Network Basics

CCNA Companion Guide

Cisco | Networking Academy®
Mind Wide Open™

Network Basics Companion Guide

Cisco Networking Academy

Cisco Press
800 East 96th Street
Indianapolis, Indiana 46240 USA

Network Basics Companion Guide

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

Printed in the United States of America

First Printing November 2013

Library of Congress Cataloging-in-Publication data is on file.

ISBN-13: 978-1-58713-317-6

ISBN-10: 1-58713-317-2

Warning and Disclaimer

This book is designed to provide information about the Cisco Networking Academy Network Basics course. 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 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.

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

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

Publisher
Paul Boger

Associate Publisher
Dave Dusthimer

Business Operation Manager, Cisco Press
Jan Cornelssen

Executive Editor
Mary Beth Ray

Managing Editor
Sandra Schroeder

Development Editor
Ellie C. Bru

Project Editor
Mandie Frank

Copy Editor
Bill McManus

Technical Editor
Tony Chen

Editorial Assistant
Vanessa Evans

Designer
Mark Shirar

Composition
Trina Wurst

Indexer
Ken Johnson

Proofreader
Charlotte Kughen

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 the United States, 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 email at feedback@ciscopress.com. Please make sure to include the book title and ISBN in your message.

We greatly appreciate your assistance.

Americas 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: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Europe Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: +31 0 800 020 0791
Fax: +31 0 20 357 1100

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 Contributing Authors

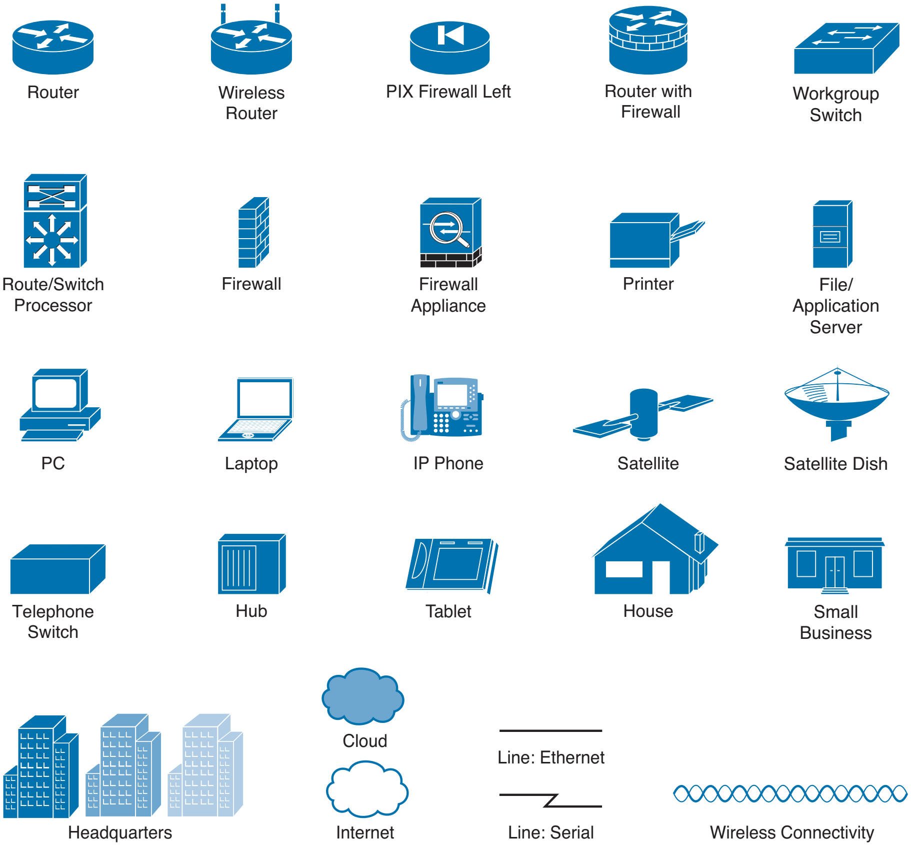
Antoon (Tony) W. Rufi is Campus Director of Academic Affairs, ECPI University, Newport News, Virginia. Tony is a networking professional who retired from the U.S. Air Force in June 2000 after 29 years. He worked on communication systems. Since retirement, Tony has worked for ECPI University teaching a variety of networking courses. The courses he has led include CCNA, CCNP, and Fundamentals of Network Security in the Cisco Academy at ECPI University, as well as numerous courses in the university's Cloud Computing program. Tony is a PhD candidate, Applied Management and Decision Science, with an Information Systems Management specialty at Walden University.

Rick McDonald is an Associate Professor in the Information Systems department at the University of Alaska Southeast, in Ketchikan, Alaska, where he teaches computer and networking courses. He specializes in developing and delivering networking courses via e-learning. Rick worked in the airline industry for several years before returning to full-time teaching. He taught CCNA and CCNP courses in North Carolina before moving to Alaska in 2003.

Contents at a Glance

Contents

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).
- *Italic* indicates arguments for which you supply actual values.
- Vertical bars (|) separate alternative, mutually exclusive elements.
- Square brackets ([ ]) indicate an optional element.
- Braces ({ }) indicate a required choice.
- Braces within brackets ([{ }]) indicate a required choice within an optional element.

Introduction

Network Basics Companion Guide is the official supplemental textbook for the CCNA Routing and Switching Network Basics course in the Cisco Networking Academy Program.

As a textbook, this book provides a ready reference to explain the same networking concepts, technologies, protocols, and devices that are covered in the online course. This book emphasizes key topics, terms, and activities and provides some alternate explanations and examples as compared with the online course. You can use the online curriculum as directed by your instructor and then use this *Companion Guide*'s study tools to help solidify your understanding of all the topics.

Who Should Read This Book

This book is intended for students in the Cisco Networking Academy CCNA Routing and Switching Network Basics course. The goal of this book is to introduce you to fundamental networking concepts and technologies. In conjunction with the online course materials, this book will assist you in developing the skills necessary to plan and implement small networks across a range of applications. The specific skills covered in each chapter are described at the start of each chapter.

Book Features

The educational features of this book focus on supporting topic coverage, readability, and practice of the course material to facilitate your full understanding of the course material.

Topic Coverage

The following features give you a thorough overview of the topics covered in each chapter so that you can make constructive use of your study time:

- **Objectives:** Listed at the beginning of each chapter, the objectives reference the core concepts covered in the chapter. The objectives match the objectives stated in the corresponding chapters of the online curriculum; however, the question format in the *Companion Guide* encourages you to think about finding the answers as you read the chapter.

How To

- **"How-to" feature:** When this book covers a set of steps that you need to perform for certain tasks, the text lists the steps as a how-to list. When you are studying, the icon helps you easily refer to this feature as you skim through the book.

- **Chapter summaries:** Each chapter includes a summary of the chapter's key concepts. It provides a synopsis of the chapter and serves as a study aid.
- **"Practice" section:** The end of each chapter includes a full list of all the Labs, Class Activities, and Packet Tracer Activities covered in that chapter.

Readability

The following features have been updated to assist your understanding of the networking vocabulary:

- **Key terms:** Each chapter begins with a list of key terms, along with a page-number reference for each key term. The key terms are listed in the order in which they are explained in the chapter. This handy reference allows you to find a term, flip to the page where the term appears, and see the term used in context. The Glossary defines all the key terms.
- **Glossary:** This book contains an all-new Glossary with more than 250 terms.

Practice

Practice makes perfect. This new *Companion Guide* offers you ample opportunities to put what you learn to practice. You will find the following features valuable and effective in reinforcing the instruction that you receive:

- **Check Your Understanding questions and answer key:** Updated review questions are presented at the end of each chapter as a self-assessment tool. These questions match the style of questions that you see in the online course. Appendix A, "Check Your Understanding Answer Key," provides an answer key to all the questions and includes an explanation of each answer.

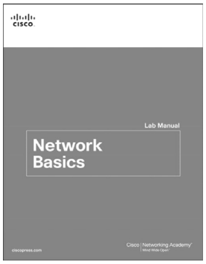
Packet Tracer
□ Activity

Video

- **Labs and Activities:** Throughout each chapter you will be directed to the online course to take advantage of the activities created to reinforce concepts. In addition, the end of each chapter includes a "Practice" section that collects a list of all the labs and activities to provide practice with the topics introduced in the chapter. The Labs and Class Activities are available in the companion *Network Basics Lab Manual* (978-158713-313-8). The Packet Tracer Activities PKA files are found in the online course.
- **Page references to online course:** After each heading you will see, for example, (1.1.2.3). This number refers to the page number in the online course so that you can easily jump to that spot online to view a video, practice an activity, perform a lab, or review a topic.

Lab Manual

The supplementary book *Network Basics Lab Manual* (978-158713-313-8), contains all the Labs and Class Activities from the course.



cisco

Lab Manual

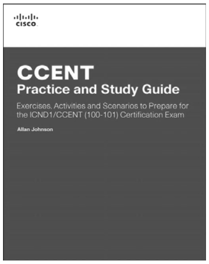
Network
Basics

ciscopress.com

Cisco | Networking Academy®
Mind Wide Open™

Practice and Study Guide

Additional study exercises, activities, and scenarios are available in the new *CCENT Practice and Study Guide* (978-158713-345-9) and *CCNA Routing and Switching Practice and Study Guide* (978-158713-344-2) books by Allan Johnson. Each Practice and Study Guide coordinates with the recommended curriculum sequence—one focusing on courses 1 and 2 (ICND1/CCENT topics) and the second focusing on courses 3 and 4 (ICND2/CCNA topics).

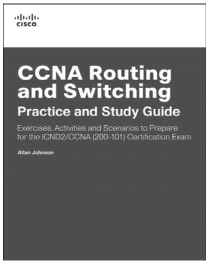


cisco

CCENT
Practice and Study Guide

Exercises, Activities and Scenarios to Prepare for
the ICND1/CCENT (100-101) Certification Exam

Allan Johnson



cisco

CCNA Routing
and Switching
Practice and Study Guide

Exercises, Activities and Scenarios to Prepare
for the ICND2/CCNA (200-101) Certification Exam

Allan Johnson

About Packet Tracer Software and Activities

Packet Tracer
□ Activity

Interspersed throughout the chapters you'll find many activities to work with the Cisco Packet Tracer tool. Packet Tracer enables you to create networks, visualize how packets flow in the network, and use basic testing tools to determine whether the network would work. When you see the Packet Tracer Activity icon, you can use Packet Tracer with the listed file to perform a task suggested in this book. The activity files are available in the course. Packet Tracer software is available only through the Cisco Networking Academy website. Ask your instructor for access to Packet Tracer.

How This Book Is Organized

This book corresponds closely to the Cisco Networking Academy Network Basics course and is divided into 11 chapters, one appendix, and a glossary of key terms:

- **Chapter 1, "Exploring the Network":** This chapter introduces the platform of data networks upon which our social and business relationships increasingly depend. The material lays the groundwork for exploring the services, technologies, and issues encountered by network professionals as they design, build, and maintain the modern network.
- **Chapter 2, "Configuring a Network Operating System":** This chapter references a basic network topology, consisting of two switches and two PCs, to demonstrate the use of Cisco IOS.
- **Chapter 3, "Network Protocols and Communications":** In this chapter you will learn about two layered models that describe network rules and functions. These models, as well as the standards that make the networks work, are discussed here to give context to detailed study of the model layers in the following chapters.
- **Chapter 4, "Application Layer":** This chapter explores the role of the application layer and how the applications, services, and protocols within the application layer make robust communication across data networks possible.
- **Chapter 5, "Transport Layer":** This chapter examines the role of the transport layer in encapsulating application data for use by the network layer. The concepts of reliable data delivery and multiple application conversations are also introduced.
- **Chapter 6, "Network Layer":** This chapter focuses on the role of the network layer. It examines how it divides networks into groups of hosts to manage the flow of data packets within a network. It also covers how communication between networks is facilitated through routing processes.
- **Chapter 7, "IP Addressing":** This chapter describes the structure of IP addresses and their application to the construction and testing of IP networks and subnetworks.
- **Chapter 8, "Subnetting IP Networks":** This chapter examines the creation and assignment of IP network and subnetwork addresses through the use of the subnet mask.
- **Chapter 9, "Network Access":** This chapter introduces the general functions of the data link layer and the protocols associated with it. It also covers the general functions of the physical layer and the standards and protocols that manage the transmission of data across local media.

- **Chapter 10, "Ethernet":** This chapter examines the characteristics and operation of Ethernet as it has evolved from a shared-media, contention-based data communications technology to today's high-bandwidth, full-duplex technology.
- **Chapter 11, "It's A Network":** Having considered the services that a data network can provide to the human network, examined the features of each layer of the OSI model and the operations of TCP/IP protocols, and looked in detail at Ethernet, a universal LAN technology, this chapter discusses how to assemble these elements together in a functioning network that can be maintained
- **Appendix A, "Check Your Understanding Answer Key":** This appendix lists the answers to the "Check Your Understanding" review questions included at the end of each chapter.
- **Glossary:** The Glossary provides you with definitions for all the key terms identified in each chapter.

CHAPTER 1

Exploring the Network

Objectives

Upon completion of this chapter, you will be able to answer the following questions:

- How do networks affect the way we interact when we learn, work, and play?
- How do networks support communication?
- What is a converged network?
- What are the four requirements for a reliable network?
- How are network devices used?
- How do local-area network (LAN) devices compare to wide-area network (WAN) devices?
- What is the basic structure of the Internet?
- How do LANs and WANs interconnect the Internet?
- What is the effect of Bring Your Own Device (BYOD) use, online collaboration, video, and cloud computing on a business network?
- How do expanding networking trends affect security considerations?
- What are the three Cisco enterprise architectures and how do they meet the needs of an evolving network environment?

Key Terms

This chapter uses the following key terms. You can find the definitions in the Glossary.

Internet	*page 4*
instant messaging (IM)	*page 7*
social media	*page 8*
collaboration tools	*page 8*
weblogs (blogs)	*page 8*
wikis	*page 8*
podcasting	*page 8*
peer-to-peer (P2P) file sharing	*page 8*
quality of service (QoS)	*page 12*
converged network	*page 13*
fault tolerant	*page 15*
packets	*page 17*
scalable	*page 19*
security	*page 21*
network service	*page 24*
end devices	*page 24*
host device	*page 24*
intermediary devices	*page 25*
medium (media)	*page 25*
local-area network (LAN)	*page 29*

wide-area network (WAN)	*page 29*
wireless LAN (WLAN)	*page 29*
storage-area network (SAN)	*page 29*
intranet	*page 32*
extranet	*page 32*
cable	*page 33*
DSL	*page 33*
cellular	*page 33*
satellite	*page 33*
dial-up	*page 34*
dedicated leased line	*page 34*
Metro Ethernet	*page 35*
Bring Your Own Device (BYOD)	*page 36*
cloud computing	*page 40*

Introduction (1.0.1.1)

We now stand at a critical turning point in the use of technology to extend and empower our ability to communicate. The globalization of the Internet has succeeded faster than anyone could have imagined. The manner in which social, commercial, political, and personal interactions occur is rapidly changing to keep up with the evolution of this global network. In the next stage of our development, innovators will use the Internet as a starting point for their efforts as they create new products and services specifically designed to take advantage of the network capabilities. As developers push the limits of what is possible, the capabilities of the interconnected networks that form the Internet will play an increasing role in the success of these projects.

This chapter introduces the platform of data networks upon which our social and business relationships increasingly depend. The material lays the groundwork for exploring the services, technologies, and issues encountered by network professionals as they design, build, and maintain the modern network.

Class Activity 1.0.1.2: Draw Your Concept of the Internet

The Networking Academy curriculum has a new component called Modeling Activities. You will find them at the beginning and end of each chapter. Some activities can be completed individually (at home or in class), and some will require group or learning-community interaction. Your instructor will be facilitating so that you can obtain the most from these introductory activities. These activities will help you enhance your understanding by providing an opportunity to visualize some of the abstract concepts that you will be learning in this course. Be creative and enjoy these activities!

The Network Basics Lab Manual (ISBN 978-1-58713-313-8) contains all the Labs and Class Activities from the course. You can access the full instructions in the course itself or in this printed Lab Manual.

Here is your first modeling activity:

Draw Your Concept of the Internet

In this activity you will draw and label a map of the Internet as you interpret it now. Include your home or school/university location and its respective cabling, equipment, devices, etc. The following are some items you may want to include:

Devices/Equipment

Media (cabling)

Link Addresses or Names

Sources & Destinations

Internet Service Providers

Upon completion, be sure to save your work in a hard-copy format, as it will be used for future reference at the end of this chapter. If it is an electronic document, save it to a server location provided by your instructor. Be prepared to share and explain your work in class.

For an example to get you started, please visit http://www.kk.org/internet-mapping/.

Communicating in a Network-Centric World (1.1)

Communication methods are constantly evolving, and the changes affect the way we interact with family, friends, and society. This chapter explores how we came to communicate over computer networks.

Interconnecting Our Lives (1.1.1)

In this section we will look at how people use networked computers to learn, work, and play.

Networks in Our Daily Lives (1.1.1.1)

Among all of the essentials for human existence, the need to interact with others ranks just below our need to sustain life. Communication is almost as important to us as our reliance on air, water, food, and shelter.

The methods that we use to communicate are constantly changing and evolving. Whereas we were once limited to face-to-face interactions, breakthroughs in technology have significantly extended the reach of our communications. From cave paintings to the printing press to radio and television, each new development has improved and enhanced our ability to connect and communicate with others.

The creation and interconnection of robust data networks has had a profound effect on communication, and has become the new platform on which modern communications occur.

Networks connect people and promote unregulated communication. Networks are the platforms on which to run businesses, to address emergencies, to inform individuals, and to support education, science, and government. The Internet is the largest network in existence. In fact, the term ***Internet*** means a network of networks. It is actually a collection of interconnected private and public networks. It is incredible how quickly the Internet has become an integral part of our daily routines.

Technology Then and Now (1.1.1.2)

Imagine a world without the Internet. No more Google, YouTube, instant messaging, Facebook, Wikipedia, online gaming, Netflix, iTunes, and easy access to current information. No more price comparison websites, avoiding lines by shopping online, or quickly looking up phone numbers and map directions to various locations at the click of a finger. How different would our lives be without all of this? That was the world we lived in just 15 to 20 years ago. But over the years, data networks have slowly expanded and been repurposed to improve the quality of life for people everywhere.

In the course of a day, resources that are available through the Internet can help you

- Post and share your photographs, home videos, and experiences with friends or with the world
- Access and submit school work
- Communicate with friends, family, and peers using email, instant messaging, or video applications
- Watch videos, movies, or television episodes on demand
- Play online games with friends
- Decide what to wear using online current weather conditions
- Find the least congested route to your destination by displaying weather and traffic video from webcams
- Check your bank balance and pay bills electronically

Innovators are figuring out new ways to use the Internet more every day. As developers push the limits of what is possible, the capabilities of the Internet and the role the Internet plays in our lives will expand broader and broader. Consider the changes that have happened within the last couple of decades, as depicted in Figure 1-1. Now consider what changes will happen within the next decade. What else do you think we will be able to do using the network as the platform?

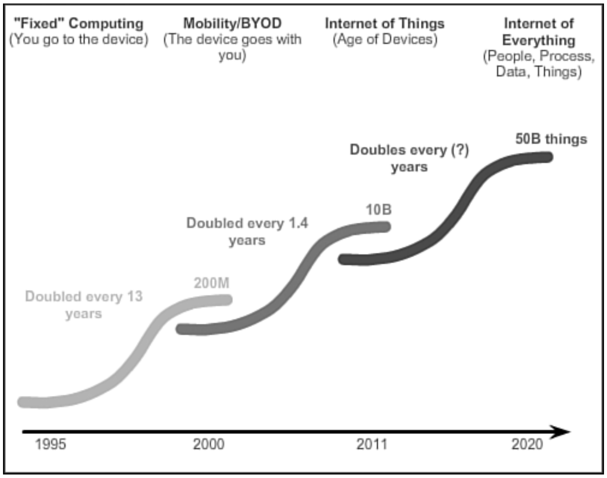


Figure 1-1 Computing Timeline

The Global Community (1.1.1.3)

Advancements in networking technologies are perhaps the most significant change agent in the world today. They are helping to create a world in which national borders, geographic distances, and physical limitations become less relevant, and present ever-diminishing obstacles.

The Internet has changed the manner in which social, commercial, political, and personal interactions occur. The immediate nature of communications over the Internet encourages the creation of global communities. Global communities allow for social interaction that is independent of location or time zone. The creation of online communities for the exchange of ideas and information has the potential to increase productivity opportunities across the globe.

Cisco refers to this as the *human network*. The human network centers on the impact of the Internet and networks on people and businesses.

How has the human network affected you?

Networks Support the Way We Learn (1.1.1.4)

Networks and the Internet have changed everything we do—the way we learn, the way we communicate, how we work, and even how we play.

Changing the Way We Learn

Communication, collaboration, and engagement are fundamental building blocks of education. Institutions are continually striving to enhance these processes to maximize the dissemination of knowledge. Traditional learning methods provide primarily two sources of expertise from which the student can obtain information: the textbook and the instructor. These two sources are limited, both in the format and the timing of the presentation.

Networks have changed the way we learn. Robust and reliable networks support and enrich student learning experiences. They deliver learning material in a wide range of formats, including interactive activities, assessments, and feedback. Networks now

- Support the creation of virtual classrooms
- Provide on-demand video
- Enable collaborative learning spaces
- Enable mobile learning

Access to high-quality instruction is no longer restricted to students living in proximity to where that instruction is being delivered. Online distance learning has removed geographic barriers and improved student opportunity. Online (e-learning) courses can now be delivered over a network. These courses can contain data (text, links), voice, and video available to the students at any time from any place. Online discussion groups and message boards enable a student to collaborate with the instructor, with other students in the class, or even with students across the world. Blended courses can combine instructor-led classes with online courseware to provide the best of both delivery methods.

In addition to the benefits for the student, networks have improved the management and administration of courses as well. Some of these online functions include student enrollment, assessment delivery, and progress tracking.

Networks Support the Way We Communicate (1.1.1.5)

Changes in network communications have enabled friends, families, and businesses to communicate in ways that could only be imagined by previous generations.

Changing the Way We Communicate

The globalization of the Internet has ushered in new forms of communication that empower individuals to create information that can be accessed by a global audience.

Some forms of communications include

- ***Instant messaging (IM)*** **and texting:** IM and texting both enable instant, real-time communication between two or more people. Many IM and texting applications incorporate features such as file transfer. IM applications can offer additional features such as voice and video communication.

- *Social media*: Social media consists of interactive websites where people and communities create and share user-generated content with friends, family, peers, and the world.
- *Collaboration tools*: Collaboration tools give people the opportunity to work together on shared documents. Without the constraints of location or time zone, individuals connected to a shared system can speak to each other, often across real-time, interactive video. Across the network, they can share text and graphics, and edit documents together. With collaboration tools always available, organizations can move quickly to share information and pursue goals. The broad distribution of data networks means that people in remote locations can contribute on an equal basis with people at the heart of large population centers.
- *Weblogs (blogs)*: Weblogs are web pages that are easy to update and edit. Unlike commercial websites, which are created by professional communications experts, blogs give anyone, including those without technical knowledge of web design, a means to communicate their thoughts to a global audience. There are blogs on nearly every topic one can think of, and communities of people often form around popular blog authors.
- *Wikis*: Wikis are web pages that groups of people can edit and view together. Whereas a blog is more of an individual, personal journal, a wiki is a group creation. As such, it may be subject to more extensive review and editing. Like blogs, wikis can be created in stages, and by anyone, without the sponsorship of a major commercial enterprise. Wikipedia has become a comprehensive resource—an online encyclopedia—of publicly contributed topics. Private organizations and individuals can also build their own wikis to capture collected knowledge on a particular subject. Many businesses use wikis as their internal collaboration tool. With the global Internet, people of all walks of life can participate in wikis and add their own perspectives and knowledge to a shared resource.
- *Podcasting*: Podcasting is an audio-based medium that originally enabled people to record audio and convert it for use. Podcasting allows people to deliver their recordings to a wide audience. The audio file is placed on a website (or blog or wiki) where others can download it and play the recording on their computers, laptops, and other mobile devices.
- *Peer-to-peer (P2P) file sharing*: Peer-to-peer file sharing enables people to share files with each other without having to store the files on and download them from a central server. The user joins the P2P network by simply installing the P2P software. This lets them locate and share files with others in the P2P network. The widespread digitization of media files, such as music and video files, has increased the interest in P2P file sharing. P2P file sharing has not been embraced by everyone. Many people are concerned that widespread use of P2P has enabled many to violate the laws of copyrighted materials.

What other sites or tools do you use to share your thoughts?

Networks Support the Way We Work (1.1.1.6)

Businesses, whether a small family business or a multinational corporation, have changed the way they operate to reap the benefits of network communications.

Changing the Way We Work

In the business world, data networks were initially used by businesses to internally record and manage financial information, customer information, and employee payroll systems. These business networks evolved to enable the transmission of many different types of information services, including email, video, messaging, and telephony.

The use of networks to provide efficient and cost-effective employee training is increasing in acceptance. Online learning opportunities can decrease time-consuming and costly travel yet still ensure that all employees are adequately trained to perform their jobs in a safe and productive manner.

There are many success stories illustrating innovative ways networks are being used to make us more successful in the workplace. Some of these scenarios are available through the Cisco website at http://www.cisco.com.

Networks Support the Way We Play (1.1.1.7)

Games, music, and TV are all enjoyed in significantly different ways than a decade ago due to changes in network communications.

Changing the Way We Play

The widespread adoption of the Internet by the entertainment and travel industries enhances the ability to enjoy and share many forms of recreation, regardless of location. It is possible to explore places interactively that previously we could only dream of visiting, as well as preview the actual destinations before making a trip. Travelers can post the details and photographs from their adventures online for others to view.

In addition, the Internet is used for traditional forms of entertainment. We listen to recording artists, preview or view motion pictures, read entire books, and download material for future offline access. Live sporting events and concerts can be experienced as they are happening, or recorded and viewed on demand.

Networks enable the creation of new forms of entertainment, such as online games. Players participate in any kind of online competition that game designers can imagine. We compete with friends and foes around the world in the same manner as if they were in the same room.

Even offline activities are enhanced using network collaboration services. Global communities of interest have grown rapidly. We share common experiences and hobbies well beyond our local neighborhood, city, or region. Sports fans share opinions and facts about their favorite teams. Collectors display prized collections and get expert feedback about them.

Online markets and auction sites provide the opportunity to buy, sell, and trade all types of merchandise.

Whatever form of recreation we enjoy in the human network, networks are improving our experience.

How do you play on the Internet?

Lab 1.1.1.8: Researching Network Collaboration Tools

In this lab you will use collaboration tools, share documents with Google Drive, explore conferencing and web meetings, and create wiki pages.

Supporting Communication (1.1.2)

This section discusses the various forms of communication, expected communication behaviors, and communication styles.

What Is Communication? (1.1.2.1)

Communication in our daily lives takes many forms and occurs in many environments. We have different expectations depending on whether we are chatting via the Internet or participating in a job interview. Each situation has its corresponding expected behaviors and styles.

Establishing the Rules

Before beginning to communicate with each other, we establish rules or agreements to govern the conversation. These rules, or protocols, must be followed in order for the message to be successfully delivered and understood. Figures 1-2, 1-3, and 1-4 depict a few of these rules. Among the protocols that govern successful human communication are the following:

- Identified sender and receiver
- Agreed-upon method of communicating (face-to-face, telephone, letter, photograph; see Figure 1-2)
- Common language and grammar (see Figure 1-3)

- Speed and timing of delivery
- Confirmation or acknowledgement requirements (see Figure 1-4)

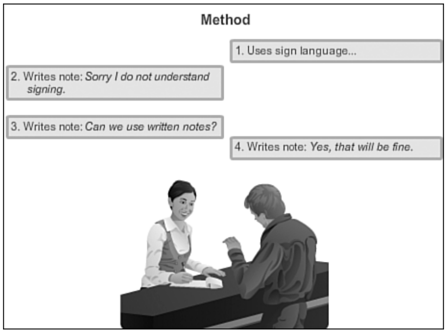

Method
1. Uses sign language...
2. Writes note: *Sorry I do not understand signing.*
3. Writes note: *Can we use written notes?*
4. Writes note: *Yes, that will be fine.*

Figure 1-2 Agreeing on a Communication Method

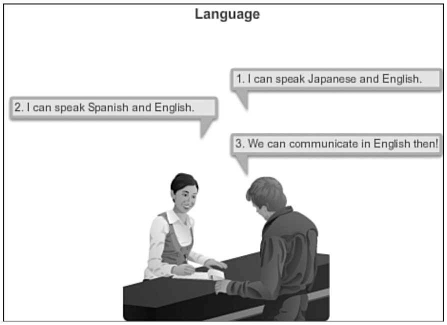

Language
1. I can speak Japanese and English.
2. I can speak Spanish and English.
3. We can communicate in English then!

Figure 1-3 Agreeing on a Common Language

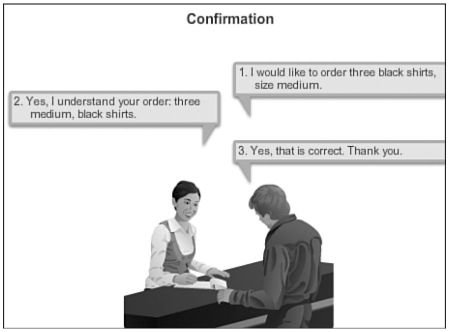

Confirmation
1. I would like to order three black shirts, size medium.
2. Yes, I understand your order: three medium, black shirts.
3. Yes, that is correct. Thank you.

Figure 1-4 Confirming a Message

Communication rules may vary according to the context. If a message conveys an important fact or concept, a confirmation that the message has been received and understood is necessary. Less important messages may not require an acknowledgement from the recipient.

The techniques that are used in network communications share these fundamentals with human conversations.

Quality of Communication (1.1.2.2)

Communication between individuals is determined to be successful when the meaning of the message understood by the recipient matches the meaning intended by the sender. For data networks, we use the same basic criteria to judge success. However, as a message moves through the network, many factors can prevent the message from reaching the recipient or distort its intended meaning. These factors can be either external or internal.

External QoS Factors

The external ***quality of service (QoS)*** factors affecting data communications are related to the complexity of the network and the number of devices a message must pass through on its route to its final destination.

External QoS factors affecting the success of communication include

- The quality of the pathway between the sender and the recipient
- The number of times the message has to change form
- The number of times the message has to be redirected or readdressed
- The number of other messages being transmitted simultaneously on the communication network
- The amount of time allotted for successful communication

QoS will be discussed in greater detail throughout the course.

Internal QoS Factors

Internal QoS factors that interfere with network communications are related to the nature of the message itself. Different types of messages may vary in complexity and importance. Clear and concise messages are usually easier to understand than complex messages. Important communications require more care to ensure that they are delivered and understood by the recipient.

Internal factors affecting successful communications across the network include

- The size of the message
- The complexity of the message
- The importance of the message

Large messages may be interrupted or delayed at different points within the network. A message with a low importance or priority could be dropped if the network becomes overloaded.

Both the internal and external factors that affect the receipt of a message must be anticipated and controlled for network communications to be successful. New innovations in network hardware and software are being implemented to ensure the quality and reliability of network communications.

The Network as a Platform (1.2)

In the past, traditional networks such as television, telephone, and computer networks worked in very different ways. This chapter explores how those differences are rapidly shrinking.

Converged Networks (1.2.1)

In this section you will learn how different types of networks are becoming increasingly alike as network technologies change.

Traditional Service Networks (1.2.1.1)

Modern networks are constantly evolving to meet user demands. Early data networks were limited to exchanging character-based information between connected computer systems. Traditional telephone and television networks were maintained separately from data networks. In the past, every one of these services required a dedicated network, with different communications channels and different technologies to carry a particular communication signal. Each service had its own set of rules and standards to ensure successful communication.

Consider a hospital built 40 years ago. Back then, hospital rooms were cabled for the data network, telephone network, and video network for televisions. These separate networks were disparate, meaning that they could not communicate with each other, as shown on the left in Figure 1-5.

Advances in technology are enabling us to consolidate these different kinds of networks onto one platform, referred to as the ***converged network***. Unlike dedicated networks, converged networks are capable of delivering voice, video streams, text, and graphics between many different types of devices over the same communications channel and network structure, as shown on the right in Figure 1-5. Previously separate and distinct communication forms have converged onto a common platform. This platform provides access to a wide range of alternative and new communication methods that enable people to interact directly with each other almost instantaneously.

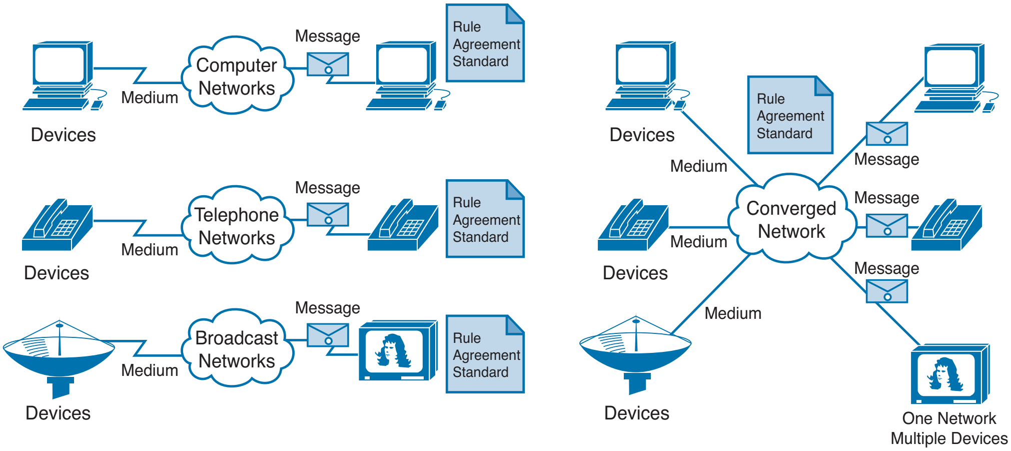


Figure 1-5 Traditional Networks (Left) and Converged Network (Right)

On a converged network, there are still many points of contact and many specialized devices, such as personal computers, phones, TVs, and tablet computers, but there is one common network infrastructure. This network infrastructure uses the same set of rules, agreements, and implementation standards.

Planning for the Future (1.2.1.2)

The convergence of the different types of communications networks onto one platform represents the first phase in building the intelligent information network. We are currently in this phase of network evolution. The next phase will be to not only consolidate the different types of messages onto a single network, but also consolidate the applications that generate, transmit, and secure the messages onto integrated network devices.

Not only will voice and video be transmitted over the same network, the devices that perform the telephone switching and video broadcasting will be the same devices that route the messages through the network. The resulting communications platform will provide high-quality application functionality at a reduced cost.

The pace at which the development of exciting new converged network applications is occurring can be attributed to the rapid growth and expansion of the Internet. This expansion has created a wider audience for whatever message, product, or service can be delivered. The underlying mechanics and processes that drive this explosive growth have resulted in a network architecture that is both capable of supporting changes and able to grow. As the supporting technology platform for living, learning, working, and playing in the human network, the network architecture of the Internet must adapt to constantly changing requirements for a high quality of service and security.

Lab 1.2.1.3: Researching Converged Network Services

In this lab you will explore converged services offered by local ISPs and research how converged networks are in use by institutions.

Reliable Network (1.2.2)

In this section you will learn about characteristics of a reliable network.

The Supporting Network Architecture (1.2.2.1)

Networks must support a wide range of applications and services, as well as operate over many different types of cables and devices that make up the physical infrastructure. The term *network architecture*, in this context, refers to the technologies that support the infrastructure and the programmed services and rules, or protocols, that move messages across the network.

As networks evolve, we are discovering that there are four basic characteristics that the underlying architectures need to address in order to meet user expectations:

- Fault tolerance
- Scalability
- QoS
- Security

Fault Tolerance in Circuit-Switched Networks (1.2.2.2)

Designing for unforeseen problems is an essential element of network design. This section explains how networks can manage unexpected equipment failure.

Fault Tolerance

The expectation is that the Internet is always available to the millions of users who rely on it. This requires a network architecture that is built to be ***fault tolerant***. A fault-tolerant network is one that limits the effect of a failure, so that the fewest number of devices are affected by it. It is also built in a way that enables quick recovery when such a failure occurs. Fault-tolerant networks depend on multiple paths between the source and destination of a message. If one path fails, the messages can be instantly sent over a different link. Having multiple paths to a destination is known as redundancy, as shown in Figure 1-6.

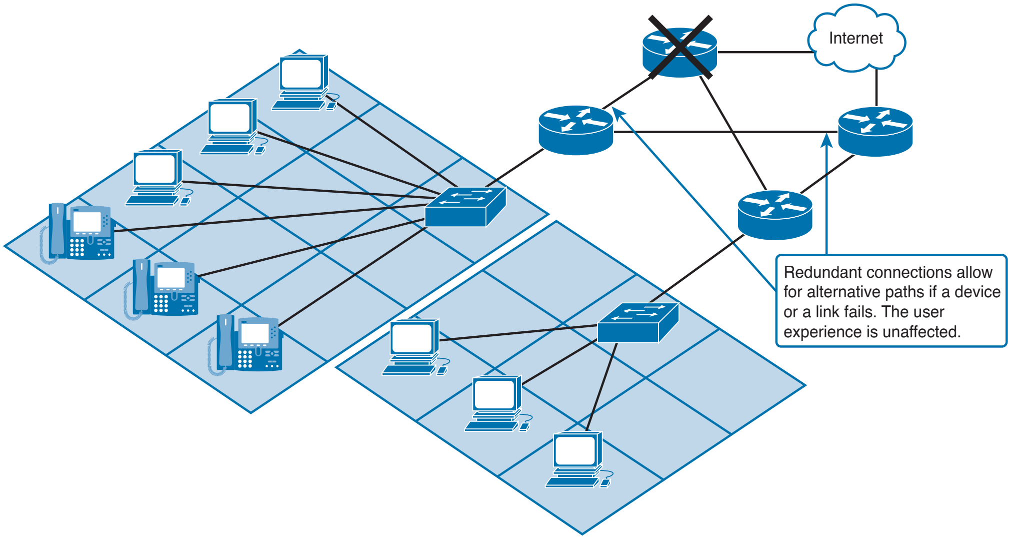

Internet
Redundant connections allow for alternative paths if a device or a link fails. The user experience is unaffected.

Figure 1-6 Fault Tolerance

Circuit-Switched, Connection-Oriented Networks

To understand the need for redundancy, we can look at how early telephone systems worked. When a person made a call using a traditional telephone set, the call first went through a setup process. This process identified the telephone switching locations between the person making the call (the source) and the phone set receiving the call (the destination). A temporary path, or *circuit*, was created for the duration of the telephone call. If any link or device in the circuit failed, the call was dropped. To reconnect, a new call had to be made, with a new circuit. This connection process is referred to as a circuit-switched process and is illustrated in Figure 1-7.

Many circuit-switched networks give priority to existing circuit connections at the expense of new circuit requests. After a circuit is established, even if no communication is occurring between the persons on either end of the call, the circuit remains connected and resources are used until one of the parties disconnects the call. Because there are only so many circuits that can be created, it is possible to get a message that all circuits are busy and a call cannot be placed. The cost to create many alternative paths with enough capacity to support a large number of simultaneous circuits, and the technologies necessary to dynamically re-create dropped circuits in the event of a failure, are why circuit-switched technology was not optimal for the Internet.

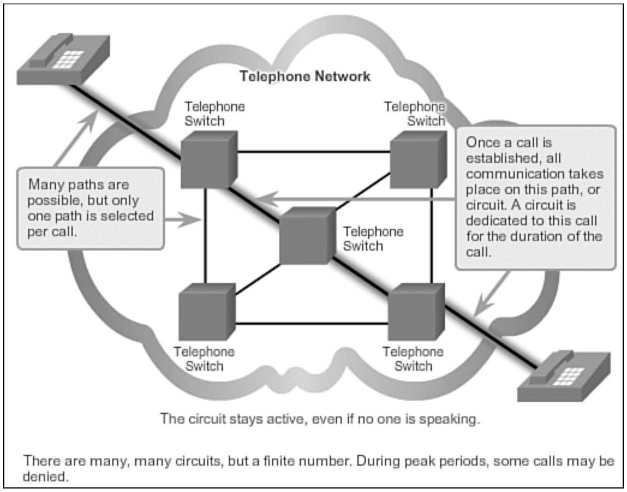

Telephone Network
Telephone Switch
Telephone Switch
Many paths are possible, but only one path is selected per call.
Telephone Switch
Once a call is established, all communication takes place on this path, or circuit. A circuit is dedicated to this call for the duration of the call.
Telephone Switch
Telephone Switch
The circuit stays active, even if no one is speaking.
There are many, many circuits, but a finite number. During peak periods, some calls may be denied.

Figure 1-7 Circuit-Switched Network

Packet-Switched Networks (1.2.2.3)

In the search for a network that was more fault tolerant, the early Internet designers researched packet-switched networks. The premise for this type of network is that a single message can be broken into multiple message blocks, with each message block containing addressing information to indicate the origination point and final destination. Using this embedded information, these message blocks, called ***packets***, can be sent through the network along various paths, and can be reassembled into the original message when they reach their destination. Figure 1-8 demonstrates how packets can travel different paths and arrive at the correct destination for sorting.

The devices within the network itself are typically unaware of the content of the individual packets. The only packet information used by intermediate devices is the original source address and the final destination address. These addresses are often referred to as *IP addresses*, represented in a dotted decimal format such as 10.10.10.10. Each packet is sent independently from one location to another. At each location, a routing decision is made as to which path to use to forward the packet toward its final destination. If a previously used path is no longer available, the routing function can dynamically choose the next best available path. Because the messages are sent in pieces, rather than as a single complete message, the few packets that may be lost can be retransmitted to the destination along a different path. In many cases, the destination device is unaware that any failure or rerouting occurred.

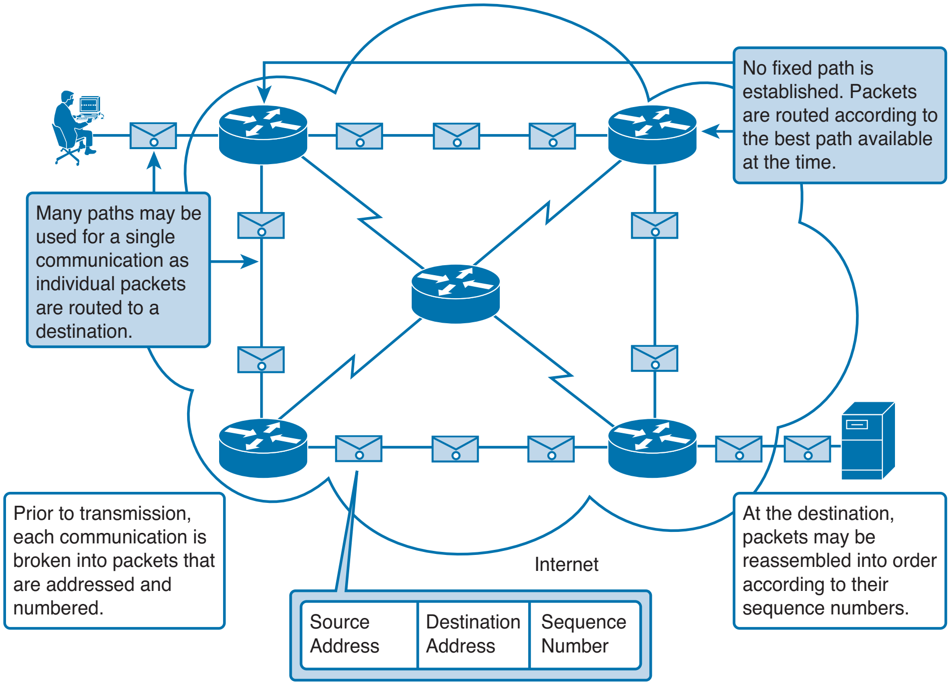

No fixed path is established. Packets are routed according to the best path available at the time.
Many paths may be used for a single communication as individual packets are routed to a destination.
Prior to transmission, each communication is broken into packets that are addressed and numbered.
Internet
Source Address
Destination Address
Sequence Number
At the destination, packets may be reassembled into order according to their sequence numbers.

Figure 1-8 Packet-Switched Network

The need for a single, reserved circuit from end to end does not exist in a packet-switched network. Any piece of a message can be sent through the network using any available path. Additionally, packets containing pieces of messages from different sources can travel the network at the same time. By providing a method to dynamically use redundant paths, without intervention by the user, the Internet has become a fault-tolerant method of communication.

Although packet-switched, connectionless networks are the primary infrastructure for today's Internet, there are some benefits to a connection-oriented system like the circuit-switched telephone system. Because resources at the various switching locations are dedicated to providing a finite number of circuits, the quality and consistency of messages transmitted across a connection-oriented network can be guaranteed. Another benefit is that the provider of the service can charge the users of the network for the period of time that the connection is active. The ability to charge users for active connections through the network is a fundamental premise of the telecommunication service industry.

Scalable Networks (1.2.2.4)

Designing a network that will be able to efficiently expand is an important network design consideration.

Scalability

Thousands of new users and service providers connect to the Internet each week. In order for the Internet to support this rapid amount of growth, it must be scalable. A *scalable* network can expand quickly to support new users and applications without affecting the performance of the service being delivered to existing users. Figure 1-9 depicts a scalable network accepting additional users.

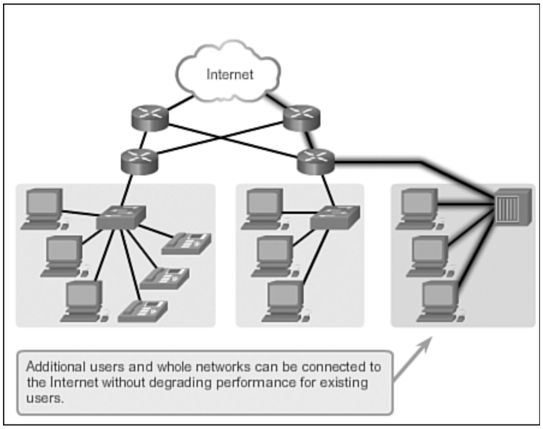

Internet
Additional users and whole networks can be connected to the Internet without degrading performance for existing users.

Figure 1-9 Scalability

The fact that the Internet is able to expand at the rate that it is, without seriously impacting the performance experienced by individual users, is a function of the design of the protocols and underlying technologies on which it is built. The Internet has a hierarchical, layered structure for addressing, for naming, and for connectivity services. As a result, network traffic that is destined for local or regional services does not need to traverse to a central point for distribution. Common services can be duplicated in different regions, thereby keeping traffic off the higher-level backbone networks.

Scalability also refers to the ability to accept new products and applications. Although there is no single organization that regulates the Internet, the many individual networks that provide Internet connectivity cooperate to follow accepted standards and protocols. The adherence to standards enables the manufacturers of hardware and software to concentrate on product development and improvements in the areas of performance and capacity, knowing that the new products can integrate with and enhance the existing infrastructure.

The current Internet architecture, while highly scalable, may not always be able to keep up with the pace of user demand. New protocols and addressing structures are under development to meet the increasing rate at which Internet applications and services are being added.

Providing QoS (1.2.2.5)

A well-designed network can prioritize network traffic to provide users with reliable quality of service, or QoS.

Quality of Service

Quality of service is also an ever-increasing requirement of networks today. New applications available to users over internetworks, such as voice and live video transmissions, as shown in Figure 1-10, create higher expectations for the quality of the delivered services. Have you ever tried to watch a video with constant breaks and pauses?

Networks must provide predictable, measurable, and, at times, guaranteed services. The packet-switched network architecture does not guarantee that all packets that comprise a particular message will arrive on time and in their correct order, or even that they will arrive at all.

Networks also need mechanisms to manage congested network traffic. Network bandwidth is the measure of the data-carrying capacity of the network. In other words, how much information can be transmitted within a specific amount of time? Network bandwidth is measured in the number of bits that can be transmitted in a single second, or bits per second (bps). When simultaneous communications are attempted across the network, the demand for network bandwidth can exceed its availability, creating network congestion. The network simply has more bits to transmit than what the bandwidth of the communications channel can deliver.

In most cases, when the volume of packets is greater than what can be transported across the network, devices *queue*, or hold, the packets in memory until resources become available to transmit them, as shown in Figure 1-10. Queuing packets causes delay because new packets cannot be transmitted until previous packets have been processed. If the number of packets to be queued continues to increase, the memory queues fill up and packets are dropped.

Achieving the required QoS by managing the delay and packet loss parameters on a network becomes the secret to providing a successful solution for end-to-end application quality. One way this can be accomplished is through classification. To create QoS classifications of data, we use a combination of communication characteristics and the relative importance assigned to the application. We then treat all data within the same classification according to the same rules. For example, communication that is time-sensitive, such as voice transmissions, would be classified differently from communication that can tolerate delay, such as file transfers.

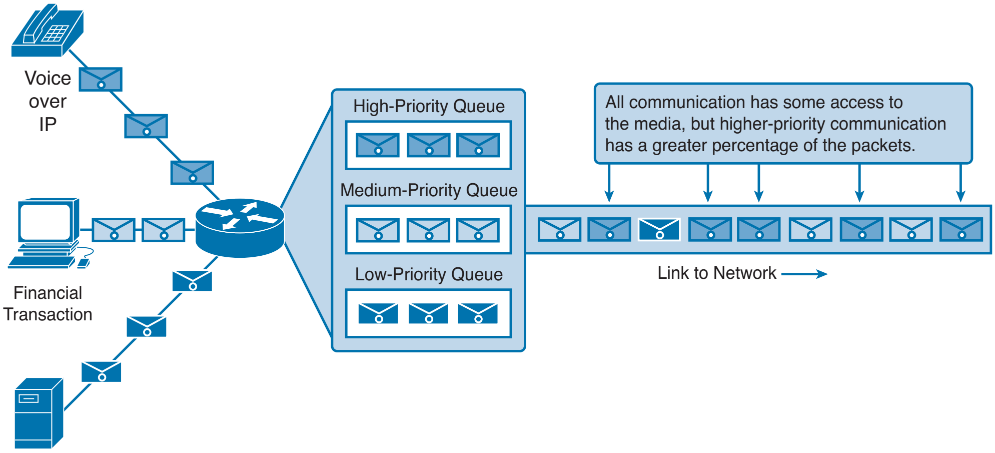

Voice over IP
Financial Transaction
High-Priority Queue
Medium-Priority Queue
Low-Priority Queue
All communication has some access to the media, but higher-priority communication has a greater percentage of the packets.
Link to Network

Figure 1-10 Priority Queuing

Examples of priority decisions for an organization might include

- **Time-sensitive communication:** Increase priority for services like telephony or video distribution
- **Non-time-sensitive communication:** Decrease priority for web page retrieval or email
- **High importance to organization:** Increase priority for production control or business transaction data
- **Undesirable communication:** Decrease priority or block unwanted activity, like peer-to-peer file sharing or live entertainment

Providing Network Security (1.2.2.6)

Security is one of the most important design elements in a computer network.

Security

The Internet has evolved from a tightly controlled internetwork of educational and government organizations to a widely accessible means for transmission of business and personal communications. As a result, the security requirements of the network have changed. The network infrastructure, the network services, and the data contained on network-attached devices are crucial personal and business assets. Compromising the integrity of these assets could have serious consequences, such as

- Network outages that prevent communications and transactions from occurring, with consequent loss of business
- Intellectual property (research ideas, patents, or designs) that is stolen and used by a competitor

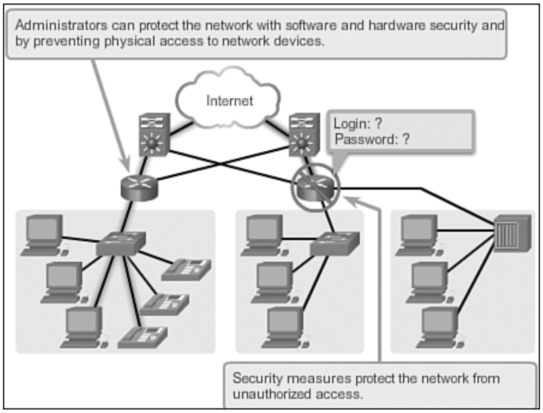
- Personal or private information that is compromised or made public without the user's consent
- Misdirection and loss of personal or business funds
- Loss of important data that takes a significant labor to replace, or is irreplaceable

There are two types of network security concerns that must be addressed: network infrastructure security and information security.

Securing a network infrastructure includes physically securing devices that provide network connectivity, and preventing unauthorized access to the management software that resides on those devices.

Information security refers to protecting the information contained within the packets being transmitted over the network and the information stored on network-attached devices. Security measures taken in a network should prevent the following:

- Unauthorized disclosure
- Theft of information (see Figure 1-11)
- Unauthorized modification of information
- Denial of service (DoS)



Administrators can protect the network with software and hardware security and by preventing physical access to network devices.

Security measures protect the network from unauthorized access.

Figure 1-11 Security in a Computer Network.

In order to achieve the goals of network security, there are three primary requirements:

- **Ensuring confidentiality:** Data confidentiality means that only the intended and authorized recipients—individuals, processes, or devices—can access and read data. This is accomplished by having a strong system for user authentication, enforcing passwords that are difficult to guess, and requiring users to change their passwords frequently. Encrypting data, so that only the intended recipient can read it, is also part of confidentiality.

- **Maintaining communication integrity:** Data integrity means having the assurance that the information has not been altered in transmission, from origin to destination. Data integrity can be compromised when information has been corrupted—willfully or accidentally. Data integrity is made possible by requiring validation of the sender and by using mechanisms to validate that the packet has not changed during transmission.
- **Ensuring availability:** *Availability* means having the assurance of timely and reliable access to data services for authorized users. Network firewall devices, along with desktop and server antivirus software, can ensure system reliability and the robustness to detect, repel, and cope with such attacks. Building fully redundant network infrastructures, with few single points of failure, can reduce the impact of these threats.

Interactive Graphic

Activity 1.2.2.7: Reliable Networks

Go to the online course to perform this practice activity.

LANs, WANs, and the Internet (1.3)

Most web users never consider how the Internet works. In this section you will begin to explore the pieces that come together to enable network communications.

Components of a Network (1.3.1)

In this section you will begin to learn about the devices and equipment that work together in networks.

Components of the Network (1.3.1.1)

The path that a message takes from source to destination can be as simple as a single cable connecting one computer to another or as complex as a network that literally spans the globe. This network infrastructure is the platform that supports the network. It provides the stable and reliable channel over which our communications can occur.

The network infrastructure contains three categories of network components:

- End devices
- Intermediary devices
- Network media

Devices and media are the physical elements, or *hardware*, of the network. Hardware comprises the components of the network platform that typically are visible, such as a laptop, PC, switch, router, wireless access point, or the cabling used to connect the devices. Occasionally, some network components may not be visible. In the case of wireless media, for example, messages are transmitted through the air using invisible radio frequency or infrared waves.

Network components are used to provide services and processes. These services and processes are the communication programs, called *software*, that run on the networked devices. A ***network service*** provides information in response to a request. Services include many of the common network applications people use every day, like email hosting services and web hosting services. Processes provide the functionality that directs and moves the messages through the network. Processes are less obvious to us but are critical to the operation of networks.

End Devices (1.3.1.2)

The network devices that people are most familiar with are called ***end devices***, or hosts. These devices form the interface between users and the underlying communication network.

Some examples of end devices are

- Computers (work stations, laptops, file servers, web servers)
- Network printers
- VoIP phones
- TelePresence endpoints
- Security cameras
- Mobile handheld devices (such as smartphones, tablets, PDAs, and wireless debit/credit card readers and barcode scanners)

A ***host device*** is either the source or destination of a message transmitted over the network. In order to distinguish one host from another, each host on a network is identified by an address. When a host initiates communication, it uses the address of the destination host to specify where the message should be sent.

In modern networks, a host can act as a client, a server, or both. Software installed on the host determines which role it plays on the network. *Servers* are hosts that have software installed that enables them to provide information and services, like email or web pages, to other hosts on the network. *Clients* are hosts that have software installed that enables them to request and display the information obtained from the server.

Intermediary Devices (1.3.1.3)

Intermediary devices interconnect end devices. These devices provide connectivity and work behind the scenes to ensure that data flows across the network. Intermediary devices connect the individual hosts to the network and can connect multiple individual networks to form an internetwork.

Interactive Graphic

Activity 1.3.1.3: Internetworks

Go to the online course and view the animation.

Examples of intermediary network devices are

- Network access devices (switches and wireless access points)
- Internetworking devices (routers)
- Security devices (firewalls)

The management of data as it flows through the network is also a role of the intermediary devices. These devices use the destination host address, in conjunction with information about the network interconnections, to determine the path that messages should take through the network.

Processes running on the intermediary network devices perform these functions:

- Regenerate and retransmit data signals
- Maintain information about which pathways exist through the network and internetwork
- Notify other devices of errors and communication failures
- Direct data along alternate pathways when there is a link failure
- Classify and direct messages according to QoS priorities
- Permit or deny the flow of data, based on security settings

Network Media (1.3.1.4)

Communication across a network is carried on a *medium*. The medium provides the channel over which the message travels from source to destination.

Modern networks primarily use the following three types of media to interconnect devices and to provide the pathway over which data can be transmitted:

- Metallic wires within cables
- Glass or plastic fibers (fiber-optic cable)
- Wireless transmission

Figure 1-12 shows examples of the three types of physical media.

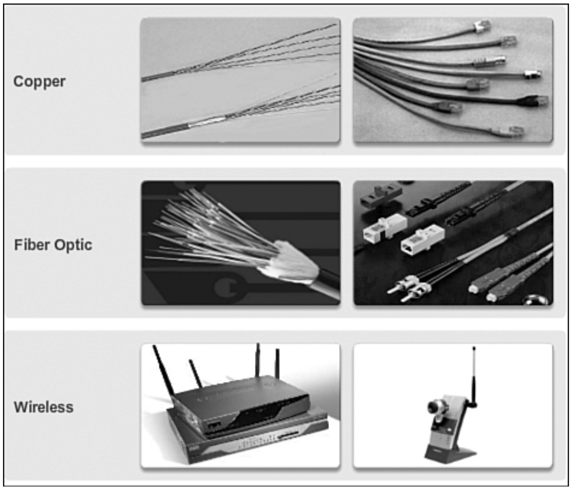


Figure 1-12 Network Media

The signal encoding that must occur for the message to be transmitted is different for each media type. On metallic wires, the data is encoded into electrical impulses that match specific patterns. Fiber-optic transmissions rely on pulses of light, within either infrared or visible light ranges. In wireless transmission, patterns of electromagnetic waves depict the various bit values.

Different types of network media have different features and benefits. Not all network media types have the same characteristics or are appropriate for the same purpose. The criteria for choosing network media are

- The distance the media can successfully carry a signal
- The environment in which the media is to be installed
- The amount of data and the speed at which it must be transmitted
- The cost of the media and installation

Network Representations (1.3.1.5)

When conveying complex information, such as displaying all the devices and media in a large internetwork, it is helpful to use visual representations. A diagram provides an easy way to understand the way the devices in a large network are connected. Such a diagram uses symbols to represent the different devices and connections that make up a network. This type of "picture" of a network is known as a *topology diagram*.

Like any other language, the language of networking uses a common set of symbols to represent the different end devices, network devices, and media, as shown in Figure 1-13. The ability to recognize the logical representations of the physical networking components is critical to being able to visualize the organization and operation of a network. Throughout this course and its accompanying labs, you will learn both how these devices operate and how to perform basic configuration tasks on these devices.

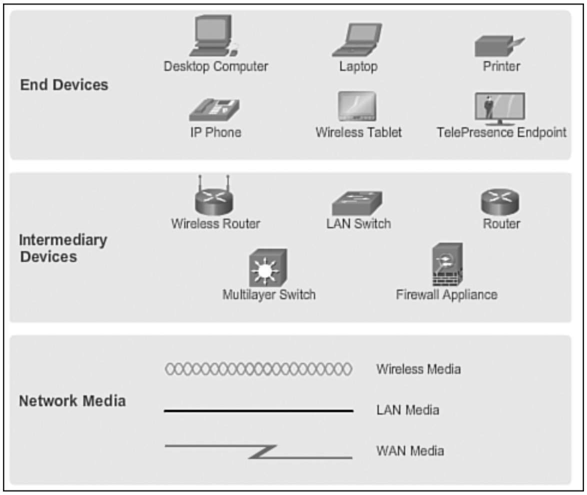


Figure 1-13 Network Representations

In addition to being able to recognize these representations, you need to understand the specialized terminology that is used when discussing how each of these devices and media connect to each other. Important terms to remember are

- **Network interface card (NIC):** Provides the physical connection to the network at the PC or other host device. The media connecting the PC to the networking device plugs directly into the NIC (also known as a LAN adapter).
- **Physical port:** A connector or outlet on a networking device where the media is connected to a host or other networking device.
- **Interface:** Specialized ports on an internetworking device that connect to individual networks. Because routers are used to interconnect networks, the ports on a router are referred to as network interfaces.

Topology Diagrams (1.3.1.6)

Topology diagrams are mandatory for anyone working with a network. A topology diagram provides a visual map of how the network is connected.

There are two types of topology diagrams:

- **Physical topology diagram:** Identifies the physical location of intermediary devices, configured ports, and cable installation, as shown on the left in Figure 1-14.
- **Logical topology diagram:** Identifies devices, ports, and the IP addressing scheme, as shown on the right in Figure 1-14.

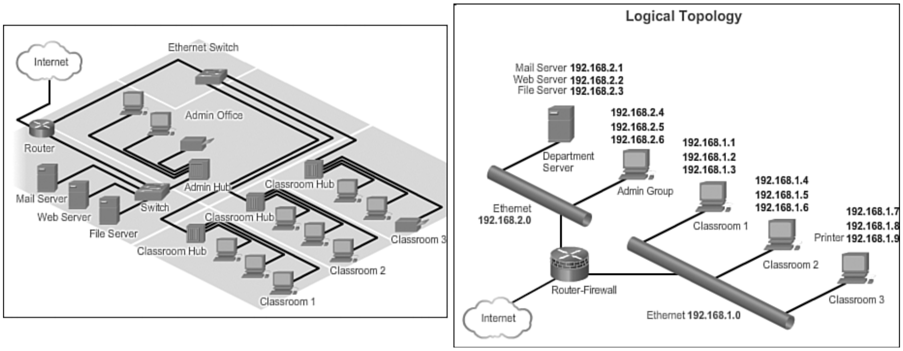


Figure 1-14 Physical Topology (Left) and Logical Topology (Right)

Interactive Graphic

Activity 1.3.1.7: Network Component Representations and Functions

Go to the online course to perform this practice activity.

LANs and WANs (1.3.2)

This section explains how LANs and WANs form computer networks.

Types of Networks (1.3.2.1)

Network infrastructures can vary greatly in terms of

- Size of the area covered
- Number of users connected
- Number and types of services available

Figure 1-15 illustrates the two most common types of network infrastructures:

- *Local-area network (LAN)*: A network infrastructure that provides access to users and end devices in a small geographical area.
- *Wide-area network (WAN)*: A network infrastructure that provides access to other networks over a wide geographical area.

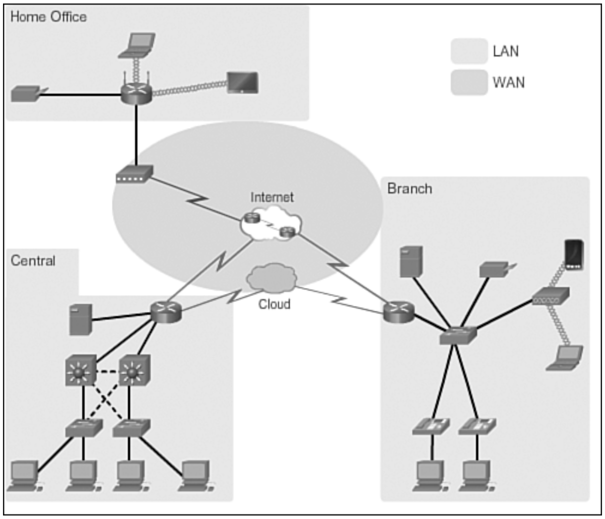


Figure 1-15 LANs Separated by Geographic Distance Connected by a WAN

Other types of networks include

- **Metropolitan-area network (MAN):** A network infrastructure that spans a physical area larger than a LAN but smaller than a WAN (e.g., a city). MANs are typically operated by a single entity, such as a large organization.
- *Wireless LAN (WLAN)*: Similar to a LAN but wirelessly interconnects users and endpoints in a small geographical area.
- *Storage-area network (SAN)*: A network infrastructure designed to support file servers and provide data storage, retrieval, and replication. It involves high-end servers, multiple disk arrays (called *blocks*), and Fibre Channel interconnection technology.

Local-Area Networks (1.3.2.2)

LANs are a network infrastructure that spans a small geographical area. Specific features of LANs include

- LANs interconnect end devices in a limited area such as a home, school, office building, or campus.

- A LAN is usually administered by a single organization or individual. The administrative control that governs the security and access control policies is enforced on the network level.
- LANs provide high-speed bandwidth to internal end devices and intermediary devices.

Wide-Area Networks (1.3.2.3)

WANs are a network infrastructure that spans a wide geographical area. WANs are typically managed by service providers (SPs) or Internet service providers (ISPs).

Specific features of WANs include

- WANs interconnect LANs over wide geographical areas such as between cities, states, provinces, countries, or continents.
- WANs are usually administered by multiple service providers.
- WANs typically provide slower-speed links between LANs.

The Internet (1.3.3)

This section explains how the Internet consists of many connected LANs and WANs.

The Internet (1.3.3.1)

Although there are benefits to using a LAN or WAN, most individuals need to communicate with a resource on another network, outside of the local network within the home, campus, or organization. This is done using the Internet.

As shown in Figure 1-16, the Internet is a worldwide collection of interconnected networks (internetworks or the Internet for short), cooperating with each other to exchange information using common standards. Through telephone wires, fiber-optic cables, wireless transmissions, and satellite links, Internet users can exchange information in a variety of forms.

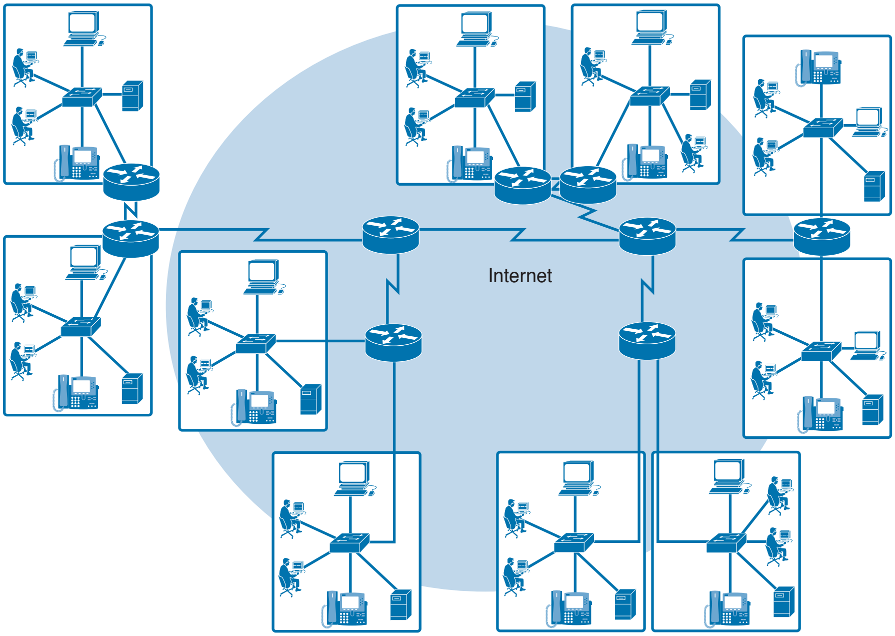


Figure 1-16 Internetworks Made Up of LANs and WANs

The Internet is a conglomerate of networks and is not actually owned by any individual or group. Ensuring effective communication across this diverse infrastructure requires the application of consistent and commonly recognized technologies and standards as well as the cooperation of many network administration agencies. There are organizations that have been developed for the purpose of helping to maintain structure and standardization of Internet protocols and processes. These organizations include the Internet Engineering Task Force (IETF), Internet Corporation for Assigned Names and Numbers (ICANN), and the Internet Architecture Board (IAB), plus many others.

Note

The term internet (with a lower case "i") is used to describe multiple networks interconnected. When referring to the global system of interconnected computer networks or the World Wide Web, the term Internet (with a capital "I") is used.

Intranet and Extranet (1.3.3.2)

Two other terms are similar to the term Internet:

- Intranet
- Extranet

Intranet is a term often used to refer to a private connection of LANs and WANs that belongs to an organization, and is designed to be accessible only by the organization's members, employees, or others who have authorization. An intranet is basically an internet that is usually only accessible from within the organization.

An organization may publish on its intranet web pages about internal events, health and safety policies, staff newsletters, and staff phone directories. For example, a school may have an intranet that includes class schedule information, online curriculum, and discussion forums. Intranets usually help eliminate paperwork and speed up workflows. An organization's intranet may be accessible to staff working outside of the organization by using secure connections to the internal network.

An organization may use an *extranet* to provide secure and safe access to individuals who work for different organizations but require company data. Examples of extranets include

- A company providing access to outside suppliers/contractors
- A hospital providing a booking system to doctors so they can make appointments for their patients
- A local office of education providing budget and personnel information to the schools in its district

Lab 1.3.3.3: Mapping the Internet

In this lab you will test network connectivity, trace network routes using different tools, and compare the results provided by those tools.

Connecting to the Internet (1.3.4)

This section explores the different ways to access the Internet.

Internet Access Technologies (1.3.4.1)

There are many different ways to connect users and organizations to the Internet.

Home users, teleworkers (remote workers), and small offices typically require a connection to an Internet service provider (ISP) to access the Internet. Connection options vary greatly depending on the ISP and the geographical location. However, popular choices include broadband cable, broadband digital subscriber line (DSL), wireless WANs, and mobile services.

Organizations typically require access to other corporate sites and the Internet. Fast connections are required to support business services, including IP phones, video conferencing, and data center storage.

Business-class interconnections are usually provided by service providers (SPs). Popular business-class services include business DSL, leased lines, and Metro Ethernet.

Connecting Remote Users to the Internet (1.3.4.2)

Figure 1-17 illustrates common Internet connection options for small office and home office users, which include

- *Cable*: Typically offered by cable television service providers, the Internet data signal is carried on the same coaxial cable that delivers cable television. It provides a high-bandwidth, always-on connection to the Internet. A special cable modem separates the Internet data signal from the other signals carried on the cable and provides an Ethernet connection to a host computer or LAN.

- *DSL*: Provides a high-bandwidth, always-on connection to the Internet. It requires a special high-speed modem that separates the DSL signal from the telephone signal and provides an Ethernet connection to a host computer or LAN. DSL runs over a telephone line, with the line split into three channels. One channel is used for voice telephone calls. This channel allows an individual to receive phone calls without disconnecting from the Internet. A second channel is a faster download channel, used to receive information from the Internet. The third channel is used for sending or uploading information. This channel is usually slightly slower than the download channel. The quality and speed of the DSL connection depends mainly on the quality of the phone line and the distance from your phone company's central office. The farther you are from the central office, the slower the connection.

- *Cellular*: Cellular Internet access uses a cell phone network to connect. Wherever you can get a cellular signal, you can get cellular Internet access. Performance will be limited by the capabilities of the phone and the cell tower to which it is connected. The availability of cellular Internet access is a real benefit in those areas that would otherwise have no Internet connectivity at all, and for people who are constantly on the go.

- *Satellite*: Satellite service is a good option for homes or offices that do not have access to DSL or cable. Satellite dishes require a clear line of sight to the satellite, so satellite service might not be an option in heavily wooded areas or places with other overhead obstructions. Speeds will vary depending on the contract, though they are generally good. Equipment and installation costs can be high (although check the provider for special deals), with a moderate monthly fee thereafter. The availability of satellite Internet access is a real benefit in those areas that would otherwise have no Internet connectivity at all.

- *Dial-up* **telephone:** An inexpensive option that uses any phone line and a modem. To connect to the ISP, a user calls the ISP access phone number. The low bandwidth provided by a dial-up modem connection is usually not sufficient for large data transfer, although it is useful for mobile access while traveling. A modem dial-up connection should only be considered when higher-speed connection options are not available.

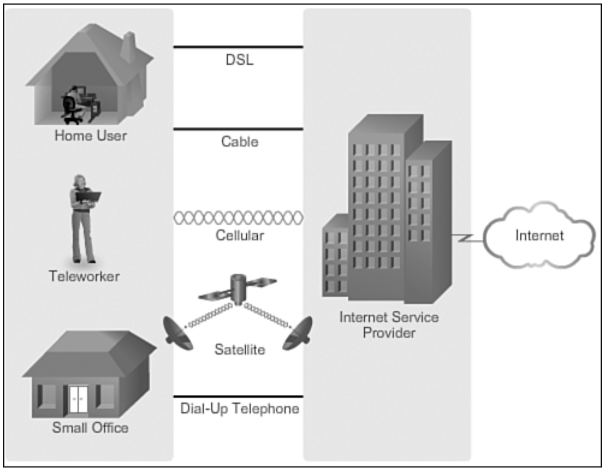


Figure 1-17 Internet Connection Options

Many homes and small offices are more commonly being connected directly with fiber-optic cables. This enables an ISP to provide higher bandwidth speeds and support more services such as Internet, phone, and TV.

The choice of connection varies depending on geographical location and service provider availability.

What are your options for connecting to the Internet?

Connecting Businesses to the Internet (1.3.4.3)

Corporate connection options differ from home-user options. Businesses may require higher bandwidth, dedicated bandwidth, and managed services. Connection options available differ depending on the number of service providers located nearby.

Common connection options for organizations include

- *Dedicated leased line*: This is a dedicated connection from the service provider to the customer premises. Leased lines are actually reserved circuits that connect geographically separated offices for private voice and/or data networking. The circuits are typically rented at a monthly or yearly rate, which tends to make it expensive. In North America, common leased-line circuits include T1 (1.54

Mbps) and T3 (44.7 Mbps), whereas in other parts of the world they are available in E1 (2 Mbps) and E3 (34 Mbps).

- *Metro Ethernet*: Metro Ethernet is typically available from a provider to the customer premises over a dedicated copper or fiber connection providing bandwidth speeds of 10 Mbps to 10 Gbps. Ethernet over Copper (EoC) is more economical than fiber-optic Ethernet service in many cases, is quite widely available, and reaches speeds of up to 40 Mbps. However, EoC is limited by distance. Fiber-optic Ethernet service delivers the fastest connections available at an economical price per megabit. Unfortunately, there are still many areas where this service is unavailable.
- **DSL:** Business DSL is available in various formats. A popular choice is symmetric DSL (SDSL), which is similar to asymmetric DSL (ADSL) but provides the same upload and download speeds. ADSL is designed to deliver bandwidth at different rates downstream than upstream. For example, a customer getting Internet access may have downstream rates that range from 1.5 to 9 Mbps, whereas upstream bandwidth ranges are from 16 to 640 kbps. ADSL transmissions work at distances up to 18,000 feet (5,488 meters) over a single copper twisted pair.
- **Satellite:** Satellite service can provide a connection when a wired solution is not available. Satellite dishes require a clear line of sight to the satellite. Equipment and installation costs can be high, with a moderate monthly fee thereafter. Connections tend to be slower and less reliable than terrestrial competition, which makes satellite less attractive than other alternatives.

The choice of connection varies depending on geographical location and service provider availability.

Packet Tracer
☐ **Activity**

Packet Tracer Activity 1.3.4.4: Network Representation

In this activity you will learn the essentials of using Packet Tracer. Packet Tracer is a downloadable software program that will help you with your Cisco Certified Network Associate (CCNA) studies. You will explore a relatively complex network that highlights a few of Packet Tracer's features. While doing so, you will learn how to access Help and the tutorials. Finally, you will explore how Packet Tracer serves as a modeling tool for network representations.

The Expanding Network (1.4)

The Internet has continuously expanded in the last two decades, and there is no indication that the expansion is slowing.

Network Trends (1.4.1)

In this section you will learn about emerging Internet trends.

New Trends (1.4.1.1)

When you look at how the Internet has changed so many of the things people do daily, it is hard to believe that it has only been around for most people for about 20 years. It has truly transformed the way individuals and organizations communicate. For example, before the Internet became so widely available, organizations and small businesses largely relied on print marketing to make consumers aware of their products. It was difficult for businesses to determine which households were potential customers, so businesses relied on mass print marketing programs. These programs were expensive and varied in effectiveness. Compare that to how consumers are reached today. Most businesses have an Internet presence where consumers can learn about their products, read reviews from other customers, and order products directly from the website. Social networking sites partner with businesses to promote products and services. Bloggers partner with businesses to highlight and endorse products and services. Most of this product placement is targeted to the potential consumer, rather than to the masses.

As new technologies and end-user devices come to market, businesses and consumers must continue to adjust to this ever-changing environment. The role of the network is transforming to enable the connections of people, devices, and information. There are several new networking trends that will affect organizations and consumers. Some of the top trends include

- Bring Your Own Device (BYOD)
- Online collaboration
- Video communication
- Cloud computing

These trends are interconnected and will continue to build off of one another in the coming years. The next couple of topics will cover these trends in more detail.

But keep in mind, new trends are being dreamed up and engineered every day. How do you think the Internet will change in the next 10 years? 20 years?

Bring Your Own Device (BYOD) (1.4.1.2)

The concept of any device, to any content, in any way is a major global trend occurring in business IT environments that requires significant changes to the way devices are used. This trend is known as ***Bring Your Own Device (BYOD)***.

In the past, an employee who needed access to the corporate network would be issued a company-provided device, such as a laptop or PC. These devices were typically expensive and were seen as tools for work. With the growth of consumer devices, and the related drop in cost, employees can be expected to have some of the most advanced tools for personal use. These personal tools include laptops, netbooks, tablets, smartphones, and e-readers. BYOD is about end users having the freedom to use these personal tools to access information and communicate across the corporate network. These can be devices purchased by the employer, devices purchased by the employee, or both. BYOD means any device, with any ownership, used anywhere. Extended connectivity through mobile and remote access to the corporate network gives employees tremendous flexibility and increased productivity.

BYOD is an influential trend that has or will touch every IT organization. There are many effects and considerations when providing for a BYOD environment.

BYOD Considerations (1.4.1.3)

In a BYOD environment, individuals are likely to have multiple devices connected to the network, possibly simultaneously. This leads to a large increase in the overall number of connected devices. The network must be designed in a way to support these additional devices and their traffic.

Additionally, a complete BYOD solution must consider how to extend the full services of the organization seamlessly, providing the same types of services to a user on a BYOD as are available to a user on a corporate PC. This includes collaboration tools such as integrated voice, video, IM, conferencing, and application sharing.

Finally, the network and applications must be able to offer quality of service regardless of whether the connectivity to those applications or collaboration tools occurs in the main campus, branch office, home office, or mobile teleworker location. Any solution must consider not only the employee using their own device, but also the individuals and applications that they are connecting and communicating with.

Security is a major consideration in a BYOD environment; therefore, any solution must be a highly secure mobile solution. Mobile and remote-access devices are typically not under the same strict control and scrutiny as employer-provided desktop and laptop computers. Therefore, appropriate security and user policies need to be applied to protect corporate data when employees connect with these devices. The range of those policies may vary depending on the spectrum of BYOD access that an organization wants.

Depending on the needs of the organization, a range of BYOD policies may be in place, from limited access to advanced BYOD implementation. Each of these implementations must include end-user agreements that outline the use of personal devices on corporate networks, policies for how and what those devices can access, and guidelines for how lost or stolen devices will be handled. Organizations may also need an agreement about when and if data can be accessed from the personal device of an employee. There have been several legal challenges recently for cases involving an employer who remotely "wiped" an employee-owned device, including both the corporate and personal data it contained. Imagine your surprise as an employee when you discover that by using your new tablet to access the corporate network, you unknowingly agreed to let IT delete your favorite family photos remotely.

Online Collaboration (1.4.1.4)

Employees want to connect to the network not only for access to data applications, but also to collaborate with one another. Collaboration is defined as "the act of working with another or others on a joint project."

For businesses, collaboration is a critical and strategic priority. To remain competitive, organizations must answer three primary collaboration questions:

- How can they get everyone on the same page?
- With decreased budgets and personnel, how can they balance resources to be in more places at once?
- How can they maintain face-to-face relationships with a growing network of colleagues, customers, partners, and peers in an environment that is more dependent on 24-hour connectivity?

One way to answer these questions in today's environment is through online collaboration tools. In traditional workspaces, and with BYOD environments alike, employees are taking advantage of voice, video, and conferencing services in collaboration efforts.

The ability to collaborate online is changing business processes. New and expanding collaboration tools allow individuals to quickly and easily collaborate, regardless of physical location. Organizations have much more flexibility in the way they are organized. Employees are no longer restricted to physical locations. Expert knowledge is easier to access than ever before. Expansions in collaboration allow organizations to improve their information gathering, innovation, and productivity

Collaboration tools give employees, customers, and partners a way to instantly connect, interact, and conduct business, through whatever communications channels they prefer, and achieve business objectives.

Collaboration Considerations (1.4.1.5)

The ability to work together to solve a common problem has proven to be one of mankind's greatest accomplishments. Great things can happen when we all work together. However, implementing a collaboration strategy is not always easy and there can be many challenges to overcome.

End users have high expectations that application performance will be maintained, regardless of time, location, and end device. Users also want to be able to have collaboration capabilities regardless of service provider, meaning they want those capabilities to be available whether they are connecting with collaboration tools across a corporate-maintained network or connecting via their home or hotel Internet connection.

For an organization to be successful in its collaboration strategy, it must determine its collaboration needs and establish which tools effectively meet those needs. Additionally, an organization must be able to prioritize traffic and effectively monitor and manage the performance of those collaboration tools. Finally, an organization must consider security requirements for collaboration and establish proper-use policies to ensure corporate data remains secure.

There's a wide range of collaboration tools available on the market today, including mobile applications, telePresence, and online web-conferencing tools, just to name a few.

Video Communication (1.4.1.6)

Another trend in networking that is critical in the communication and collaboration effort is the use of video. Video conferencing and person-to-person video calling are already proving particularly powerful for sales processes and for doing business at a distance, both locally and globally. Today, businesses are using video to transform key business processes to create competitive advantage, lower costs, and reduce environmental impact, particularly by avoiding the need for travel. Figure 1-18 shows the trend of video in communication.

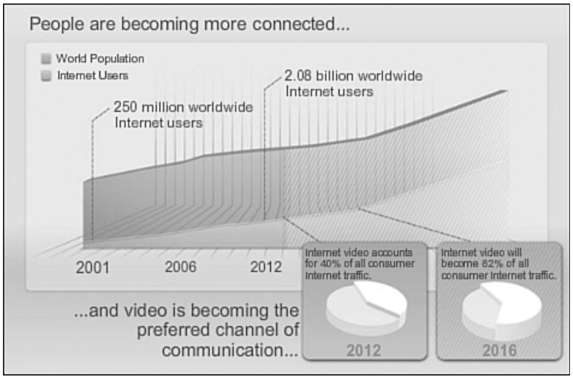


Figure 1-18 Use of Video on the Internet Is Growing.

Both consumers and businesses are driving this change. Video is becoming a key requirement for effective collaboration as organizations extend across geographical and cultural boundaries. Video users now demand the ability to view any content, on any device, anywhere.

Businesses are also recognizing the role of video to enhance the human network. The growth of media, and the new uses to which it is being put, is driving the need to integrate audio and video into many forms of communication. The audio conference will coexist with the video conference. Collaboration tools designed to link distributed employees will integrate desktop video to bring teams closer together.

There are many drivers and benefits for including a strategy for using video. Each organization is unique. The exact mix, and the nature of the drivers for adopting video, will vary from organization to organization, and by business function. Marketing, for example, may focus on globalization and fast-changing consumer tastes, while the focus of the Chief Information Officer (CIO) may be on cost savings by reducing travel costs of employees who need to meet face-to-face.

Cloud Computing (1.4.1.7)

Cloud computing is the use of computing resources (hardware and software) that are delivered as a service over a network. A company uses the hardware and software in the cloud and pays a service fee to the cloud provider.

Local computers no longer have to do all the “heavy lifting” when it comes to running network applications. The network of computers that make up the cloud handles them instead. The hardware and software requirements of the user are decreased. The user’s computer must interface with the cloud using software, which may be a web browser, and the cloud’s network takes care of the rest.

Cloud computing is another global trend changing the way organizations access and store data. Cloud computing uses cloud-based services to reduce costs and improve business processes. Cloud computing encompasses any subscription-based or pay-per-use service, in real time over the Internet, that extends the capabilities of IT without requiring investment in new infrastructure, training new personnel, or licensing new software. These services are available on demand and delivered economically to any device anywhere in the world without compromising security or function.

Cloud computing helps enterprise IT shift spending from large, one-time capital expenditures to ongoing operating expenses. It also allows enterprise IT to share cloud solution assets and provide dynamic, on-demand delivery of services to the enterprise as a whole.

Cloud computing offers the following potential benefits:

- **Organizational flexibility:** Users can access the information anytime and anyplace using a web browser.
- **Agility and rapid deployment:** The IT department can focus on delivering the tools to mine, analyze, and share the information and knowledge from databases, files, and people.
- **Reduced cost of infrastructure:** Technology is moved from on site to a cloud provider, eliminating the cost of hardware and applications.
- **Refocus of IT resources:** Cost savings of hardware and applications can be applied elsewhere.
- **Creation of new business models:** Applications and resources are easily accessible, so companies can react quickly to customer needs. This helps them set strategies to promote innovation while potentially entering new markets.

Types of Clouds (1.4.1.8)

There are four primary types of clouds:

- **Public clouds:** Cloud-based applications and services offered in a public cloud are made available to the general population. Services may be free or may be offered on a pay-per-use model, such as paying for online storage. A public cloud uses the Internet to provide services.
- **Private clouds:** Cloud-based applications and services offered in a private cloud are intended for a specific organization or entity, such as the government. A private cloud can be set up using the organization’s private network, though this can be expensive to build and maintain. A private cloud can also be managed by an outside organization with strict access security.
- **Custom clouds:** These are clouds built to meet the needs of a specific industry, such as healthcare or media. Custom clouds can be private or public.
- **Hybrid clouds:** A hybrid cloud is made up of two or more clouds (for example, part custom and part public), where each part remains a distinctive object but both parts are connected using a single architecture. Individuals on a hybrid cloud would be able to have degrees of access to various services based on user access rights.

Data Centers (1.4.1.9)

Cloud computing is possible because of data centers. A *data center* is a facility used to house computer systems and associated components, including

- Redundant data communications connections
- High-speed virtual servers (sometimes referred to as server farms or server clusters)
- Redundant storage systems (typically use SAN technology)
- Redundant or backup power supplies
- Environmental controls (e.g., air conditioning, fire suppression)
- Security devices

A data center can occupy one room of a building, one or more floors, or an entire building. Modern data centers make use of cloud computing and virtualization to efficiently handle large data transactions. Virtualization is the creation of a virtual version of something, such as a hardware platform, operating system (OS), storage device, or network resources. Whereas a physical computer is an actual discrete device, a virtual machine consists of a set of files and programs running on an actual physical system. Unlike multitasking, which involves running several programs on the same OS, virtualization runs several different OSs in parallel on a single CPU. This drastically reduces administrative and cost overheads.

Data centers are typically very expensive to build and maintain. For this reason, only large organizations use privately built data centers to house their data and provide services to users. For example, a large hospital may own a separate data center where patient records are maintained electronically. Smaller organizations that cannot afford to maintain their own private data center can reduce the overall cost of ownership by leasing server and storage services from a larger data center organization in the cloud.

Network Security (1.4.2)

This section explores how securing a network is becoming an increasingly complex task.

Security Threats (1.4.2.1)

Network security is an integral part of computer networking. As new technologies and trends emerge, so too must the protections that organizations use. Network security requirements must take into account the BYOD environment, the collaboration applications, video requirements, and cloud computing needs. Network security must be able to secure the corporate data while still allowing for the quality of service that is expected of each technology.

Securing a network involves protocols, technologies, devices, tools, and techniques to secure data and mitigate threats. Many external network security threats today are spread over the Internet. The most common external threats to networks include

- **Viruses, worms, and Trojan horses:** Malicious software and arbitrary code running on a user device
- **Spyware and adware:** Software installed on a user device that secretly collects information about the user
- **Zero-day attack, also called zero-hour attack:** An attack that occurs on the first day that a vulnerability becomes known
- **Hacker attack:** An attack by a knowledgeable person using software or network vulnerabilities to exploit devices or network resources
- **Denial of service attack:** An attack designed to slow or crash applications and processes on a network device
- **Data interception and theft:** An attack to capture private information from an organization's network
- **Identity theft:** An attack to steal the login credentials of a user in order to access private data

It is equally important to consider internal threats. There have been many studies that show that the most common data breaches happen because of employees. This can be attributed to lost or stolen devices, accidental misuse by employees, and even malicious insiders. With the evolving BYOD strategies, corporate data is much more vulnerable. Therefore, when developing a security policy, it is important to address both external and internal security threats. Figure 1-19 depicts threats from internal and external sources.

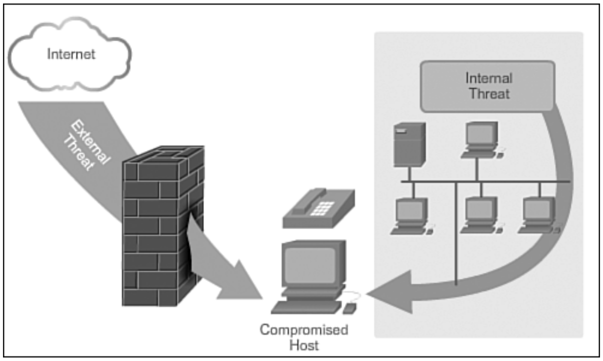


Figure 1-19 Network Threats

Security Solutions (1.4.2.2)

No single solution can protect the network from the variety of threats that exist. For this reason, security should be implemented in multiple layers, using more than one security solution. If one security component fails to identify and protect the network, others still stand.

The network security implementation for a corporate network usually consists of many components built into the network to monitor and filter traffic. Ideally, all components work together, which minimizes maintenance and improves security.

Network security components for a home or small office network should include, at a minimum, the following:

- **Antivirus and antispyware:** To protect user devices from malicious software.
- **Firewall filtering:** To block unauthorized access to the network. This may include a host-based firewall system that is implemented to prevent unauthorized access to the host device, or a basic filtering service on the home router to prevent unauthorized access from the outside world into the network.

Larger networks and corporate networks often have additional security requirements:

- **Dedicated firewall system:** To provide more advanced firewall capability that can filter large amounts of traffic with more granularity
- **Access control lists (ACL):** To further filter access and traffic forwarding
- **Intrusion prevention system (IPS):** To identify fast-spreading threats, such as zero-day or zero-hour attacks
- **Virtual private network (VPN):** To provide secure access to remote workers

Network security requirements must take into account the network environment, as well as the various applications and the computing requirements. Both home environments and businesses must be able to secure their data, while still allowing for the quality of service that is expected of each technology. Additionally, the security solution implemented must be adaptable to the growing and changing trends of the network.

The study of network security threats and mitigation techniques starts with a clear understanding of the underlying switching and routing infrastructure used to organize network services.

Interactive Graphic

Activity 1.4.2.3: Network Security Terminology

Go to the online course to perform this practice activity.

Network Architectures (1.4.3)

This section explores network architectures and how they evolve to handle new technologies.

Cisco Network Architectures (1.4.3.1)

The role of the network has changed from a data-only network to a system that enables the connections of people, devices, and information in a media-rich, converged network environment.

In order for networks to function efficiently and grow, the network must be built upon a standard architecture. The *network architecture* refers to the devices, connections, and products that are integrated to support the necessary technologies and applications. A well-planned network technology architecture helps to ensure that any device can be connected across any combination of network, increases cost efficiency by integrating network security and management, and improves business processes.

With the constant evolution of networks, Cisco has updated its enterprise architectures and frameworks and has created the following three enterprise architectures to address the new network trends, as shown in Figure 1-20:

- Borderless networks architecture
- Collaboration architecture
- Data center and virtualization architecture

These three enterprise technology architectures can be implemented separately, or combined.

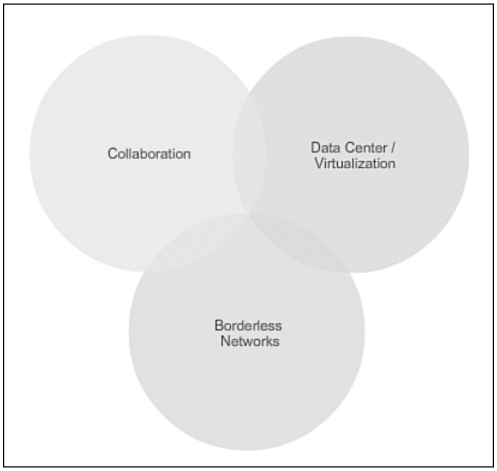


Figure 1-20 Three Cisco Network Architectures

Cisco Borderless Network (1.4.3.2)

The Cisco Borderless Network Architecture is a network solution that enables organizations and individuals to connect securely, reliably, and seamlessly to the corporate network in a BYOD environment.

This architecture separates the network functions into four areas of responsibility:

- **Cisco Borderless End Point/User Services:** Connects the various devices to provide access to network services. Devices that can connect to the borderless network can range from PCs to tablets and smartphones.
- **Cisco Borderless Network Services:** Optimizes the network connection and includes wireless access, secure access to corporate assets, and video performance optimization.
- **Cisco Borderless Network Systems:** Spans an organization from initial device network access to connecting devices to the cloud.
- **Cisco Borderless Infrastructure:** Supports services and systems with an infrastructure of scalable and resilient hardware and software.

The borderless network architecture supports a highly secure, high-performing network that is accessible to a wide range of devices. It needs to be flexible enough to scale in its support for future growth in terms of business expansion, including BYOD, mobility, and cloud computing, and must be able to support the growing requirements for online voice and video.

Collaboration Architecture (1.4.3.3)

To help organizations meet expanding collaboration needs, Cisco provides a collaboration architecture consisting of four categories of collaboration products:

- **TelePresence:** Provides next-generation video conferencing, where everyone, everywhere can be face-to-face and more effective through the most natural and lifelike communications experience available.
- **Collaboration Applications:** Stay connected and productive with voice, video, and web conferencing; messaging; mobile applications; and enterprise social software. For example, Cisco WebEx Meetings enables users to create and attend web conference calls. Users can meet to present ideas, share desktops, work on files together, and collaborate with others. Callers can see one another using webcams, and meetings can be recorded for people who are unable to attend.
- **Customer Collaboration:** Creates the foundation for positive customer service, a primary factor in building a stronger business. An example of this is the Cisco SocialMiner social media customer care solution. It can help companies proactively respond to customers and prospects communicating through public social media networks such as Twitter, Facebook, and other public forums or blogging sites.

- **Unified Communications:** View, optimize, and manage the entire communications system from one screen. With Cisco Unified Communications, organizations can seamlessly manage voice, video, mobility, and presence services between IP endpoints, media-processing devices, Voice over IP (VoIP) gateways, mobile devices, and multimedia applications.

Data Center Architecture (1.4.3.4)

The Cisco Unified Data Center is a complete data center infrastructure architecture that combines computing, networking, security, virtualization, and management solutions in a framework that delivers outstanding performance for physical and virtualized business applications. It is uniquely capable of providing the kind of simplicity, performance, and security that IT departments demand as they transition from physical to virtual to cloud environments.

The Cisco Unified Data Center incorporates three main data center technologies:

- **Cisco Unified Computing:** Integrates computing, networking, and storage resources to provide a unique, open, managed system that can scale to hundreds of server blades and thousands of desktops on virtual machines. Cisco Unified Computing reduces infrastructure costs, and can be deployed nearly 90 percent more quickly than traditional server platforms.
- **Cisco Unified Fabric:** Flexible network solutions deliver network services to servers, storage, and applications, providing transparent convergence, scalability, and sophisticated intelligence using Cisco Nexus and Catalyst switches.
- **Cisco Unified Management:** Provides the framework for IT service-creation and self-service capabilities, enabling IT to operate more efficiently and to more quickly offer new services to the business.

CCNA (1.4.3.5)

The three Cisco architectures previously discussed are built on an infrastructure of scalable and resilient hardware and software. Components of the architectures come together to build network systems that span your organization from network access to the cloud, and provide organizations with the services they need.

At the foundation of all three of these architectures, and in fact, at the foundation of the Internet itself, are routers and switches. Routers and switches transport data, voice, and video communications, allow for wireless access, and provide for security. After a basic network infrastructure with routing and switching is built, organizations can grow their network over time, adding features and functionality in an integrated solution.

As the use of these integrated, expanding networks increases, so does the need for training for individuals who implement and manage network solutions. This training must begin with the routing and switching foundation. Achieving Cisco Certified Network Associate (CCNA) certification is the first step in helping an individual prepare for a career in networking.

CCNA certification validates an individual's ability to install, configure, operate, and troubleshoot medium-size routed and switched networks, including implementation and verification of connections to remote sites in a WAN. This CCNA curriculum includes lessons that address the basic mitigation of security threats, introduction to wireless networking concepts and terminology, and performance-based skills. This CCNA curriculum also includes the use of various protocols, such as Internet Protocol (IP), Open Shortest Path First (OSPF), Serial Line Interface Protocol (SLIP), Frame Relay, VLANs, Ethernet, access control lists (ACLs), and others.

This course helps set the stage for networking concepts and basic routing and switching configurations and is a start on your path for CCNA certification.

Lab 1.4.3.6: Researching IT and Networking Job Opportunities

In this lab you will research job opportunities and reflect on that research.

Summary (1.5)

This section reviews the key networking concepts explained in this chapter.

Class Activity 1.5.1.1: Draw Your Concept of the Internet Now

In this activity you will use the knowledge you have acquired throughout Chapter 1, and the modeling activity document that you prepared at the beginning of this chapter.

Networks and the Internet have changed the way we communicate, learn, work, and even play.

Networks come in all sizes. They can range from simple networks consisting of two computers, to networks connecting millions of devices.

The Internet is the largest network in existence. In fact, the term *Internet* means a network of networks. The Internet provides the services that enable us to connect and communicate with our families, friends, and coworkers.

The network infrastructure is the platform that supports the network. It provides the stable and reliable channel over which communication can occur. It is made up of network components, including end devices, intermediate devices, and network media.

Networks must be reliable. This means the network must be fault tolerant and scalable, provide quality of service, and ensure security of the information and resources on the network. Network security is an integral part of computer networking, regardless of whether the network is limited to a home environment with a single connection to the Internet or is as large as a corporation with thousands of users. No single solution can protect the network from the variety of threats that exist. For this reason, security should be implemented in multiple layers, using more than one security solution.

The network infrastructure can vary greatly in terms of size, number of users, and number and types of services that are supported on it. The network infrastructure must grow and adjust to support the way the network is used. The routing and switching platform is the foundation of any network infrastructure.

This chapter focused on networking as a primary platform for supporting communication. The next chapter will introduce you to the Cisco Internetwork Operating System (IOS) used to enable routing and switching in a Cisco network environment.

Practice

The following activities provide practice with the topics introduced in this chapter. The Labs and Class Activities are available in the companion *Network Basics Lab Manual* (978-1-58713-313-8). The Packet Tracer Activities PKA files are found in the online course.

Class Activities

Class Activity 1.0.1.2: Draw Your Concept of the Internet

Class Activity 1.5.1.1: Draw Your Concept of the Internet Now

Labs

Lab 1.2.1.3: Researching Converged Network Services

Lab 1.1.1.8: Researching Network Collaboration Tools

Lab 1.3.3.3: Mapping the Internet

Lab 1.4.3.6: Researching IT and Networking Job Opportunities

Packet Tracer Activity

Packet Tracer Activity 1.3.4.4: Network Representation

Check Your Understanding

Complete all the review questions listed here to test your understanding of the topics and concepts in this chapter. The appendix, “Answers to the ‘Check Your Understanding’ Questions,” lists the answers.

1. Which of the following is an example of QoS?

   A. Data arrives via different physical media.

   B. Intermediate devices deliver all packets along the same physical route.

   C. Different types of traffic are delivered according to planned priority.

   D. An intermediate device fails and traffic is rerouted and delivered reliably.

2. Fill in the blanks of the sentence with the best terms from the following list (not all of which will be used): *fault tolerance, security, QoS, data integrity, and scalability.*

   The network designer for the small bank needed to plan for the network to double in size over 5 years, requiring her to allow for ____. Of course, all information needed to be kept confidential and safe, so she incorporated __ into the design. She accounted for ___ when she ensured packets arrived with minimal loss or delay, and accounted for ___ by making sure the network would recover quickly if there was a hardware failure.

3. Which type of communications allows for dynamic routing over multiple paths and adaptation to failures in a network?

   A. Circuit switching

   B. QoS

   C. Leased fiber lines for packet delivery

   D. Packet-switched, connectionless data communications

4. Employees of an insurance company accessing company data on restricted local-area and wide-area networks is an example of using a(n)

   A. Internet

   B. Extranet

   C. Intranet

   D. BYOD nets

5. An organization that allows employees to use their own tablets and notebook computers in a secure environment has implemented which type of network?

   A. WAN

   B. BYOD

   C. QoS

   D. Intranet

6. A group of movie critics posting a recording of their weekly radio show about movies is an example of

   A. Podcasting

   B. Webhosting

   C. Blogging

   D. A wiki

7. When instructors provide common space on a computer to create and share documents they can access on their mobile devices or desktops, they are using:

   A. Podcasts

   B. Instant messaging

   C. Social media

   D. Collaboration tools

8. The complexity of a message can affect successful communication across a network. The level of complexity in a message is considered a(n):

   A. Switching factor

   B. External factor

   C. Internal factor

   D. Routing factor

9. Which of the following describes a converged network?

   A. A network that enables people in different countries to work together in the cloud

   B. A network that allows songs and videos to be shared peer to peer

   C. A network that carries voice, video, and data traffic at the same time

   D. A network that allows secure access to the Internet from inside a firewall

10. A system that allows communications between local networks around the world is a/the

    A. BYOD

    B. Internet

    C. LANs

    D. SAN

11. Which of the following is an intermediary device?

    A. Router

    B. Hand-held device

    C. Security camera

    D. Laptop

12. A group of computers connected to store data is which type of network?

    A. LAN
    B. SAN
    C. BYOD
    D. WAN

13. What is the function of a WLAN?

    A. Wireless connection in a small geographical area
    B. Wired connections in a local-area network
    C. Worldwide communications between local-area networks
    D. Wireless communications across the Internet

14. If there are two DSL customers with consistent line quality, which will have the faster connection speed?

    A. The one closest to the cable company
    B. They will have the same connection speed
    C. The one closest to the central office
    D. The one whose cable modem is on the last mile

15. Which items can be associated with network availability? (Choose three.)

    A. Firewall devices
    B. Antivirus software
    C. Collaboration software
    D. Redundant devices

This page intentionally left blank

Index