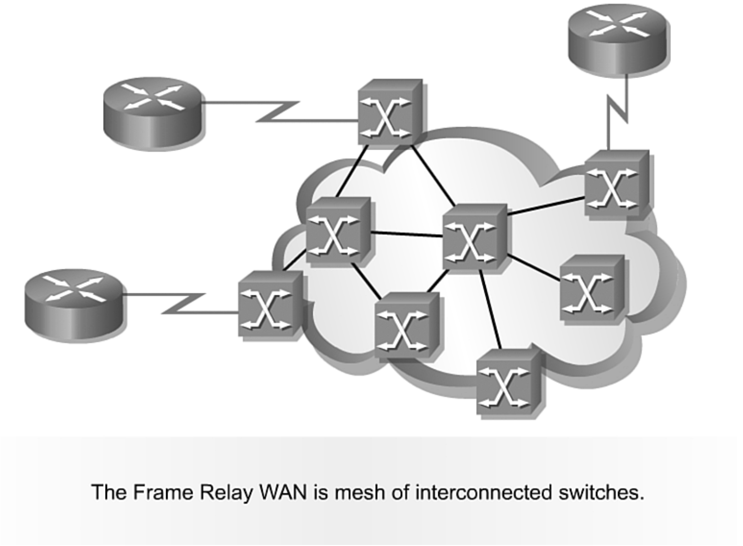
A Frame Relay network may be privately owned but is more commonly provided as a service by a public carrier. It typically consists of many geographically scattered Frame Relay switches interconnected by trunk lines, as shown in Figures 78 and 79.

**Figure 78** Frame Relay Switches Interconnected by Trunk Lines



The Frame Relay WAN is mesh of interconnected switches.

**Figure 79** Frame Relay Switches Interconnected by Trunk Lines



The Frame Relay WAN is mesh of interconnected switches.

Frame Relay is often used to interconnect LANs. When this is the case, a router on each LAN is the DTE. These routers have a serial connection, such as a T1/E1 leased line, to a Frame Relay switch at the carrier's nearest point of presence. The Frame Relay switch is a DCE device. Frames from one DTE are moved via DCEs, across the network, for delivery to the other DTE.

Computing equipment not on a LAN may also send data across a Frame Relay network. The computing equipment uses a Frame Relay access device (FRAD) as the DTE.

## Lesson 5.2: Basic Frame Relay Configuration

See Chapter 15, "Frame Relay," of the Cisco Press Companion Guide, Third Edition, for more information.

This lesson explains how to configure a basic Frame Relay permanent virtual circuit (PVC), as shown in Figures 80 and 81. Frame Relay is configured on a serial interface, and the default encapsulation type is the Cisco proprietary version of HDLC. To change the encapsulation to Frame Relay, use the **encapsulation frame-relay** [*cisco* | *ietf*] command.

**Figure 80** Frame Relay Overview

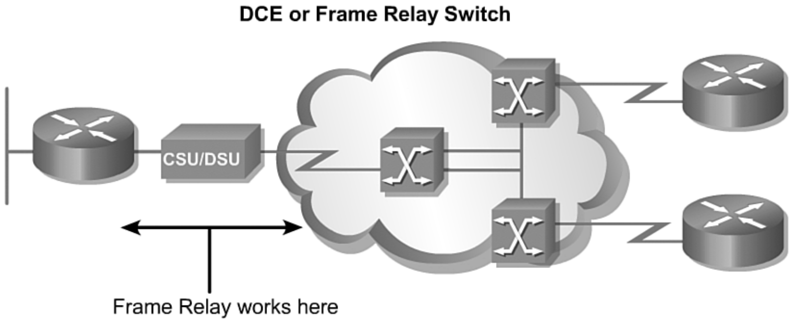
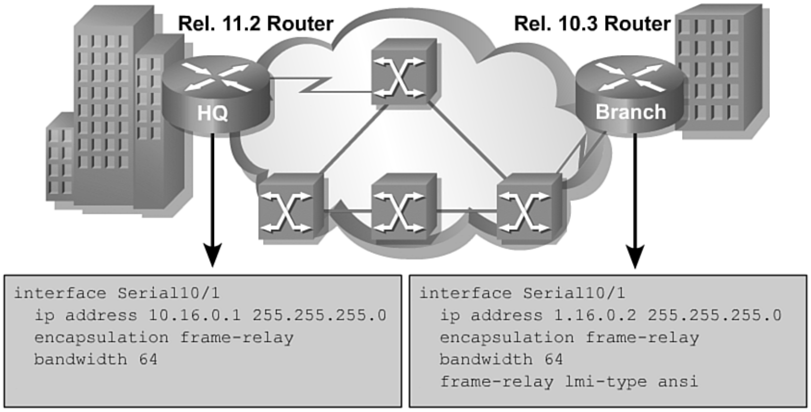


**Figure 81** Configuring Basic Frame Relay



```
interface Serial10/1
  ip address 10.16.0.1 255.255.255.0
  encapsulation frame-relay
  bandwidth 64
```

```
interface Serial10/1
  ip address 1.16.0.2 255.255.255.0
  encapsulation frame-relay
  bandwidth 64
  frame-relay lmi-type ansi
```

| | |
|---|---|
| *cisco* | Uses the Cisco proprietary Frame Relay encapsulation. Use this option if connecting to another Cisco router. Many non-Cisco devices also support this encapsulation type. This is the default. |
| *ietf* | Sets the encapsulation method to comply with the Internet Engineering Task Force (IETF) standard RFC 1490. Select this if connecting to a non-Cisco router. |

Cisco's proprietary Frame Relay encapsulation uses a 4-byte header, with 2 bytes to identify the data-link connection identifier (DLCI) and 2 bytes to identify the packet type. Use IETF Frame Relay encapsulation to connect to other vendors. RFCs 1294 and 1490 define the IETF standard.

Set an IP address on the interface using the **ip address** command. Set the bandwidth of the serial interface using the **bandwidth** command (using the kbps format). This command notifies the routing protocol that bandwidth is statically configured on the link. The bandwidth value is used by Interior Gateway Routing Protocol (IGRP), Enhanced Interior Gateway Routing Protocol (EIGRP), and Open Shortest Path First (OSPF) to determine the metric of the link. This command also affects bandwidth utilization statistics, which you can find by using the **show interfaces** command.

You can establish and configure the Local Management Interface (LMI) connection with the **frame-relay lmi-type** [*ansi* | *cisco* | *q933a*] command. This command is only needed if using Cisco IOS Release 11.1 or earlier; with IOS Release 11.2 or later, the LMI type is autosensed, so no configuration is needed. The default LMI type is Cisco. The LMI type is set on a per-interface basis and displays in the output of the **show interfaces** command.

These configuration steps are the same regardless of the network layer protocols operating across the network.

## Module 6—Introduction to Network Administration

### Lesson 6.1: Workstations and Servers

See Chapter 16, "Introduction to Network Administration,"of the Cisco Press Companion Guide, Third Edition, for more information.

The first PCs were designed as standalone desktop systems. The operating system (OS) software enabled one user at a time to access files and system resources. The user had physical access to the PC. As PC-based computer networks gained popularity in the workplace, software companies developed specialized network operating systems (NOSs). Developers designed NOSs to provide file security, user privileges, and resource sharing among multiple users. The explosive growth of the Internet compelled developers to build the NOS of today around Internet-related technologies and services such as the World Wide Web.

Within a decade, networking has become of central importance to desktop computing. The distinction between modern desktop OSs, now loaded with networking features and services, and their NOS counterparts has blurred. Now, most popular OSs, such as Microsoft Windows 2000 and Linux, are found on high-powered network servers and on the desktops of end users.

Your knowledge of several different OSs will help you to select the “proper” OS, one that offers the wide range of services needed. Therefore, this lesson covers UNIX, Linux, Mac OS X, and several Windows OSs.

A workstation is a client computer that is used to run applications and is connected to a server from which it obtains data shared with other computers. A server is a computer that runs a network operating system (NOS). A workstation uses special software, such as a network shell program, to perform the following tasks:

- Intercept user data and application commands
- Decide whether the command is for the local operating system or for the NOS
- Direct the command to the local operating system or to the network interface card (NIC) for processing and transmission onto the network
- Deliver transmissions from the network to the application running on the workstation

Windows NT/2000/XP Professional operating systems can run on a personal computer. Any system that is running one of these operating systems is referred to as either a workstation or a server. A PC is a system running any of the other popular operating systems originally designed for the PC such as DOS, Windows 95, or Windows 98.

UNIX or Linux can serve as a desktop operating system but are most commonly found on high-end computers. These workstations are employed in engineering and scientific applications, which require dedicated high-performance computers. Some of the specific applications typically run on UNIX workstations include the following:

- Computer-aided design (CAD)
- Electronic circuit design
- Weather-data analysis
- Computer graphics animation
- Telecommunications equipment management

Most current desktop operating systems include networking capabilities and support multi-user access. For this reason, it is becoming more common to classify computers and operating systems based on the types of applications the computer runs. Such a classification reflects the role or function that the computer plays, such as workstation or server. Typical desktop or low-end workstation applications might include word processing, spreadsheets, and financial management. On high-end workstations, the applications might include graphical design or equipment management and others as listed previously.

The term *diskless workstation* refers to a special class of computer designed to run on a network. As the name implies, it has no disk drives but does have a monitor, keyboard, memory, booting instructions in ROM, and a NIC. The software that establishes a network connection is loaded from the bootable ROM chip located on the NIC.

Because a diskless workstation does not have disk drives, you cannot upload data from the workstation or download anything to it. A diskless workstation cannot pass on a virus to the network, nor can you use it to take data from the network (for instance, by copying information to a disk drive). As a result, diskless workstations offer greater security than ordinary workstations. For this reason, diskless workstations are used in networks where security is paramount.

Laptops can also serve as workstations on a LAN and can be connected through a docking station, external LAN adapter, or a PCMCIA card. A docking station is an add-on device that turns a laptop into a desktop.

In a network operating system (NOS) environment, many client systems access and share the resources of one or more servers. Desktop client systems are equipped with their own memory and peripheral devices, such as a keyboard, monitor, and a disk drive. The server systems must support multiple concurrent users and multiple tasks as clients make demands on the server for remote resources.

NOSs have additional network management tools and features that are designed to support access by large numbers of simultaneous users. On all but the smallest networks, NOSs are installed on powerful servers. Many users, known as clients, share these servers. Servers usually have high-capacity, high-speed disk drives, large amounts of RAM, high-speed NICs, and in some cases multiple CPUs. These servers are typically configured to use the Internet family of protocols, TCP/IP, and offer one or more TCP/IP services.

Servers running NOSs are also used to authenticate users and provide access to shared resources. These servers are designed to handle requests from many clients simultaneously. Before a client can access the server resources, the client must be identified and be authorized to use the resource. Identification and authorization is achieved by assigning each client an account name and password. The account name and password are then verified by an authentication service acting as a sentry to guard access to the network. By centralizing user accounts, security, and access control, server-based networks simplify the work of network administration.

Servers are typically larger systems with additional memory to support multiple tasks that are all active, or resident, in memory at the same time. Additional disk space is required on servers to hold shared files and to function as an extension to the internal memory on the system. Servers also typically require extra expansion slots on their system boards to connect shared devices, such as printers and multiple network interfaces.

Another feature of systems capable of acting as servers is the processing power. Ordinarily, computers have a single CPU, which executes the instructions that make up a given task or process. To work efficiently and deliver fast responses to client requests, an NOS server requires a powerful CPU to execute its tasks or programs. Single-processor systems with one CPU can meet the needs of most servers if the CPU has the necessary speed. To achieve higher execution speeds, some systems are equipped with more than one processor. Such systems are called multiprocessing systems. Multiprocessing systems are capable of executing multiple tasks in parallel by assigning each task to a different processor. The aggregate amount of work that the server can perform in a given time is greatly enhanced in multiprocessor systems.

## Lesson 6.1: Network Management

See Chapter 16, "Introduction to Network Administration," of the Cisco Press Companion Guide, Third Edition, for more information.

Effective management of LANs and WANs is the key element to maintaining a productive environment in the networking world. As more services become available to more users, the performance of networks suffers. Network administrators, through constant monitoring, must recognize and be able to rectify problems before they become noticeable to the end users.

Various tools and protocols enable administrators to monitor the network on a local and remote basis. A comprehensive understanding of these tools is critical to effective network management.

As a network evolves and grows, it becomes a more critical and indispensable resource to the organization. However, the more resources the network offers its users and the more complex the network gets, the more things that can go wrong. Loss of network resources, or even to have the network perform poorly, is not acceptable to the users. The network administrator must actively manage the network, diagnose problems, prevent situations from occurring, and provide the best network performance possible for the users. At some point, networks become too large to manage without automated network management tools.

Network management tasks include the following:

- Monitor network availability
- Improve automation
- Monitor response time

- Maintain security
- Reroute traffic
- Restore capability
- Register users

The driving forces, or goals, of network management are as follows:

- **Control corporate assets—**Unless network resources are effectively controlled, they will not provide the payback that management requires.
- **Control complexity—**With massive growth in the number of network components, users, interfaces, protocols, and vendors, loss of control of the network and its resources threatens management.
- **Improve service—**Users expect the same or improved service as the network grows and the resources become more distributed.
- **Balance various needs—**Users must be provided with various applications at a given level of support, with specific requirements in the areas of performance, availability, and security.
- **Reduce downtime—**Network administrators, through effective redundant design, must ensure high availability of resources.
- **Control costs—**Network administrators must monitor and control resource utilization so that user needs can be satisfied at a reasonable cost.

## Module 7—Emerging Technologies

### Lesson 7.1: Basics of Optical Networks

See Chapter 17, "Optical Networking Fundamentals," of the Cisco Press Companion Guide, Third Edition, for more information.

Optical networks are an extremely efficient means of transporting data, video, and voice. Optical networks are not affected by electrical interference and may be used in a variety of topologies. This module covers the use of optical fiber in the backbone structure of LANs and MANs and discusses how optical fiber is used in WANs to cover long distances around the globe.

Optical fiber provides fast, reliable transport of information, high bandwidth availability, and network scalability. Optical networks use light pulses over fiber to achieve transfer speeds up to 10 Gbps.

This module introduces some of the advanced technologies used in fiber networking. These technologies are being developed to continue improving the performance and scalability of fiber installations.

Networks must be able to transmit data, voice, and video quickly, efficiently, and cost effectively. In comparison to any other resource, fiber optic is the most efficient medium for transmitting information. Fiber optic offers the highest bandwidth capacity for network traffic, and the technology is expanding exponentially.

The burgeoning Internet economy and surging amounts of data traffic call for scalable, multiservice platforms that can support next-generation, IP-based services and security. Today, service providers look for networks with the following characteristics:

- Capacity/scalability
- Reliability
- Accelerated profits
- Broad coverage
- End-to-end flexibility
- Adaptability
- Space efficiency
- Security

Fiber-optic technology is becoming the core of high-speed networks. Connecting both distant cities and many points within a metropolitan area, optical-fiber networks are made of thin glass strands that carry rapid light pulses, faster and more reliably than copper wires, at speeds up to 10 Gbps.

Information is transmitted at the speed of light in optical fiber. At approximately the diameter of a human hair, optical fiber is extremely strong and can carry a tremendous amount of information.

All communications systems have three things in common: a signal source, a medium for the signal to travel through, and a receiver. In fiber optics, the transmitter is a light source, the medium is a light guide or optical fiber, and the receiver is an optical sensor.

An optical transmitter is just a source of light, like a lightbulb. An electrical signal, such as a voice, data, or video transmission, is converted to light by using the electrical signal to turn the light on and off (for a digital signal) or to vary the intensity of the light (for an analog signal). In a digital signal, the presence of light is a one and the absence of light is a zero. In an analog signal, the intensity of the light matches the strength of the electrical signal level.

The receiver is a semiconductor that converts the light into a corresponding electrical signal. It is generically called an optical-to-electrical (O-E) converter. In a digital signal, the presence of light produces a higher electrical signal level. The absence of light produces a lower electrical signal level. In an analog system, the electrical level corresponds to the power level of the light received by the O-E converter.

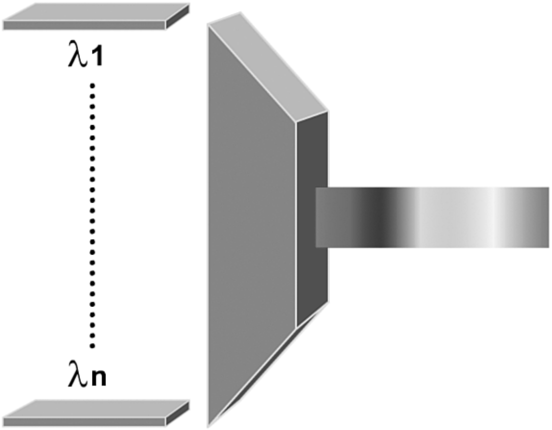
Even with no light reaching an O-E converter, an electrical signal will still exist, caused by the dark current that exists in all detector circuits. (*Dark current* refers to the electrical noise that naturally occurs on every electrical circuit.)

## Lesson 7.2: Optical Transmission and Multiplexing

See Chapter 17, "Optical Networking Fundamentals," of the Cisco Press Companion Guide, Third Edition, for more information.

In fiber optics, information is carried by modulating the light power, not the wavelength or frequency of the light. It is possible to mix two wavelengths of light on the same fiber without interference between them. This is called *wavelength-division multiplexing* (WDM). WDM allows more than one wavelength to be sent over a single fiber, thereby increasing the capacity, as shown in Figure 82.

**Figure 82** Wavelength-Division Multiplexing

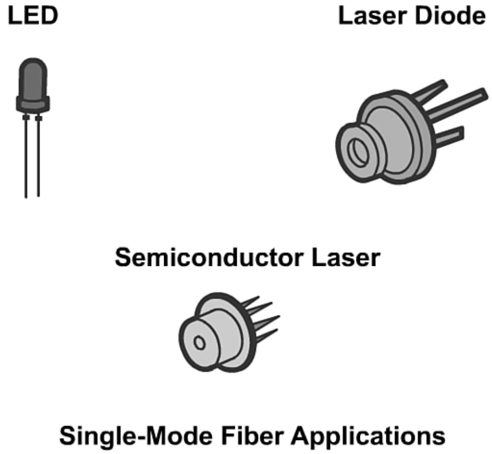


The light source used in the design of a system is an important consideration because it can be one of the most costly elements. The light source characteristics often constitute a strong limiting factor in the final performance of an optical link. Light emitting devices used in optical transmission must be compact, monochromatic, stable, and long lasting.

Figure 83 shows the two general types of light emitting devices used in optical transmission.

- Light emitting diodes (LEDs) and laser diodes
- Semiconductor lasers

**Figure 83** LED



LEDs are relatively slow devices suitable for use at speeds of less than 1 Gbps, exhibit a relatively wide spectrum width, and transmit light in a relatively wide cone. LEDs and laser diodes are inexpensive devices, often used in multimode fiber communications.

Semiconductor lasers have performance characteristics better suited to longer-distance and higher-bandwidth applications.