Interconnecting Cisco Network Devices, Part 1 (ICND1)

Foundation Learning Guide

ciscopress.com

Anthony Sequeira

Interconnecting Cisco Network Devices Part I (ICND1) Foundation Learning Guide

Anthony Sequeira CCIE #15626

Cisco Press

800 East 96th Street

Indianapolis, IN 46240

Interconnecting Cisco Network Devices Part I (ICND1) Foundation Learning Guide

Anthony Sequeira

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

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

First Printing June 2013

Library of Congress Cataloging-in-Publication Number: 2013938764

ISBN-13: 978-1-58714-376-2

ISBN-10: 1-58714-376-3

Warning and Disclaimer

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

The information is provided on an "as is" basis. The author, 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.

Corporate and Government Sales

The publisher offers excellent discounts on this book when ordered in quantity for bulk purchases or special sales, which may include electronic versions and/or custom covers and content particular to your business, training goals, marketing focus, and branding interests. For more information, please contact U.S. Corporate and Government Sales 1-800-382-3419.

corpsales@pearsontechgroup.com

For sales outside of the U.S., please contact: International Sales international@pearsoned.com.

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 feedback@ciscopress.com. Please make sure to include the book title and ISBN in your message.

We greatly appreciate your assistance.

Publisher: Paul Boger

Associate Publisher: Dave Dusthimer

Business Operation Manager, Cisco Press: Jan Cornelssen

Executive Editor: Brett Bartow

Development Editor: Eleanor C. Bru

Copy Editor: John Edwards

Technical Editors: Narbik Kocharians, Ryan Lindfield

Editorial Assistant: Vanessa Evans

Managing Editor: Sandra Schroeder

Project Editor: Mandie Frank

Proofreader: Sheri Cain

Indexer: Erika Millen

Cover Designer: Mark Shirar

Composition: Trina Wurst

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

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

About the Author

Anthony Sequeira, CCIE No. 15626, is a seasoned trainer and author regarding all levels and tracks of Cisco certification. Anthony formally began his career in the information technology industry in 1994 with IBM in Tampa, Florida. He quickly formed his own computer consultancy, Computer Solutions, and then discovered his true passion—teaching and writing about Microsoft and Cisco technologies.

Anthony joined Mastering Computers in 1996 and lectured to massive audiences around the world about the latest in computer technologies. Mastering Computers became the revolutionary online training company, KnowledgeNet, and Anthony trained there for many years.

Anthony is currently pursuing his second CCIE in the area of security and then his third Cisco Data Center! When not writing for Cisco Press, Anthony is a full-time instructor for the next-generation of KnowledgeNet, StormWind.com.

Anthony is an avid tennis player, is a private pilot, and enjoys getting beaten up by women and children at his and his daughter's martial arts school, www.sparta.fm.

About the Technical Reviewers

Narbik Kocharians, CCSI, CCIE No. 12410, (R&S, Security, SP) who has over 36 years of experience in the industry, is a Triple CCIE. He has designed, implemented, and supported numerous enterprise networks. Some of the international companies that Narbik has worked for are IBM, Carlton United Breweries, Australian Cable and Wireless, BP, and AMOCO. In the United States, he has worked for 20th Century Insurance, Home Savings of America, Verizon, TTI, Trinet Inc, Andersen Networking and Consulting, and many more. Narbik has been a dedicated CCIE instructor for over 12 years. In 2012, he was awarded the Sirius Top Quality Instructor Award.

Narbik Kocharians established his own school, Micronics Networking & Training, Inc. (www.micronicstraining.com) in 2006, where he teaches Cisco authorized courses from CCNA to CCIE in R&S, Security, SP, and Data Center.

Ryan Lindfield is a Certified Cisco Systems Instructor (CCSI) and consultant, based in Tampa, FL. His first position in 1996 was the systems administrator of Gorilla, a video game developer for Mattel and Disney. In 2001, he became an independent contractor, handling system, network, and security contracts for a wide range of customers, including commercial business (IBM), service providers (Verizon), government contractors (L3), and government entities (TSA). In 2003, he became associated with Boson as technical instructor and developer. Topics of expertise include routing and switching, offensive and defensive security, data center technologies, and IPv6. In 2008, with the help of his wife and fellow Cisco instructor, Desiree Lindfield, he launched Westchase Technologies, providing consulting and educational services for clients globally. On a typical day, he can be found providing authorized training for Computer Data, Global Knowledge, and Boson. When not in the classroom, he spends time designing, troubleshooting, and securing customer networks. He is a frequent attendee of Cisco Live, Blackhat, and Defcon conferences. Ryan holds the following certifications: CCNP, CCNP-Data Center, CCNP-Security, HP MASE Networking, VCP, CISSP, CEH, CHFI, GCFA, OSWP, CPTE, LPI-2, and a variety of Microsoft and CompTIA certifications.

Dedication

This book is dedicated to my amazingly talented daughter, Bella Joy Sequeira. Remember that you can do and become anything that you really put your mind to!

Acknowledgments

As always, thanks to my friend, fantasy baseball nemesis, and tequila-drinking partner, Brett Bartow of Cisco Press. Thanks also to Ellie Bru and everyone else at Cisco Press who worked so tirelessly to make this book a reality!

Thanks also to my friends Ryan Lindfield and Narbik Kocharians, who were kind enough to lend their technical editing services to this text. You guys helped this product tremendously!

Finally, thanks to everyone at StormWind.com for the time and the resources to make this book, and the videos for each chapter, a reality.

Contents at a Glance

Contents

Icons


Router
Switch
Multilayer Switch
Cisco ASA
Database
Cisco CallManager
IP
IP Phone
Access Server
VPN Concentrator
PIX Firewall
Router with Firewall
ATM Switch
CSU/DSU
Web Server
Server
Hub
Mac
PC
Laptop
100BaseT Hub
Repeater
Bridge
IP Telephony Router
uBR910 Cable DSU
Access Point
Modem
Host
Printer
Headquarters
Branch Office
Home Office
Ethernet Connection
Serial Line Connection
Network Cloud

Command Syntax Conventions

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

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

Introduction

This book was written to allow students to gain a comprehensive foundation in the many different technologies that are found in modern internetworks today. From the most critical network devices to their configuration and troubleshooting, this text provides students with numerous examples, illustrations, and real-world scenarios to gain confidence in the vast world of computer networking.

Goals and Methods

The goal of this book is simple: to provide the reader with a strong foundation in each aspect of computer networking covered in the ICND1 Version 2 blueprint from Cisco Systems.

To accomplish this goal, great pains were taken to reorganize, simplify, and elaborate on specific content from previous editions of this text. Review questions were added for each technology to endure mastery. In addition, two new sections were added to each chapter: Additional Resources and Production Network Simulation Questions. The Additional Resources sections each contain a link to a video created by the author. These videos both complement and supplement the material from the chapter. We hope you enjoy them! The Production Network Simulation Questions help bring the material to life and also challenge the reader with a more "real-world" review.

Who Should Read This Book

Three primary audiences were identified for this text:

- The network engineer needing to review key technologies that are important in today's networks.
- The reader who is interested in learning about computer networking and who might lack any previous experience in the subject.
- The reader who is interested in obtaining the Cisco CCNA Certification.

How This Book Is Organized

Although you could read this book from cover to cover, it is designed to be flexible and allow you to easily move between chapters and sections of chapters to cover only the material you need. If you intend to read all the chapters, the order in which they are presented is an excellent sequence.

Chapters 1 through 20 cover the following topics:

- Chapter 1, "The Functions of Networking": What are the key devices that make up a network today? And for that matter, what is so important about a computer network anyway? These questions and more are explored in this first chapter.
- Chapter 2, "The OSI and TCP/IP Models": While most students shudder at the thought of learning these important networking models, this chapter makes this pursuit simple—and perhaps even enjoyable!
- Chapter 3, "LANs and Ethernet": The local-area network and the Ethernet connections that help build it are some of the most important aspects to learn in modern networking. This chapter details these important technologies for the reader.
- Chapter 4, "Operating Cisco IOS Software": This chapter covers the basics of using the software that powers the majority of Cisco devices today.
- Chapter 5, "Switch Technologies": Switch technologies replaced the need for hubs in our network environments and, as such, are a critical component in the modern network. This chapter explores the inner workings of these important devices.
- Chapter 6, "VLANS and Trunks": VLANs permit the creation of broadcast domains (IP subnets) in the local-area network and are of critical importance. So are the trunk links that carry VLAN traffic from Cisco device to Cisco device. This chapter ensures that the reader is well versed in these important technologies.
- Chapter 7, "The TCP/IP Internet Layer": One of the key layers in the OSI model for any network engineer to master is the Internet layer. This chapter is dedicated to this important concept.
- Chapter 8, "IP Addressing and Subnets": What is one topic that many fear in the CCNA curriculum? The mastery of IP addressing—including subnetting. This chapter dispels these fears and provides simple instructions for creating the best IP addressing schemes for your small network.
- Chapter 9, "The TCP/IP Transport Layer": The transport layer of the OSI model is often misunderstood. This chapter ensures that readers can describe the importance and operation of this key layer.
- Chapter 10, "The Functions of Routing": Why is routing so important? How does it work? This chapter is a must-read for anyone who requires more information about these critical network devices called routers.
- Chapter 11, "The Packet Delivery Process": Everything that must occur when you type www.ciscopress.com in your web browser and press Enter is absolutely amazing. This chapter details the processes that occur when two systems communicate on a typical network today.

- Chapter 12, "Configuring a Cisco Router": In Chapter 10, you learn all about the functions that a router must perform, and how the device does it. In this chapter, you learn the basics of configuring a Cisco router to perform its important jobs!
- Chapter 13, "Static Routing": Static routes are extremely important in your network infrastructure. This chapter ensures that you can create them with accuracy and ease in your Cisco-based network.
- Chapter 14, "Dynamic Routing Protocols": There are many different implementations of routing protocols. This chapter sheds light on the different protocols and their differences.
- Chapter 15, "OSPF": OSPF is the most popular interior gateway protocol in use on the planet today. This chapter is dedicated to this important protocol and provides the reader with a strong foundation in this complex routing protocol.
- Chapter 16, "DHCP and NAT": How can we dynamically provide our workstations with their correct IP address information? What are we to do about the exhaustion of TCP/IP addresses today? These critical questions are answered in this chapter.
- Chapter 17, "Securing the Network": To be a CCNA, you must understand the basic concepts involved with network security. This chapter provides that knowledge!
- Chapter 18, "Managing Traffic with Access Control Lists": Access control lists are fundamental constructs in Cisco devices. If you want to master Cisco networking, you must be knowledgeable about these components.
- Chapter 19, "Introducing WAN Technologies": There are a wide variety of methods in use today for sending data long distances in the network. This chapter is dedicated to these various options and provides an overview of WANs for further more in-depth study.
- Chapter 20, "Introducing IPv6": The future of the TCP/IP protocol is here! And it is here to stay (at least for a while). This chapter educates the reader on IP version 6 and even gets him or her configuring this protocol in a dynamically routed network environment!

This page intentionally left blank

Chapter 3

LANs and Ethernet

This chapter includes the following sections:

- Chapter Objectives
- Understanding LANs
- Connecting to an Ethernet LAN
- Chapter Summary
- Additional Resources
- Review Questions
- Production Network Simulation Question 3-1

Local-area networks (LAN) tend to spoil us as network users. These collections of high-speed network equipment allow us to achieve remarkable speeds in accessing network data and information. LANs are a relatively low-cost means of sharing expensive resources. LANs allow multiple users in a relatively small geographic area to exchange files and messages and to access shared resources such as file servers. LANs have rapidly evolved into support systems that are critical to communications within an organization. This chapter will ensure that you are comfortable describing these important network structures.

This chapter also describes different Ethernet media options (copper and fiber), which are presented together with a description of the most common connectors and cable types. Ethernet frame structure is introduced, and important fields are described. MAC addresses and their function are also elaborated on.

Chapter Objectives

Upon completing this chapter, you will be able to describe LAN networks. You will also be able to describe common Ethernet technologies typically found within these important areas of the overall network. These abilities include meeting these objectives:

- Define a LAN
- Identify the components of a LAN
- Describe the types of Ethernet LAN connection media
- Describe the fields of an Ethernet frame
- Define the structure and function of MAC addresses

Understanding LANs

A local-area network is a common type of network found in home offices, small businesses, and large enterprises. Understanding how a LAN functions, including network components, frames, Ethernet addresses, and operational characteristics, is important for an overall knowledge of networking technologies.

This section describes LANs and provides fundamental knowledge about LAN characteristics, components, and functions. It also describes the basic operations of an Ethernet LAN and how frames are transmitted over it.

The Definition of a LAN

A LAN is a network of computers and other components located relatively close together in a limited area. LANs can vary widely in their size. A LAN might consist of only two computers in a home office or small business, or it might include hundreds of computers in a large corporate office or multiple buildings. Figure 3-1 shows some examples of LANs.

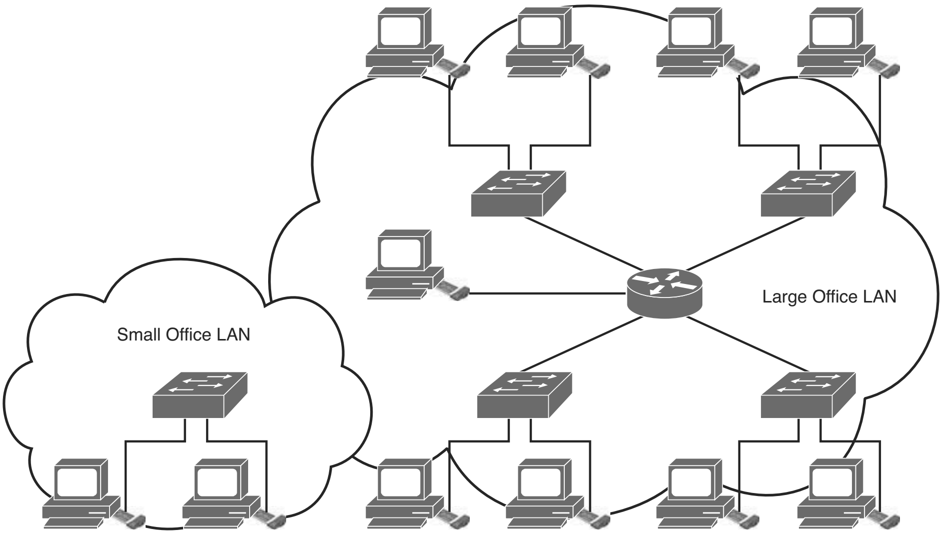

Figure 3-1 *Examples of LANs*

A small home business or a small office environment could use a small LAN to connect two or more computers and to connect the computers to one or more shared peripheral devices such as printers. A large corporate office could use multiple LANs to accommodate hundreds of computers and shared peripheral devices, for departments such as finance or operations, spanning many floors in an office complex.

Components of a LAN

Every LAN has specific components, including hardware, interconnections, and software. Figure 3-2 highlights some typical hardware components of a LAN.

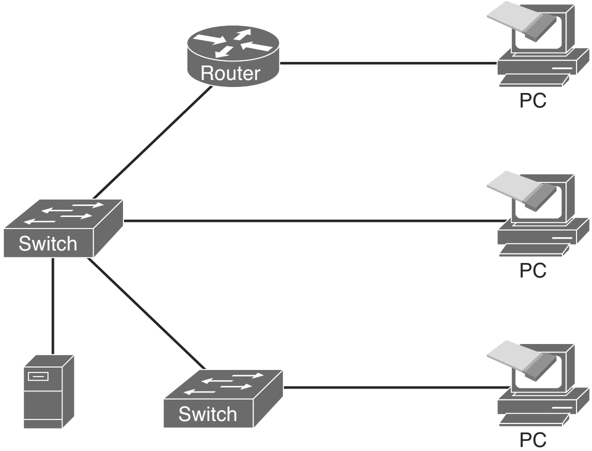

Figure 3-2 *Typical Components of a LAN*

Regardless of the size of the LAN, it requires these fundamental components for its operation:

- **Computers:** Computers serve as the endpoints in the network, sending and receiving data.
- **Interconnections:** Interconnections enable data to travel from one point to another in the network. Interconnections include these components:
  - **NICs:** Network interface cards (NIC) translate the data produced by the computer into a format that can be transmitted over the LAN.
  - **Network media:** Network media, such as cables or wireless media, transmit signals from one device on the LAN to another.
- **Network devices:** A LAN requires the following network devices:
  - **Hubs:** Hubs provide aggregation devices operating at Layer 1 of the OSI reference model. However, hubs have been replaced in this function by switches, and it is very rare to see hubs in any LAN these days.
  - **Ethernet switches:** Ethernet switches form the aggregation point for LANs. Ethernet switches operate at Layer 2 of the OSI reference model and provide intelligent distribution of frames within the LAN.
  - **Routers:** Routers, sometimes called gateways, provide a means to connect LAN segments. Routers operate at Layer 3 of the OSI reference model.
- **Protocols:** Protocols govern the way data is transmitted over a LAN and include the following:
  - Ethernet protocols
  - Internet Protocol (IP)
  - Internet Protocol version 6 (IPv6)
  - Address Resolution Protocol (ARP) and Reverse Address Resolution Protocol (RARP)
  - Dynamic Host Configuration Protocol (DHCP)

Functions of a LAN

LANs provide network users with communication and resource-sharing functions, including the following:

- **Data and applications:** When users are connected through a network, they can share files and even software application programs. This makes data more easily available and promotes more efficient collaboration on work projects.
- **Resources:** The resources that can be shared include both input devices, such as cameras, and output devices, such as printers.

- **Communication path to other networks:** If a resource is not available locally, the LAN, through a gateway, can provide connectivity to remote resources—for example, access to the web.

How Big Is a LAN?

A LAN can be configured in a variety of sizes, depending on the requirements of the environment in which it operates.

LANs can be of various sizes to fit different work requirements, including the following:

- **Small office/home office (SOHO):** The SOHO environment typically has only a few computers and some peripherals such as printers.
- **Enterprise:** The enterprise environment might include many separate LANs in a large office building or in different buildings on a corporate campus. In the enterprise environment, each LAN might contain hundreds of computers and peripherals..

Figure 3-3 demonstrates the dramatic differences that can exist with the size of LANs.

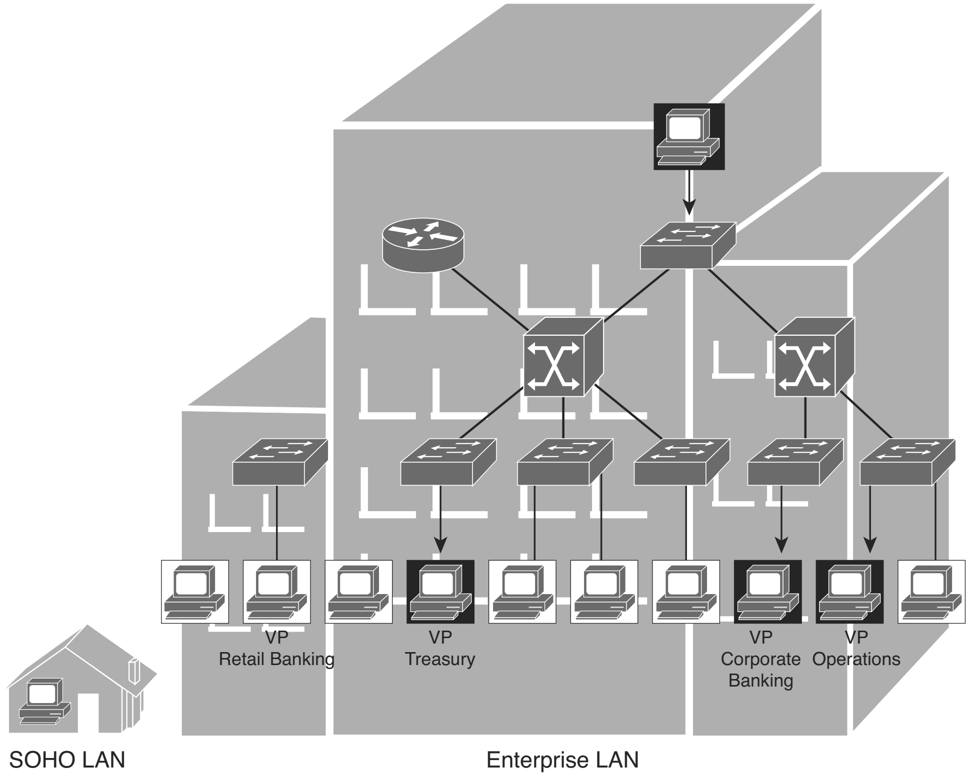

Figure 3-3 *Different LAN Sizes*

Ethernet

Ethernet is the most common type of LAN. It was originally developed in the 1970s by Digital Equipment Corporation (DEC), Intel, and Xerox (DIX) and was called DIX Ethernet. It later came to be called thick Ethernet (because of the thickness of the cable used in this type of network), and it transmitted data at 10 megabits per second (Mbps). The standard for Ethernet was updated in the 1980s to add more capability, and the new version of Ethernet was referred to as Ethernet Version 2 (also called Ethernet II).

The Institute of Electrical and Electronics Engineers (IEEE) is a professional organization that defines network standards. IEEE standards are the predominant LAN standards in the world today. In the mid-1980s, an IEEE workgroup defined new standards for Ethernet-like networks. The set of standards they created was called Ethernet 802.3 and was based on the carrier sense multiple access with collision detection (CSMA/CD) process. Ethernet 802.3 specified the physical layer (Layer 1) and the MAC portion of the data link layer (Layer 2). Today, this set of standards is most often referred to as simply "Ethernet."

Ethernet LAN Standards

Ethernet LAN standards specify cabling and signaling at both the physical and data link layers of the OSI reference model. This topic describes Ethernet LAN standards at the data link layer.

Figure 3-4 shows how LAN protocols map to the OSI reference model.

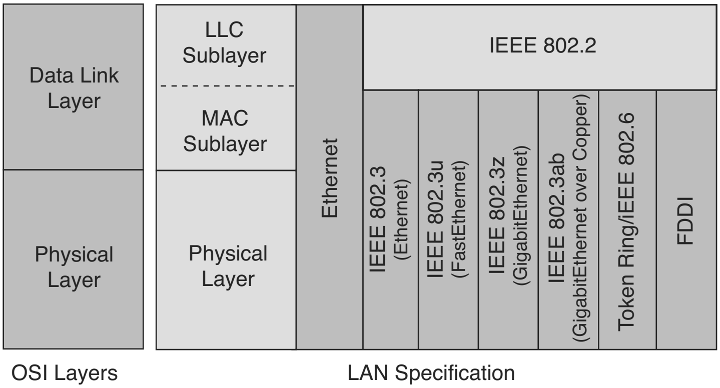

Figure 3-4 *Ethernet and the OSI Model*

The IEEE divides the OSI data link layer into two separate sublayers:

- **Logical link control (LLC):** Transitions up to the network layer
- **MAC:** Transitions down to the physical layer

LLC Sublayer

The IEEE created the LLC sublayer to allow part of the data link layer to function independently from existing technologies. This layer provides versatility in services to the network layer protocols that are above it, while communicating effectively with the variety of MAC and Layer 1 technologies below it. The LLC, as a sublayer, participates in the encapsulation process.

An LLC header tells the data link layer what to do with a packet when it receives a frame. For example, a host receives a frame and then looks in the LLC header to understand that the packet is destined for the IP protocol at the network layer.

The original Ethernet header (prior to IEEE 802.2 and 802.3) did not use an LLC header. Instead, it used a type field in the Ethernet header to identify the Layer 3 protocol being carried in the Ethernet frame.

MAC Sublayer

The MAC sublayer deals with physical media access. The IEEE 802.3 MAC specification defines MAC addresses, which uniquely identify multiple devices at the data link layer. The MAC sublayer maintains a table of MAC addresses (physical addresses) of devices. To participate on the network, each device must have a unique MAC address.

The Role of CSMA/CD in Ethernet

Ethernet signals are transmitted to every station connected to the LAN, using a special set of rules to determine which station can "talk" at any particular time. This topic describes that set of rules.

Ethernet LANs manage the signals on a network by CSMA/CD, which is an important aspect of Ethernet. Figure 3-5 illustrates the CSMA/CD process.

In an Ethernet LAN, before transmitting, a computer first listens to the network media. If the media is idle, the computer sends its data. After a transmission has been sent, the computers on the network compete for the next available idle time to send another frame. This competition for idle time means that no one station has an advantage over another on the network.

Stations on a CSMA/CD LAN can access the network at any time. Before sending data, CSMA/CD stations listen to the network to determine whether it is already in use. If it is, the CSMA/CD stations wait. If the network is not in use, the stations transmit. A collision occurs when two stations listen for network traffic, hear none, and transmit simultaneously (see Figure 3-5). In this case, both transmissions are damaged, and the stations must retransmit at some later time. CSMA/CD stations must be able to detect collisions to know that they must retransmit.

When a station transmits, the signal is referred to as a carrier. The NIC senses the carrier and consequently refrains from broadcasting a signal. If no carrier exists, a waiting station knows that it is free to transmit. This is the "carrier sense" part of the protocol.

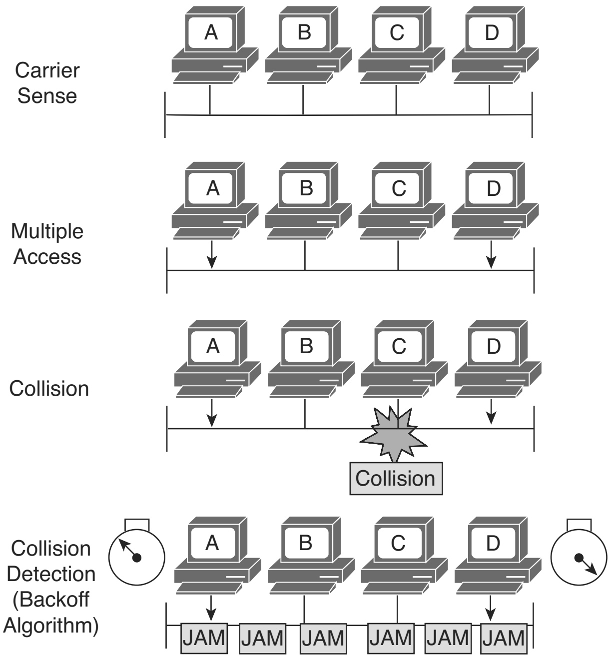

Figure 3-5 *CSMA/CD Process*

The extent of the network segment over which collisions occur is referred to as the collision domain. The size of the collision domain has an impact on efficiency and therefore on data throughput. In today's LANs, switches have replaced hubs. The reason this occurs is that switches create tiny collision domains containing just one device. This eliminates the potential for collisions. This process is often called "microsegmentation" of the network.

In the CSMA/CD process, priorities are not assigned to particular stations, so all stations on the network have equal access. This is the "multiple access" part of the protocol. If two or more stations attempt a transmission simultaneously, a collision occurs. The stations are alerted of the collision, and they execute a backoff algorithm that randomly schedules retransmission of the frame. This scenario prevents the machines from repeatedly attempting to transmit at the same time. Collisions are normally resolved in microseconds. This is the "collision detection" part of the protocol.

While collisions are resolved quickly, it is still advantageous to eliminate them entirely from the network. This allows much more efficient communications. This is accomplished through the use of switches as described earlier.

Ethernet Frames

Bits that are transmitted over an Ethernet LAN are organized into frames. In Ethernet terminology, the "container" into which data is placed for transmission is called a *frame*. The frame contains header information, trailer information, and the actual data that is being transmitted.

Figure 3-6 illustrates all the fields that are in a MAC layer of the Ethernet frame, which include the following:

- **Preamble:** This field consists of 7 bytes of alternating 1s and 0s, which synchronize the signals of the communicating computers.
- **Start-of-frame (SOF) delimiter:** This field contains bits that signal the receiving computer that the transmission of the actual frame is about to start and that any data following is part of the packet.
- **Destination address:** This field contains the address of the NIC on the local network to which the packet is being sent.
- **Source address:** This field contains the address of the NIC of the sending computer.
- **Type/length:** In Ethernet II, this field contains a code that identifies the network layer protocol. In 802.3, this field specifies the length of the data field. The protocol information is contained in 802.2 fields, which are at the LLC layer. The newer 802.3 specifications have allowed the use of Ethertype protocol identifiers when not using the 802.2 field.
- **Data and pad:** This field contains the data that is received from the network layer on the transmitting computer. This data is then sent to the same protocol on the destination computer. If the data is too short, an adapter adds a string of extraneous bits to "pad" the field to its minimum length of 46 bytes.
- **Frame check sequence (FCS):** This field includes a checking mechanism to ensure that the packet of data has been transmitted without corruption.

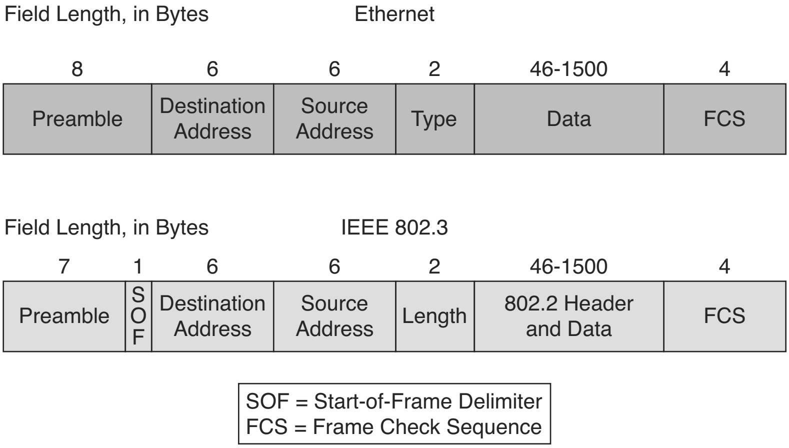

Figure 3-6 *Ethernet Frames*

Ethernet Frame Addressing

Communications in a network occur in three ways: unicast, broadcast, and multicast. Ethernet frames are addressed accordingly. Figure 3-7 shows forms of Ethernet communications.

The three major types of network communications are as follows:

- **Unicast:** Communication in which a frame is sent from one host and addressed to one specific destination. In a unicast transmission, you have just one sender and one receiver. Unicast transmission is the predominant form of transmission on LANs and within the Internet.
- **Broadcast:** Communication in which a frame is sent from one address to all other addresses. In this case, you have just one sender, but the information is sent to all connected receivers. Broadcast transmission is essential when sending the same message to all devices on the LAN.
- **Multicast:** Communication in which information is sent to a specific group of devices or clients. Unlike broadcast transmission, in multicast transmission, clients must be members of a multicast group to receive the information.

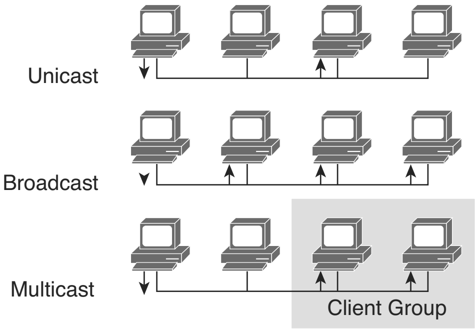

Figure 3-7 *Ethernet Communications*

Ethernet Addresses

The address used in an Ethernet LAN, which is associated with the network adapter, is the means by which data is directed to the proper receiving location. Figure 3-8 shows the format of an Ethernet MAC address.

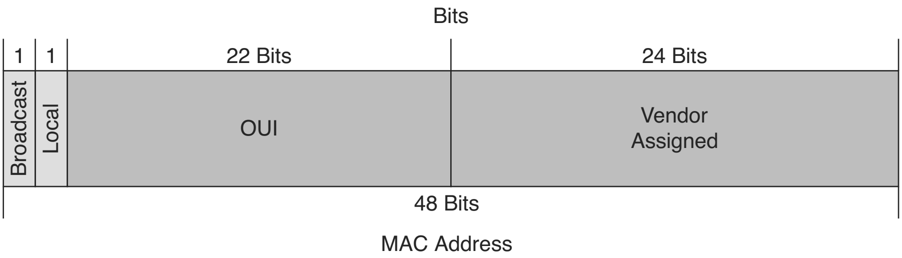

Figure 3-8 *Ethernet MAC Address*

The address that is on the NIC is the MAC address, often referred to as the burned-in address (BIA), and some vendors allow the modification of this address to meet local needs. A 48-bit Ethernet MAC address has two components:

- **24-bit Organizational Unique Identifier (OUI):** The letter *O* identifies the manufacturer of the NIC. The IEEE regulates the assignment of OUI numbers. Within the OUI, the two following bits have meaning only when used in the destination address:
  - **Broadcast or multicast bit:** This indicates to the receiving interface that the frame is destined for all or a group of end stations on the LAN segment.
  - **Locally administered address bit:** Normally the combination of OUI and a 24-bit station address is universally unique; however, if the address is modified locally, this bit should be set.
- **24-bit vendor-assigned end station address:** This uniquely identifies the Ethernet hardware.

MAC Addresses and Binary-Hexadecimal Numbers

The MAC address plays a specific role in the function of an Ethernet LAN. The MAC sublayer of the OSI data link layer handles physical addressing issues, and the physical address is a number in hexadecimal format that is actually burned into the NIC. This address is referred to as the MAC address, and it is expressed as groups of hexadecimal digits that are organized in pairs or quads, such as the following: 00:00:0c:43:2e:08 or 0000:0c43:2e08. Figure 3-9 shows the MAC address format compared to the MAC frame.

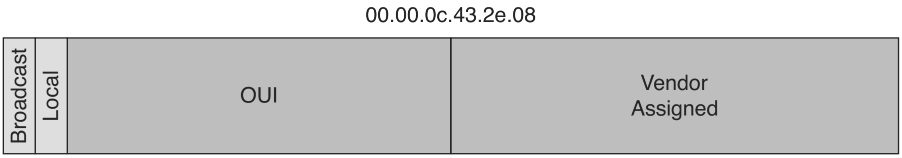

Figure 3-9 *Hexadecimal MAC Address*

Each device on a LAN must have a unique MAC address to participate in the network. The MAC address identifies the location of a specific computer on a LAN. Unlike other kinds of addresses used in networks, the MAC address should *not* be changed unless you have some specific need.

Connecting to an Ethernet LAN

In addition to understanding the components of an Ethernet LAN and the standards that govern its architecture, you need to understand the connection components of an Ethernet LAN. This section describes the connection components of an Ethernet LAN, including network interface cards (NIC) and cable.

Ethernet Network Interface Cards

A NIC is a printed circuit board that provides network communication capabilities to and from a personal computer on a network. Figure 3-10 shows an example of a NIC.

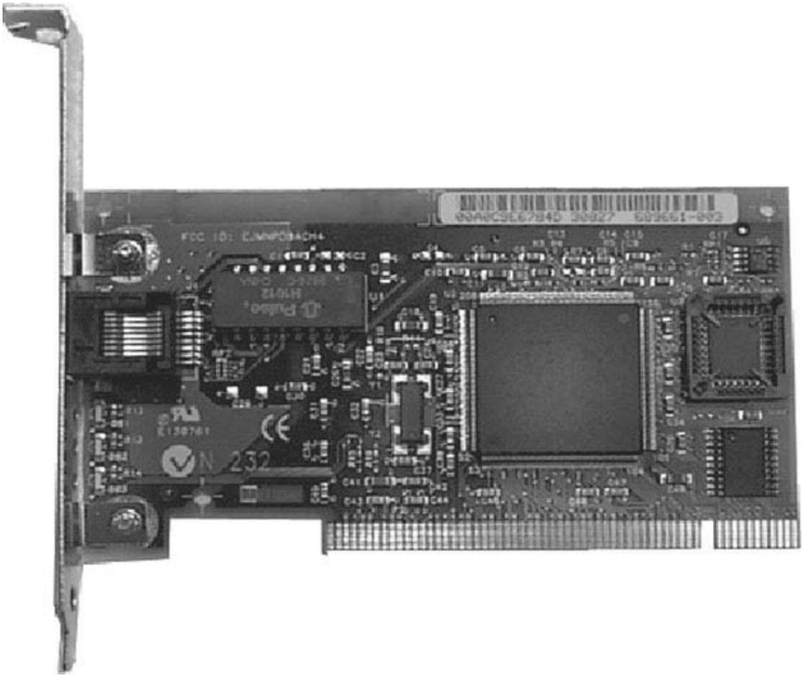

Figure 3-10 *Network Interface Card*

Also called a LAN adapter, the NIC plugs into a motherboard and provides a port for connecting to the network. The NIC constitutes the computer interface with the LAN.

The NIC communicates with the network through a serial connection, and with the computer through a parallel connection. When a NIC is installed in a computer, it requires an interrupt request line (IRQ), an input/output (I/O) address, a memory space within the operating system (such as DOS or Windows), and drivers (software) that allow it to perform its function. An IRQ is a signal that informs a central processing unit (CPU) that an event needing its attention has occurred. An IRQ is sent over a hardware line to the microprocessor. An example of an interrupt request being issued is when a key is pressed on a keyboard, and the CPU must move the character from the keyboard to RAM. An I/O address is a location in memory used by an auxiliary device to enter data into or retrieve data from a computer.

The MAC address is burned onto each NIC by the manufacturer, providing a unique, physical network address.

Ethernet Media and Connection Requirements

Distance and time dictate the type of Ethernet connections required. This section describes the cable and connector specifications used to support Ethernet implementations.

The cable and connector specifications used to support Ethernet implementations are derived from the EIA/TIA standards body. The categories of cabling defined for Ethernet are derived from the EIA/TIA-568 (SP-2840) Commercial Building Telecommunications Wiring Standards. EIA/TIA specifies an RJ-45 connector for unshielded twisted-pair (UTP) cable.

The important difference to note is the media used for 10-Mbps Ethernet versus 100-Mbps Fast Ethernet. In networks today, where you see a mix of 10- and 100-Mbps requirements, you must be aware of the need to change over to UTP Category 5 to support Fast Ethernet.

Connection Media

Several types of connection media can be used in an Ethernet LAN implementation. Figure 3-11 shows typical connection types.

The most common type of connection media is the RJ-45 connector and jack illustrated in Figure 3-11. The letters RJ stand for registered jack, and the number “45” refers to a specific physical connector that has eight conductors.

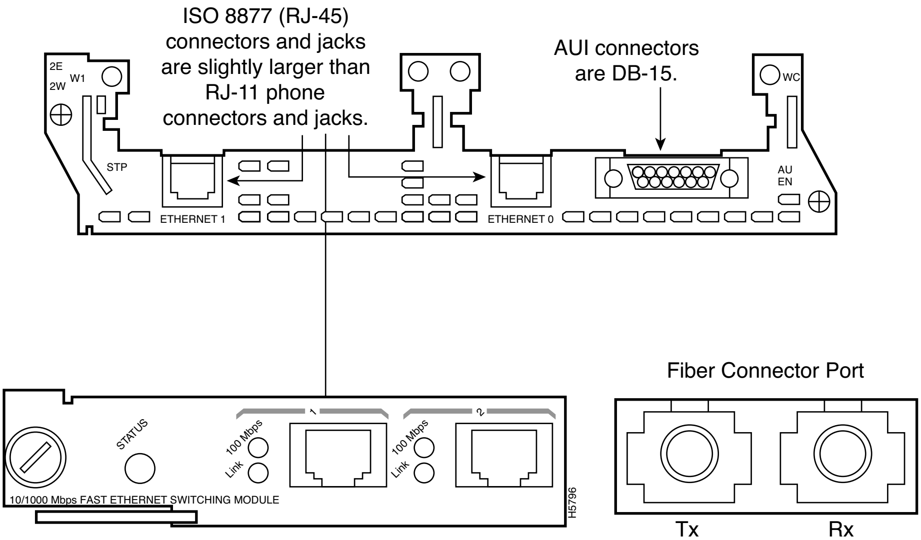

Figure 3-11 *Connection Types*

A Gigabit Interface Converter (GBIC), shown in Figure 3-12, is a hot-swappable I/O device that plugs into a Gigabit Ethernet port. A key benefit of using a GBIC is that it is interchangeable, allowing you the flexibility to deploy other 1000BASE-X technology without having to change the physical interface or model on the router or switch. GBICs support UTP (copper) and fiber-optic media for Gigabit Ethernet transmission.

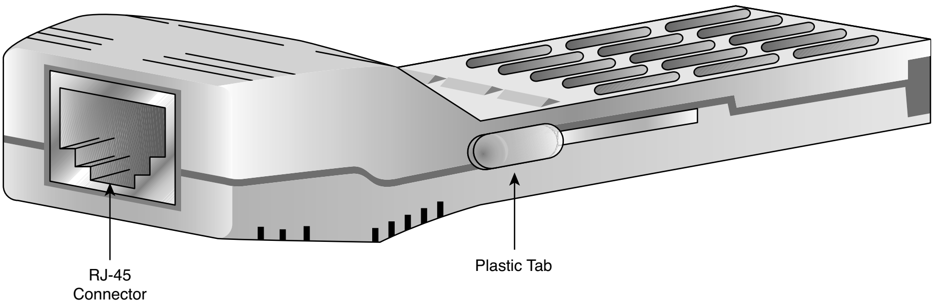

Figure 3-12 *1000BASE-T GBIC*

Typically, GBICs are used in the LAN for uplinks and are normally used for the backbone. GBICs are also seen in remote networks.

The fiber-optic GBIC, shown in Figure 3-13, is a transceiver that converts serial electric currents to optical signals and converts optical signals to digital electric currents.

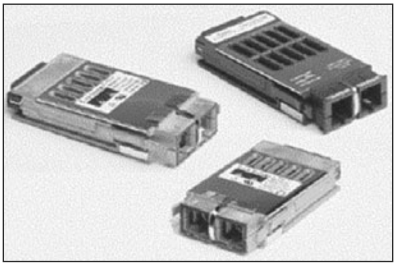

Figure 3-13 *Fiber GBIC*

Optical GBICs include these types:

- Short wavelength (1000BASE-SX)
- Long wavelength/long haul (1000BASE-LX/LH)
- Extended distance (1000BASE-ZX)

Unshielded Twisted-Pair Cable

Twisted-pair is a copper wire–based cable that can be either shielded or unshielded. UTP cable is frequently used in LANs. Figure 3-14 shows an example of a UTP cable.

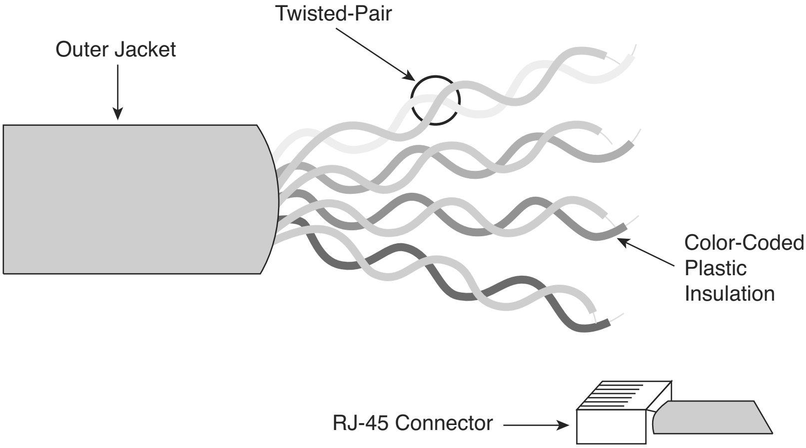

Figure 3-14 *UTP Cable*

UTP cable is a four-pair wire. Each of the eight individual copper wires in UTP cable is covered by an insulating material. In addition, the wires in each pair are twisted around each other. The advantage of UTP cable is its ability to cancel interference, because the twisted wire pairs limit signal degradation from electromagnetic interference (EMI) and radio frequency interference (RFI). To further reduce crosstalk between the pairs in UTP cable, the number of twists in the wire pairs varies. Both UTP and shielded twisted-pair (STP) cable must follow precise specifications regarding how many twists or braids are permitted per meter.

UTP cable is used in a variety of types of networks. When used as a network medium, UTP cable has four pairs of either 22- or 24-gauge copper wire. UTP used as a network medium has an impedance of 100 ohms, differentiating it from other types of twisted-pair wiring, such as that used for telephone wiring. Because UTP cable has an external diameter of approximately 0.43 cm, or 0.17 inches, its small size can be advantageous during installation. Also, because UTP can be used with most major network architectures, it continues to grow in popularity.

Here are the categories of UTP cable:

- **Category 1:** Used for telephone communications; not suitable for transmitting data
- **Category 2:** Capable of transmitting data at speeds of up to 4 Mbps
- **Category 3:** Used in 10BASE-T networks; can transmit data at speeds up to 10 Mbps
- **Category 4:** Used in Token Ring networks; can transmit data at speeds up to 16 Mbps
- **Category 5:** Capable of transmitting data at speeds up to 100 Mbps
- **Category 5e:** Used in networks running at speeds up to 1000 Mbps (1 Gbps)
- **Category 6:** Consists of four pairs of 24-gauge copper wires, which can transmit data at speeds of up to 1000 Mbps
- **Category 6a:** Used in networks running at speeds up to 10 Gbps

The most commonly used categories in LAN environments today are Categories 1 (used primarily for telephony), 5, 5e, and 6.

UTP Implementation

For a UTP implementation in a LAN, you must determine the EIA/TIA type of cable needed and also whether to use a straight-through or crossover cable. This topic describes the characteristics and uses of straight-through and crossover cables, as well as the types of connectors used when UTP is implemented in a LAN. Figure 3-15 shows an RJ-45 connector.

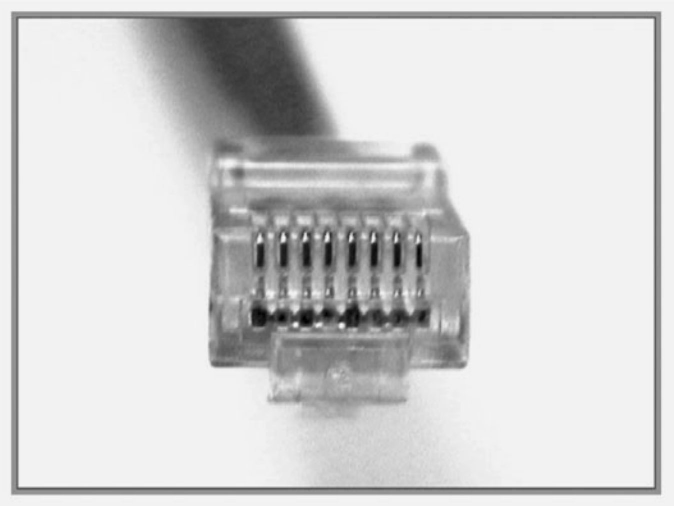

Figure 3-15 *RJ-45 Connector*

If you look at the RJ-45 transparent-end connector, you can see eight colored wires, twisted into four pairs. Four of the wires (two pairs) carry the positive or true voltage and are considered “tip” (T1 through T4); the other four wires carry the inverse of false voltage grounded and are called “ring” (R1 through R4). *Tip* and *ring* are terms that originated in the early days of the telephone. Today, these terms refer to the positive and negative wires in a pair. The wires in the first pair in a cable or a connector are designated as T1 and R1, the second pair as T2 and R2, and so on.

The RJ-45 plug is the male component, crimped at the end of the cable. As you look at the male connector from the front, the pin locations are numbered from 8 on the left to 1 on the right.

The jack is the female component in a network device, wall, cubicle partition outlet, or patch panel.

In addition to identifying the correct EIA/TIA category of cable to use for a connecting device (depending on which standard is being used by the jack on the network device), you need to determine which of the following to use:

- A straight-through cable (either T568A or T568B at each end)
- A crossover cable (T568A at one end; T568B at the other)

In Figure 3-16, the RJ-45 connectors on both ends of the cable show all the wires in the same order. If the two RJ-45 ends of a cable are held side by side in the same orientation, the colored wires (or strips or pins) can be seen at each connector end. If the order of the colored wires is the same at each end, the cable type is straight-through.

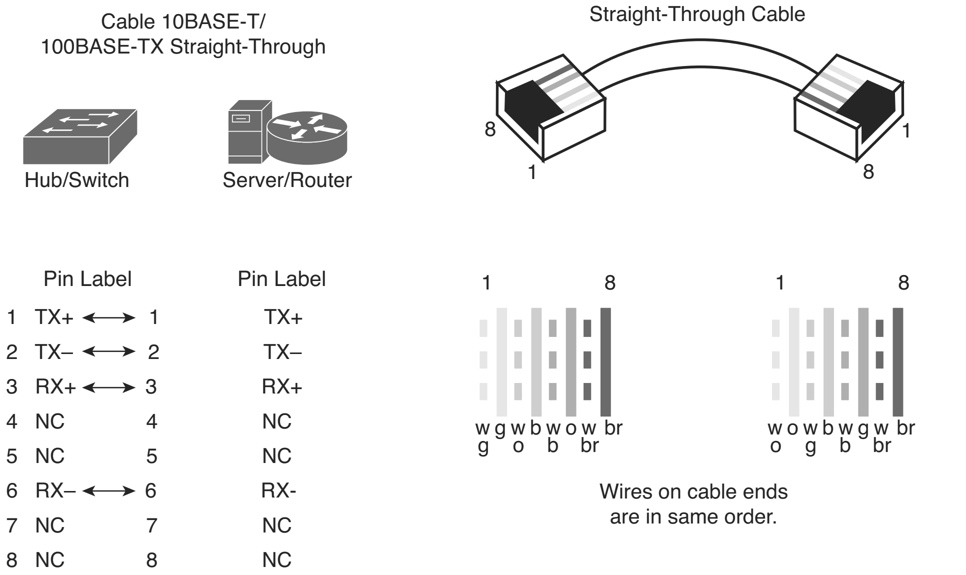

Figure 3-16 *Straight-Through Cable*

With crossover cables, the RJ-45 connectors on both ends show that some of the wires on one side of the cable are crossed to a different pin on the other side of the cable. Specifically, for Ethernet, pin 1 at one RJ-45 end should be connected to pin 3 at the other end. Pin 2 at one end should be connected to pin 6 at the other end, as shown in the Figure 3-17.

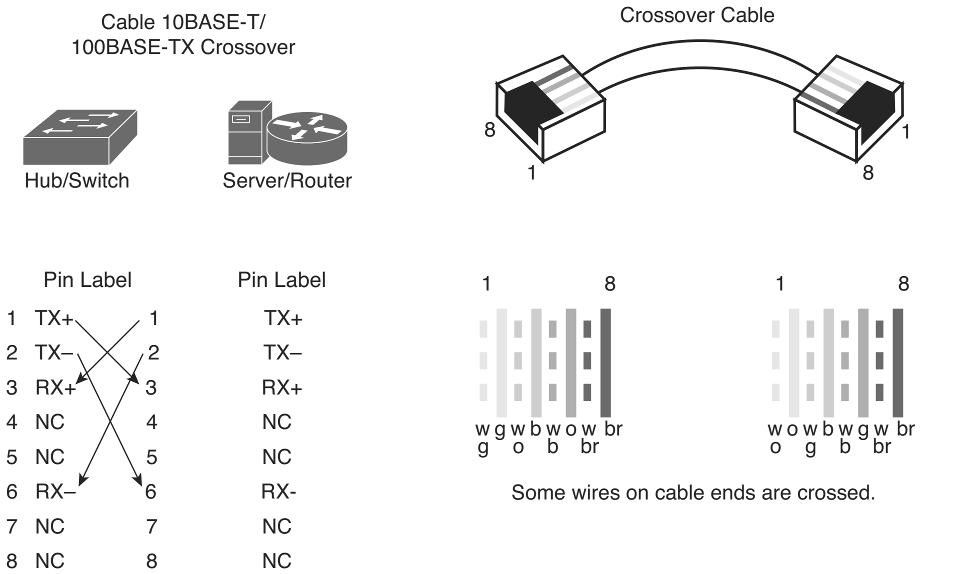

Figure 3-17 *Crossover Cable*

Figure 3-18 shows the guidelines for choosing which type of cable to use when interconnecting Cisco devices. In addition to verifying the category specification on the cable, you must determine when to use a straight-through or crossover cable.

Use straight-through cables for the following cabling:

- Switch to router
- Switch to PC or server
- Hub to PC or server

Use crossover cables for the following cabling:

- Switch to switch
- Switch to hub
- Hub to hub
- Router to router
- Router Ethernet port to PC NIC
- PC to PC

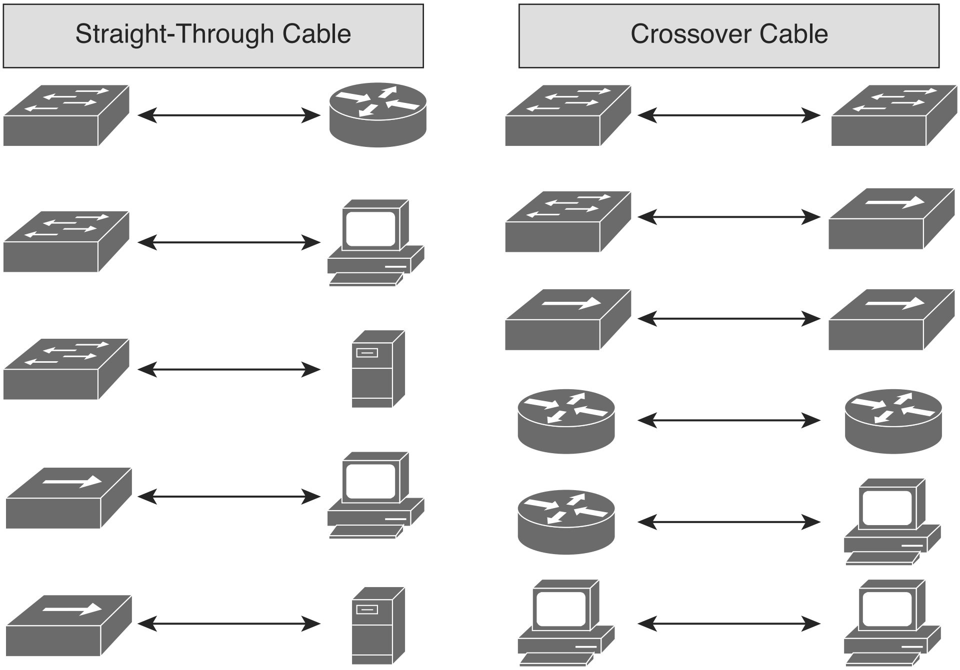

Figure 3-18 *When to Use a Straight-Through Cable Versus a Crossover Cable*

Auto-MDIX

After reading the previous section, you might be concerned about when you are cabling your network, you might make a critical mistake! Imagine, just one wrong type of cable, and your entire LAN might fail to access key resources. Fortunately, there is great news because of a new technology called Auto-MDIX. Auto-MDIX stands for automatic medium-dependent interface crossover, a feature that lets the interface automatically discover whether the wrong cable is installed. A switch that supports the Auto-MDIX feature detects the wrong cable and causes the switch to swap the pair it uses for transmitting and receiving. This solves the cabling problem, and the switch is able to communicate just fine regardless of the fact that you connected the "wrong" cable. Obviously, this new technology is very desirable and is making its way to more and more Cisco devices all the time.

Optical Fiber

An optical fiber is a flexible, transparent fiber that is made of very pure glass (silica) and is not much bigger in diameter than a human hair. It acts as a waveguide, or "light pipe," to transmit light between the two ends of the fiber. Optical fibers are widely used in fiber-optic communications, which permit transmission over longer distances and at higher bandwidths (data rates) than other forms of communication. Fibers are used instead of metal wires because signals travel along them with less loss and with immunity to electromagnetic interference. Figure 3-19 shows an example of optical fiber.

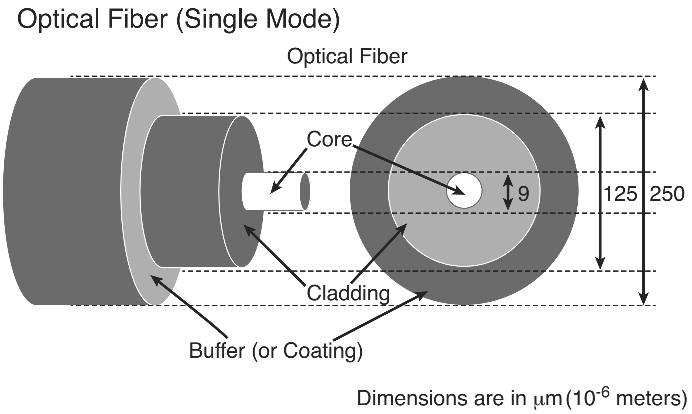

Figure 3-19 *Optical Fiber*

The two fundamental components that allow a fiber to confine light are the core and the cladding. Most of the light travels from the beginning to the end inside the core. The cladding around the core provides confinement. The diameters of the core and cladding are shown in this illustration, but the core diameter can vary for different fiber types. In this case, the core diameter of 9 µm is very small—the diameter of a human hair is about 50 µm. The outer diameter of the cladding is a standard size of 125 µm. Standardizing the size means that component manufacturers can make connectors for all fiber-optic cables.

The third element in this picture is the buffer (coating), which has nothing to do with the confinement of the light in the fiber. Its purpose is to protect the glass from scratches and moisture. The fiber-optic cable can be easily scratched and broken, like a glass pane. If the fiber is scratched, the scratch could propagate and break the fiber. Another important aspect is the need to keep the fiber dry.

The most significant difference between single-mode fiber (SMF) and multimode fiber (MMF) is in the ability of the fiber to send light for a long distance at high bit rates. In general, MMF is used for shorter distances at a lower bit rate than SMF. For long-distance communications, SMF is preferred. There are many variations of fiber for both MMF and SMF. Figure 3-20 shows the two fiber types.

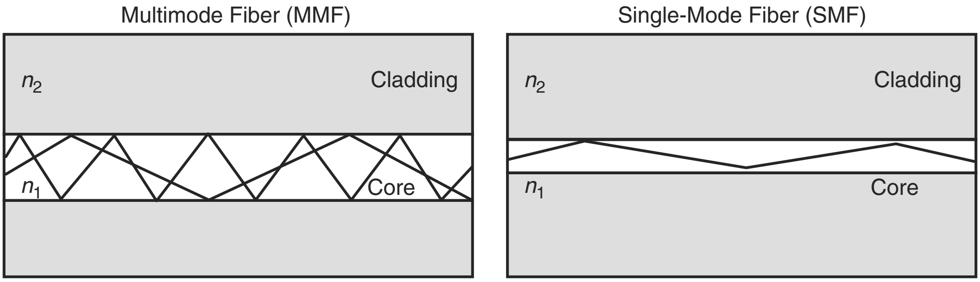

Figure 3-20 *Fiber-Optic Types*

The most significant physical difference is in the size of the core. The glass in the two fibers is the same, and the index of refraction change is similar. The core diameter can make a major difference. The diameter of the fiber cladding is universal for matching fiber ends.

The effect of having different-size cores in fiber is that the two fiber types will support different ways for the light to get through the fiber. The left image illustrates MMF. MMF supports multiple ways for the light from one source to travel through the fiber (the source of the designation "multimode"). Each path can be thought of as a mode.

For SMF, the possible ways for light to get through the fiber have been reduced to one, a "single mode." It is not exactly one, but that is a useful approximation. Table 3-1 summarizes the characteristics of MMF and SMF.

Table 3-1 *Summarizing MMF and SMF Characteristics*

MMF Characteristics	SMF Characteristics
LED transmitter usually used	Larger transmitter usually used
Lower bandwidth and speed	Higher bandwidth and speed
Shorter distances	Longer distances
Less expensive	More expensive

An optical fiber connector terminates the end of an optical fiber. A variety of optical fiber connectors are available. The main differences among the types of connectors are dimensions and methods of mechanical coupling. Generally, organizations standardize on one kind of connector, depending on the equipment that they commonly use, or they standardize per type of fiber (one for MMF, one for SMF). Taking into account all the generations of connectors, about 70 connector types are in use today. Figure 3-21 shows some common connector types.

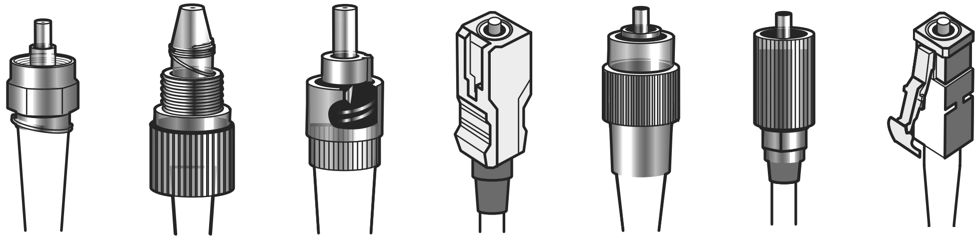

Figure 3-21 *Common Fiber-Optic Connector Types*

There are three types of connectors:

- Threaded
- Bayonet
- Push-pull

These materials are used for connectors:

- Metal
- Plastic sleeve

Most common connectors are classified as these types:

- **ST:** Typical for patch panels (for their durability)
- **FC:** Typical used by service providers for patch panels
- **SC:** Typical for enterprise equipment
- **LC:** Typical for enterprise equipment, commonly used on Small Form-Factor Pluggable (SFP) modules

In data communications and telecommunications applications today, small-form-factor connectors (for example, LCs) are replacing the traditional connectors (for example, SCs), mainly to pack more connectors on the faceplate and thus reduce system footprints.

Chapter Summary

LANs are a critical component in computer networks today. While these structures come in many different sizes, they are always used to carry data at speeds as fast as possible over short geographic distances.

Ethernet is the most common type of LAN used today. Standards unique to Ethernet specify Ethernet LAN cabling and signaling at both the physical and data link layers of the OSI reference model. Bits that are transmitted over an Ethernet LAN are organized into frames. Ethernet LANs manage the signals on a network using a process called CSMA/CD.

A NIC or LAN adapter plugs into a motherboard and provides an interface for connecting to the network. The MAC address is burned onto each NIC by the manufacturer, providing a unique, physical network address that permits the device to participate in the network.

The cable and connector specifications used to support Ethernet implementations are derived from the EIA/TIA standards body. The categories of cabling defined for Ethernet are derived from the EIA/TIA-568 (SP2840) Commercial Building Telecommunications Wiring Standards. Several connection media are used for Ethernet, with RJ-45 and GBIC being the most common.

A GBIC is a hot-swappable I/O device that plugs into a Gigabit Ethernet port on a network device to provide a physical interface.

UTP cable is a four-pair wire. Each of the eight individual copper wires in UTP cable is covered by an insulating material, and the wires in each pair are twisted around each other. A crossover cable connects between similar devices like router to router, PC to PC, or switch to switch. A straight-through cable connects between dissimilar devices like switch to router or PC to switch.

This chapter also examined fiber-optic media. Optical fiber is a flexible, transparent fiber that is made of very pure glass (silica) and is not much bigger than a human hair. It acts as a waveguide, or "light pipe," to transmit light between the two ends of the fiber. Optical fibers are widely used in fiber-optic communications, which permit transmission over longer distances and at higher bandwidths (data rates) than other forms of communication.

Additional Resources

- Gigabit Ethernet, Wikipedia: http://en.wikipedia.org/wiki/Gigabit_Ethernet
- How Fiber Optics Work, How Stuff Works: http://computer.howstuffworks.com/fiber-optic.htm

Review Questions

Use the questions here to review what you learned in this chapter. The correct answers and solutions are found in Appendix A, "Answers to Chapter Review Questions."

1. What organization is responsible for Ethernet standards?
   a. ISO
   b. IEEE
   c. EIA
   d. IEC
2. What are the characteristics of Ethernet 802.3? (Choose three.)
   a. Based on the CSMA/CD process
   b. Is a standard that has been replaced by Ethernet II
   c. Specifies the physical layer (Layer 1)
   d. Developed in the mid-1970s
   e. Specifies the MAC portion of the data link layer (Layer 2)
   f. Also referred to as thick Ethernet
3. Which statement about an Ethernet address is accurate?
   a. The address used in an Ethernet LAN directs data to the proper receiving location.
   b. The source address is the 4-byte hexadecimal address of the NIC on the computer that is generating the data packet.
   c. The destination address is the 8-byte hexadecimal address of the NIC on the LAN to which a data packet is being sent.
   d. Both the destination and source addresses consist of a 6-byte hexadecimal number.
4. Which statement about MAC addresses is accurate?
   a. A MAC address is a number in hexadecimal format that is physically located on the NIC.
   b. A MAC address is represented by binary digits that are organized in pairs.
   c. It is not necessary for a device to have a unique MAC address to participate in the network.
   d. The MAC address can never be changed.
5. Which statement about NICs is accurate?
   a. The NIC plugs into a USB port and provides a port for connecting to the network.
   b. The NIC communicates with the network through a serial connection and communicates with the computer through a parallel connection.
   c. The NIC communicates with the network through a parallel connection and communicates with the computer through a serial connection.
   d. A NIC is also referred to as a switch adapter.

6. Which minimum category of UTP is required for Ethernet 1000BASE-T?
   a. Category 3
   b. Category 4
   c. Category 5
   d. Category 5e

7. Match the UTP categories to the environments in which they are most commonly used.

   ___1. Category 1
   ___2. Category 2
   ___3. Category 3
   ___4. Category 4
   ___5. Category 5
   ___6. Category 5e
   ___7. Category 6
   ___8. Category 6e

   a. Capable of transmitting data at speeds up to 100 Mbps
   b. Used in networks running at speeds up to 1000 Mbps (1 Gbps)
   c. Consists of four pairs of 24-gauge copper wires, which can transmit data at speeds up to 1000 Mbps
   d. Used for telephone communications; not suitable for transmitting data
   e. Used in Token Ring networks; can transmit data at speeds up to 16 Mbps
   f. Capable of transmitting data at speeds up to 4 Mbps
   g. Used in 10BASE-T networks; can transmit data at speeds up to 10 Mbps
   h. Used in networks running at speeds up to 10 Gbps

8. Which type of UTP cable would you use to connect a router to a PC to have the devices pass user data?
   a. Straight-through
   b. Crossover
   c. Rollover
   d. None of these options are correct.

9. Which type of UTP cable would you use to connect a switch to another switch?
   a. Straight-through
   b. Crossover
   c. Rollover
   d. None of these options are correct.

10. What type of optical fiber provides higher speeds and bandwidths?

   a. MMF

   b. SMF

   c. MNF

   d. GMF

Production Network Simulation Question 3-1

Your colleague has come to you desperate for help. He needs to know what type of Ethernet cable he needs to use in each of these segments he is responsible for:

1. The PC to the switch
2. The switch to another switch
3. The switch to a router
4. The router to another router

None of these devices support the Auto-MDIX feature, so provide him with the correct cable type for each instance.

Index

Symbols

A

B

C

D

E

F

G

H

J-K

L

M

N

O

P

Q

R

S

T

U

V

W-X-Y-Z