Introduction to Networks

Companion Guide

Cisco | Networking Academy®
Mind Wide Open™

FREE SAMPLE CHAPTER

SHARE WITH OTHERS

Introduction to Networks

Companion Guide

Cisco Networking Academy

Cisco Press

800 East 96th Street

Indianapolis, Indiana 46240 USA

Cisco Networking Academy

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

Printed in the United States of America

First Printing December 2013

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

ISBN-13: 978-1-58713-316-9

ISBN-10: 1-58713-316-4

Warning and Disclaimer

This book is designed to provide information about the Cisco Networking Academy Introduction to Networks 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
John Edwards

Technical Editor
Aubrey Adams

Editorial Assistant
Vanessa Evans

Designer
Mark Shirar

Composition
Studio Galou, LLC

Indexer
Larry Sweazy

Proofreader
Debbie Williams

Trademark Acknowledgements

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

Mark A. Dye

Mark is the lead network engineer for Kwajalein Range Services at Ronald Reagan Ballistic Missile Defense Test Site on Kwajalein, Marshall Islands. He is responsible for the network team that provides design, deployment, and operation of all the missile test range data networks across ten islands as well as three continental U.S. locations.

He has previously worked as subject matter expert and content team lead for the Cisco Academy Program as well as an author for multiple Cisco Network Academy Fundamentals online courses. He worked to develop and review courseware and assessments for both the Academy and certification programs.

For more than 20 years, Mark served as technology manager for The Bevill Center for Advanced Manufacturing Technology of Alabama Technology Network. He developed and implemented comprehensive network strategies for intranet and Internet, including policies, administrative procedures, network security, and interconnectivity. He also implemented and taught Cisco Networking Academy Fundamentals of Wireless LANs, Fundamentals of Network Security, and CCNA and CCNP courses at The Bevill Center for instructors and students.

Allan D. Reid

Allan is a professor and program supervisor at Centennial College in Toronto, Ontario, Canada, where he teaches courses in networking, network security, virtualization, and cloud computing. He is the lead for the Centennial College ASC/ITC and has been teaching the academy curriculum since one of the earliest versions.

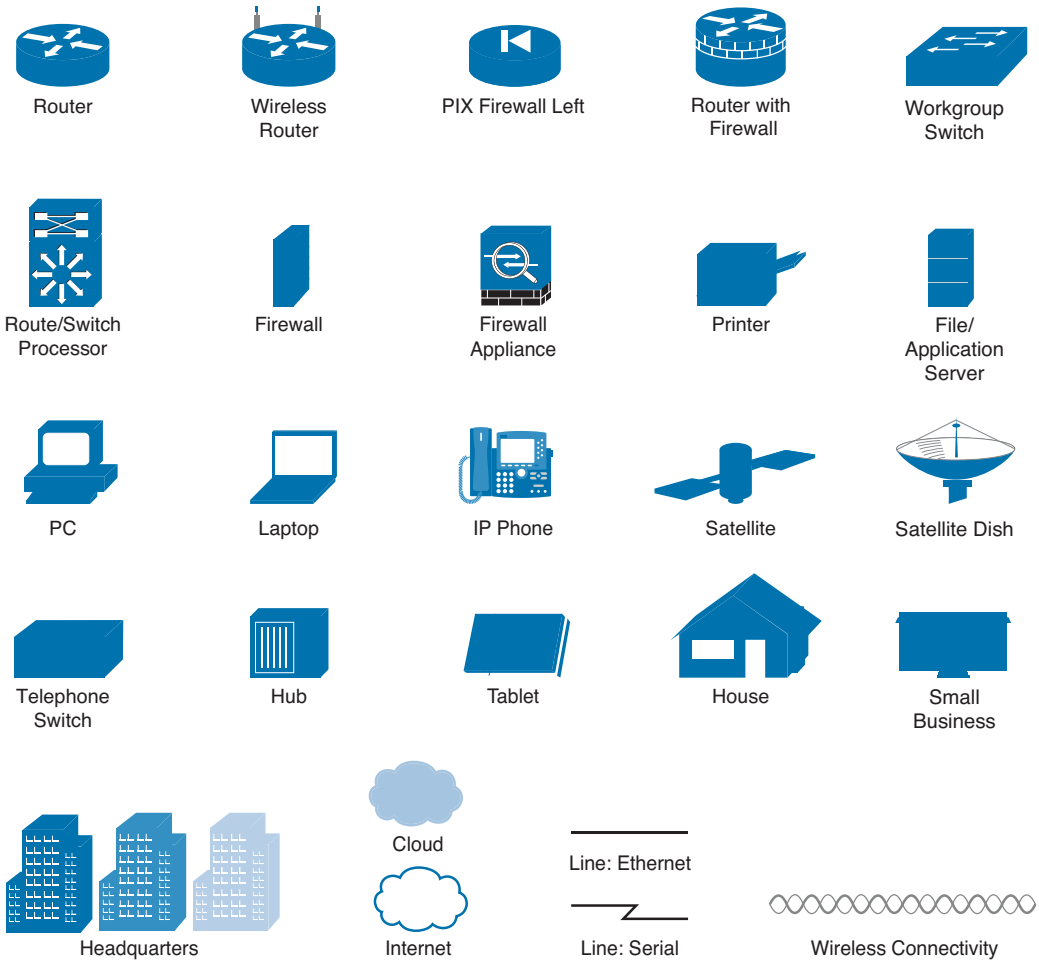
Allan has authored multiple books and online courses for the Cisco Academy program, where he is a subject matter expert and content team lead. He works as part of the core team to develop state-of-the-art assessments and courseware.

Outside of his academic responsibilities, Allan has been active in the computer and networking fields for more than 30 years and is currently a principal in a company involved in the design, installation, and management of network solutions for small- to medium-sized companies.

Contents at a Glance

Contents

Syntax Conventions



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

- **Boldface** indicates commands and keywords that are entered literally as shown. In actual configuration examples and output (not general command syntax), boldface indicates commands that are manually input by the user (such as a **show** command).
- *Italics* indicate arguments for which you supply actual values.
- Vertical bars (|) separate alternative, mutually exclusive elements.

- Square brackets ([ ]) indicate an optional element.
- Braces ({ }) indicate a required choice.
- Braces within brackets ([{ }]) indicate a required choice within an optional element.

Introduction

Introduction to Networks Companion Guide is the official supplemental textbook for the Cisco Network Academy CCNA Introduction to Networks course. Cisco Networking Academy is a comprehensive program that delivers information technology skills to students around the world. The curriculum emphasizes real-world practical application, while providing opportunities for you to gain the skills and hands-on experience needed to design, install, operate, and maintain networks in small- to medium-sized businesses, as well as enterprise and service provider environments.

As a textbook, this book provides a ready reference to explain the same networking concepts, technologies, protocols, and devices as the online curriculum. This book emphasizes key topics, terms, and activities and provides some alternate explanations and examples as compared with the 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 Introduction to Networks course. The book, as well as the course, is designed as an introduction to data network technology for those pursuing careers as network professionals as well as those who need only an introduction to network technology for professional growth. Topics are presented concisely, starting with the most fundamental concepts and progressing to a comprehensive understanding of network communication. The content of this text provides the foundation for additional Cisco Academy courses, and preparation for the CCENT and CCNA Routing and Switching certifications.

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" 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.
- **Notes:** These are short sidebars that point out interesting facts, timesaving methods, and important safety issues.
- **Chapter summaries:** At the end of each chapter is a summary of the chapter's key concepts. It provides a synopsis of the chapter and serves as a study aid.
- **Practice:** At the end of each chapter there is a full list of all the Labs, Class Activities, and Packet Tracer Activities to refer back to for study time.

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 from inside the chapter. The 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 almost 200 terms.

Practice

Practice makes perfect. This new Companion Guide offers you ample opportunities to put what you learn into 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, "Answers to the 'Check Your Understanding' Questions," provides an answer key to all the questions and includes an explanation of each answer.

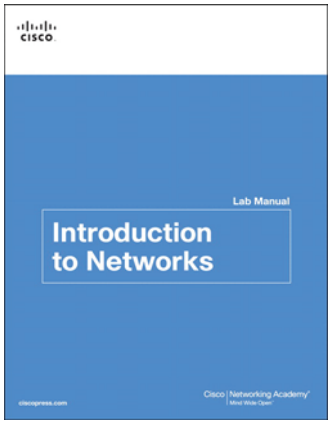
Packet Tracer
Activity

Video

- **Labs and activities:** Throughout each chapter, you will be directed back to the online course to take advantage of the activities created to reinforce concepts. In addition, at the end of each chapter, there is a "Practice" section that collects a list of all the labs and activities to provide practice with the topics introduced in this chapter. The labs and class activities are available in the companion *Introduction to Networks Lab Manual* [ISBN 978-1-58713-312-1]. The Packet Tracer Activities PKA files are found in the online course.
- **Page references to online course:** After headings, 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.

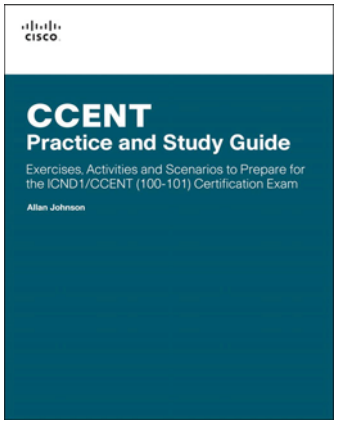
Lab Manual

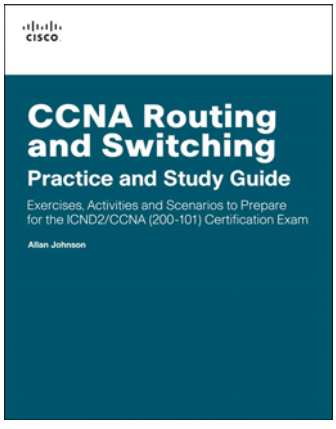
The supplementary book *Introduction to Networks Lab Manual*, by Cisco Press (ISBN 978-1-58713-312-1), contains all the labs and class activities from the course.



Practice and Study Guide

Additional Study Guide 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—the CCENT edition follows the course outlines for *Introduction to Networks* and *Routing and Switching Essentials*. The CCNA edition follows the course outlines for *Scaling Networks* and *Connecting Networks*.





Packet Tracer Activity

About Packet Tracer Software and Activities

Interspersed throughout the chapters you'll find many activities to work with the Cisco Packet Tracer tool. Packet Tracer allows 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 this 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 Introduction to Networks course and is divided into 11 chapters, one appendix, and a glossary of key terms:

- **Chapter 1, "Exploring the Network":** Introduces the concept of a network and provides an overview of the different types of networks encountered. It examines how networks impact the way we work, learn, and play. This chapter also examines new trends in networks such as video, cloud computing, and BYOD, and how to help ensure that we have a robust, reliable, secure network to support these trends.
- **Chapter 2, "Configuring a Network Operating System":** Introduces the operating system used with most Cisco devices: the Cisco IOS. The basic purpose and functions of the IOS are described as well as the methods to access the IOS. The chapter will also present maneuvering through the IOS command-line interface as well as basic IOS device configuration.
- **Chapter 3, "Network Protocols and Communications":** Examines the importance of rules or protocols for network communication. It explores the OSI reference model and the TCP/IP communication suite, examining how these models provide the necessary protocols to allow communication to occur on a modern converged network.
- **Chapter 4, "Network Access":** Introduces the lowest layer of the TCP/IP model: the transport layer. This layer is essentially the equivalent of the OSI data link layer and the physical layer. The chapter discusses how this layer prepares network layer packets for transmission, controls access to the physical media, and transports the data across various media. This chapter includes a description of the encapsulation protocols and processes that occur as data travels across the LAN and the WAN as well as the media used.
- **Chapter 5, "Ethernet":** Examines the functionality of one of the most common LAN protocols in use today. It explores how Ethernet functions and interacts with the TCP/IP protocol suite to provide high-speed data communications.
- **Chapter 6, "Network Layer":** Introduces the function of the network layer—routing—and the basic device that performs this function—the router. The important routing concepts related to addressing, path determination, and data packets for both IPv4 and IPv6 will be presented. The chapter also introduces the construction of a router and the basic router configuration.
- **Chapter 7, "Transport Layer":** Introduces Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) and examines how each transports information across the network. It explores how TCP uses segmentation, the three-way handshake, and expectational acknowledgements to ensure reliable delivery of

data. It also examines the best-effort delivery mechanism provided by UDP and describes when this would be preferred over TCP.

- **Chapter 8, "IP Addressing":** Focuses on IPv4 and IPv6 network addressing, including the types of addresses and address assignment. It describes how to use the address mask or prefix length to determine the number of subnetworks and hosts in a network. This chapter also introduces Internet Control Message Protocol (ICMP) tools, such as ping and trace.
- **Chapter 9, "Subnetting IP Networks":** Examines how to improve network performance by optimally dividing the IP address space based on network requirements. It explores the calculation of valid host addresses and the determination of both subnet and subnet broadcast addresses. This chapter examines subnetting for both IPv4 and IPv6.
- **Chapter 10, "Application Layer":** Introduces some protocols of the TCP/IP application layer, which also relates to the top three layers of the OSI model. The chapter focuses on the role of the application layer and how the applications, services, and protocols within the application layer make robust communication across data networks possible. This will be demonstrated by examining some key protocols and services including HTTP, DNS, DHCP, SMTP/POP, Telnet, and FTP.
- **Chapter 11, "It's a Network":** Reexamines the various components found in a small network and describes how they work together to allow network growth. Network security and performance issues are examined, along with some of the commands that can be used to examine the configuration of devices and the performance of the network. Router and switch file systems are also examined, along with methods for backing up and restoring their configuration files.
- **Appendix A, "Answers to the 'Check Your Understanding' Questions":** This appendix lists the answers to the "Check Your Understanding" review questions that are 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, learn, work and play?
- How do networks support communication?
- What is a converged network?
- What are the four basic requirements of a reliable network?
- What are the uses of various network devices?
- How do the devices and topologies found in a LAN compare to those found in a WAN?
- What is the basic structure of the Internet?
- How do LANs and WANs connect to the Internet?
- What impact do BYOD, online collaboration, video, and cloud computing have on a business network?
- How are networking technologies changing the home environment?
- What are some basic security threats and solutions to both small and large networks?

Key Terms

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

Internet page 3
data networks page 4
Internet of Everything (IoE) page 5
communication page 7
collaboration page 7
virtual classroom page 7
learning spaces page 7
mobile learning page 7
communities page 11
servers page 13
clients page 13
network infrastructure page 15
VoIP page 16
TelePresence page 16
encoding page 18
topology page 18
converged network page 29
circuit-switched page 33
packet-switched page 34
quality of service (QoS) page 37
congested page 37
queuing page 38

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—creating 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.

The Networking Academy curriculum has a new component: 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 Introduction to Networks Lab Manual 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:

Class Activity 1.0.1.2: 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, and so on. Some items you might want to include are as follows:

- Devices/equipment
- Media (cabling)
- Link addresses or names
- Sources and 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 www.kk.org/internet-mapping.

Globally Connected (1.1)

Networks are all around us. They provide us with a way to communicate and share information and resources with individuals in the same location or around the world. This requires an extensive array of technologies and procedures that can readily adapt to varying conditions and requirements.

Networking Today (1.1.1)

For most individuals, the use of networks has become a daily occurrence. The availability of these networks has altered the way in which we interact with each other.

Networks in Our Daily Lives (1.1.1.1)

Among all 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.

In today's world, through the use of networks, we are connected like never before. People with ideas can communicate instantly with others to make those ideas a reality. News events and discoveries are known worldwide in seconds. Individuals can even connect and play games with friends separated by oceans and continents.

Networks connect people and promote unregulated communication. Everyone can connect, share, and make a difference.

Video

Video 1.1.1.1: View the video in the online course for an understanding of how the network impacts our daily lives.

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 mouse. 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 Internet phone calls
- 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, displaying weather and traffic video from webcams
- Check your bank balance and pay bills electronically

Innovators are figuring out 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 over the last 25 years, as depicted in the Figure 1-1. Now consider what changes will happen within the next 25 years. This future holds the *Internet of Everything (IoE)*.

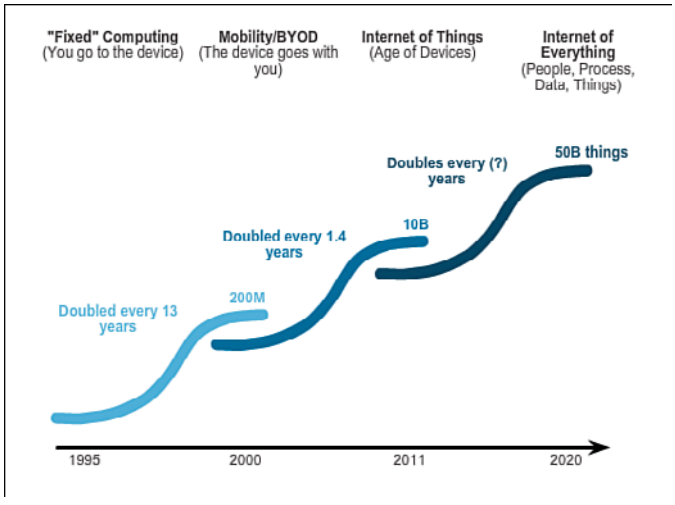


Figure 1-1 Evolution of the Network

The IoE is bringing together people, process, data, and things to make networked connections more relevant and valuable. It is turning information into actions that create new capabilities, richer experiences, and unprecedented economic opportunity for individuals, businesses, and countries.

What else do you think we will be able to do using the network as the platform?

The Global Community (1.1.1.3)

Advancements in networking technologies are perhaps the most significant change agents 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 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, from the way we learn, to the way we communicate, to 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. As shown in Figure 1-2, networks now

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

Figure 1-2 Networks Support the Way We Learn

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.

Video

Video 1.1.1.4: Click the second graphic in the online course to view a video that illustrates the way networks have expanded the classroom.

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)

Networks eliminate geographic and time-zone boundaries, allowing us to easily communicate with individuals from around the world.

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 communication include

- **Instant messaging (IM)/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 a means to communicate their thoughts to a global audience without technical knowledge of web design. 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 can 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 allows people to share files with each other without having to store and download them from a central server. The user joins the P2P network by simply installing the P2P software. This lets the user 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 about violating 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)

Networks provide fast, reliable access to business resources regardless of the geographic location of the employee.

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 that networks are being used to make us more successful in the workplace. Some of these scenarios are available through the Cisco website at www.cisco.com.

Networks Support the Way We Play (1.1.1.7)

Networks allow us to locate and interact with others who share common interests.

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 to 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.

Figure 1-3 illustrates some of the ways that networks support the way that we play. How do you play on the Internet?

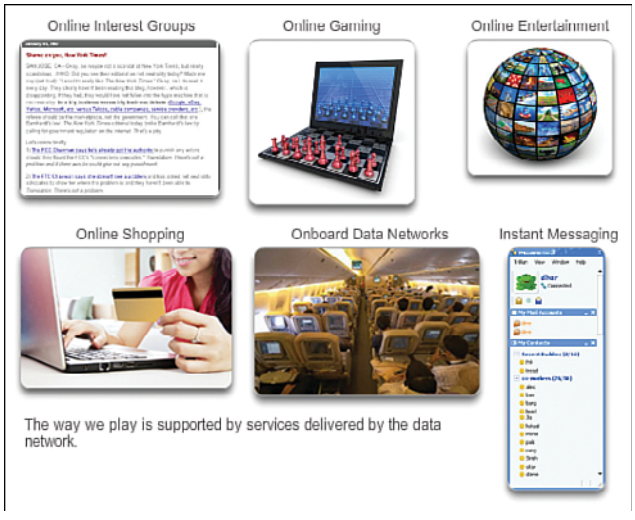


Figure 1-3 Networks Support the Way We Play

Lab 1.1.1.8: Researching Collaboration Tools

In this lab, you will research and explore various collaborative tools. You will share documents, explore conferencing and web meetings, and create a wiki page.

Providing Resources in a Network (1.1.2)

To efficiently provide resources to end users, networks occur in many sizes and forms.

Networks of Many Sizes (1.1.2.1)

Networks come in all sizes, as shown in Figure 1-4. They can range from simple networks consisting of two computers to networks connecting millions of devices.

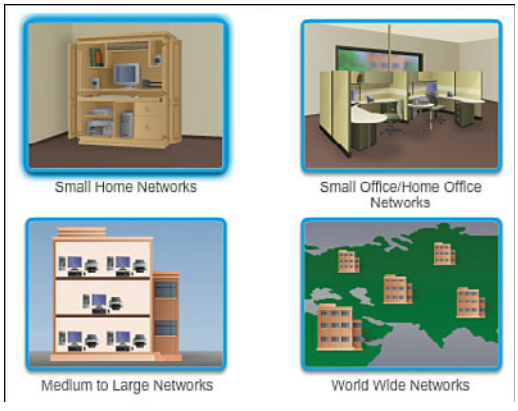


Figure 1-4 Networks Come in Many Sizes

Simple networks installed in homes enable sharing of resources, such as printers, documents, pictures, and music between a few local computers. Home networks are also used to connect several devices to the Internet.

Home office networks and small office networks are often set up by individuals who work from a home or remote office and need to connect to a corporate network or other centralized resources. Additionally, many self-employed entrepreneurs use home office and small office networks to advertise and sell products, order supplies, and communicate with customers. Communication over a network is usually more efficient and less expensive than traditional forms of communication, such as regular mail or long-distance phone calls.

In businesses and large organizations, networks can be used on an even broader scale to allow employees to provide consolidation, storage, and access to information on network servers. Networks also allow rapid communication such as email, instant messaging, and collaboration among employees. In addition to internal organizational benefits, many organizations use their networks to provide products and services to customers through their connection to the Internet. These networks can have many locations with hundreds or thousands of interconnected computers.

The Internet is the largest network in existence. In fact, the term *Internet* means a "network of networks." The Internet is literally a collection of interconnected private and public networks, such as the ones described previously. Businesses, small office networks, and even home networks usually provide a shared connection to the Internet. The Internet connects hundreds of millions of computers worldwide.

It is incredible how quickly the Internet has become an integral part of our daily routines.

Clients and Servers (1.1.2.2, 1.1.2.3)

All computers connected to a network that participate directly in network communication are classified as hosts or end devices. Hosts can send and receive messages on the network. In modern networks, end devices can act as a client, a server, or both. The software installed on the computer determines which role the computer plays.

Servers are hosts that have software installed that enable them to provide information, like email or web pages, to other hosts on the network. Each service requires separate server software. For example, a host requires web server software to provide web services to the network.

Clients are computer hosts that have software installed that enable them to request and display the information obtained from the server. An example of client software is a web browser, like Windows Internet Explorer. This client software accesses web pages that are stored on a web server. Other common client software includes Microsoft Outlook, used to access email on a web server, and Windows Explorer, used to access files stored on a file server.

A computer with server software can provide services simultaneously to one or many clients.

Additionally, a single computer can run multiple types of server software. In a home or small business, it might be necessary for one computer to act as a file server, a web server, and an email server.

A single computer can also run multiple types of client software. There must be client software for every service required. With multiple clients installed, a host can connect to multiple servers at the same time. For example, a user can check email and view a web page while instant messaging and listening to Internet radio.

Peer-to-Peer (1.1.2.4)

Client and server software usually runs on separate computers, but it is also possible for one computer to carry out both roles at the same time. In small businesses and homes, many computers function as the servers and clients on the network. This type of network is called a peer-to-peer network and is illustrated in Figure 1-5.

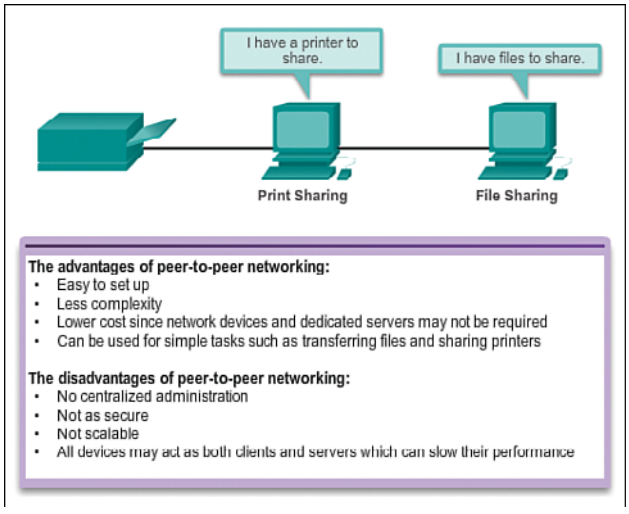


Figure 1-5 Peer-to-Peer Network

The simplest peer-to-peer network consists of two directly connected computers using a wired or wireless connection.

Multiple PCs can also be connected to create a larger peer-to-peer network, but this requires a network device, such as a hub, to interconnect the computers.

Peer-to-peer networks are easy to set up, are less complex, and can be created at lower cost than client-server networks because network devices and dedicated servers might not be required. These networks can be used for simple tasks such as transferring files and sharing printers. Peer-to-peer networks have no centralized administration, are not as secure or scalable as client-server networks, and often suffer from host performance issues if they are acting as both a client and a server at the same time.

In larger businesses, because of the potential for high amounts of network traffic, it is often necessary to have dedicated servers to support the number of service requests.

LANs, WANs, and the Internet (1.2)

Many different components are required to allow a network to provide services and resources. These various components work together to ensure that resources are delivered in an efficient manner to those requiring the services.

Components of a Network (1.2.1, 1.2.1.1)

The *network infrastructure* contains three categories of network components—devices, media, and services—as shown in Figure 1-6.

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.

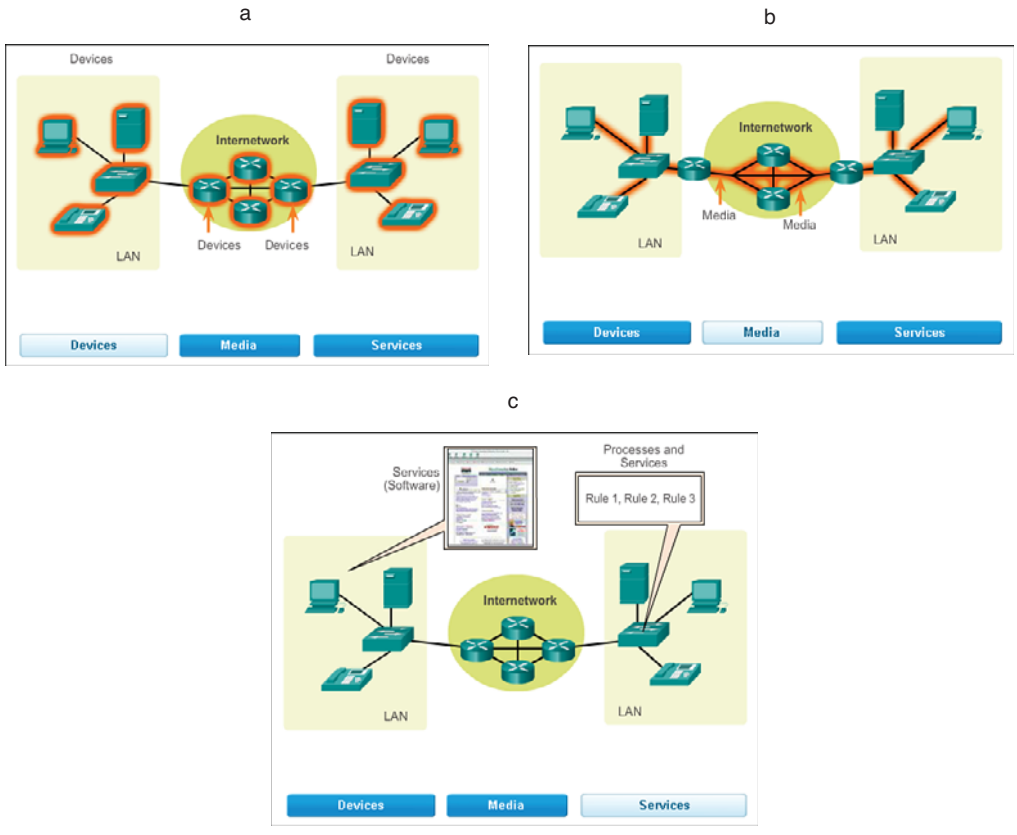


Figure 1-6 Components of the Network Infrastructure

Devices (Figure 1-6a) and media (Figure 1-6b) are the physical elements, or hardware, of the network. Hardware is often the visible components of the network platform such as a laptop, PC, switch, router, wireless access point, or the cabling used to connect the devices. Occasionally, some components might not be so visible. In the case of wireless media, messages are transmitted using invisible radio frequency or infrared waves without requiring any physical connecting media.

Network components are used to provide services and processes (Figure 1-6c). These 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 (1.2.1.2)

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 bar-code scanners)

A host device is either the source or destination of a message transmitted over the network. 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. Data originates with an end device, flows through the network, and arrives at an end device. Messages can take alternate routes through the network between end devices.

Intermediary Network Devices (1.2.1.3)

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.

Examples of intermediary network devices are

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

The management of data as it flows through the network is also a role of the intermediary devices. Intermediary devices direct the path of the data but do not generate or change the data content. 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 what 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 quality of service (QoS) priorities
- Permit or deny the flow of data, based on security settings

Network Media (1.2.1.4)

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 three types of media to interconnect devices and to provide the pathway over which data can be transmitted. As shown in Figure 1-7, these media are

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

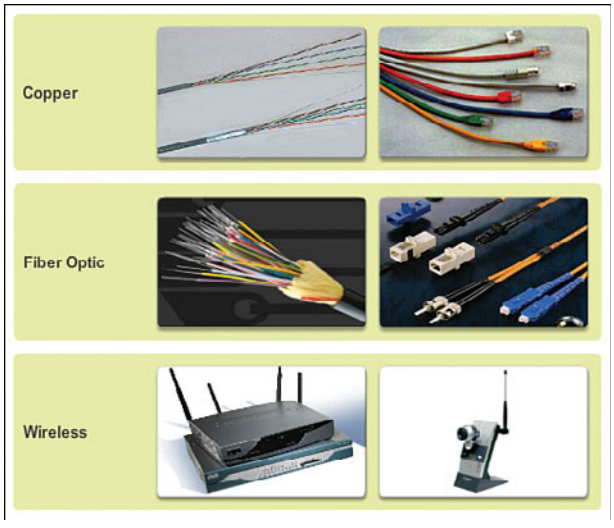


Figure 1-7 Network Media

The signal *encoding* that must occur for the message to be transmitted is different for each medium 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 have the same characteristics and are appropriate for the same purpose. The criteria for choosing network media are

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

Network Representations (1.2.1.5)

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 1-8. 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 labs, you will learn both how these devices operate and how to perform basic configuration tasks on these devices.

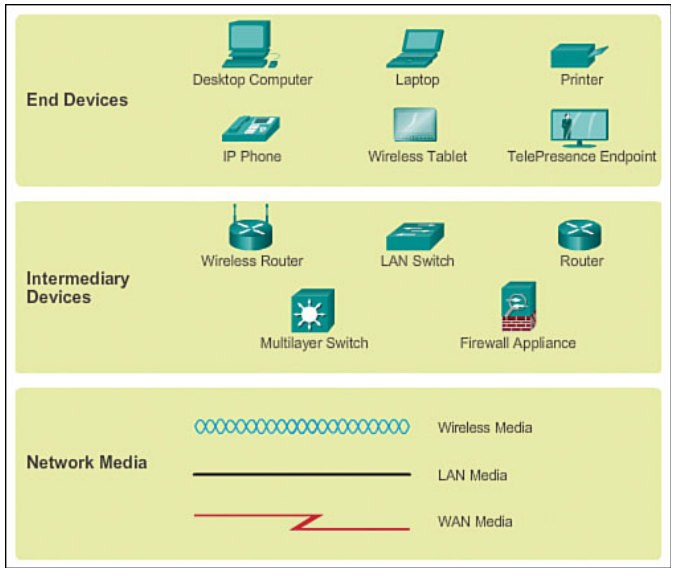


Figure 1-8 Network Symbols

In addition to these representations, specialized terminology is used when discussing how each of these devices and media connect to each other. Important terms to remember are

- **Network interface card (NIC):** A NIC, or LAN adapter, provides the physical connection to the network at the PC or other host device. The medium connecting the PC to the networking device plugs directly into the NIC.
- **Physical port:** A connector or outlet on a networking device where the medium 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*.

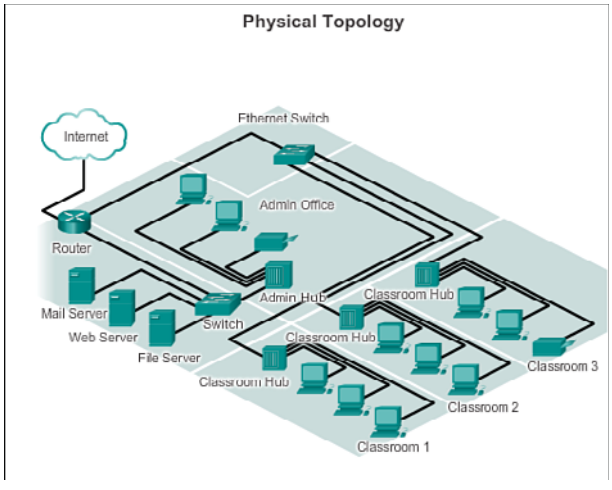
Topology Diagrams (1.2.1.6)

Topology diagrams, as shown in Figure 1-9, are mandatory for anyone working with a network. They provide a visual map of how the network is connected.

There are two types of topology diagrams:

- **Physical topology diagrams (Figure 1-9a):** Identify the physical location of intermediary devices, configured ports, and cable installation.
- **Logical topology diagrams (Figure 1-9b):** Identify devices, ports, and IP addressing scheme.

a



b

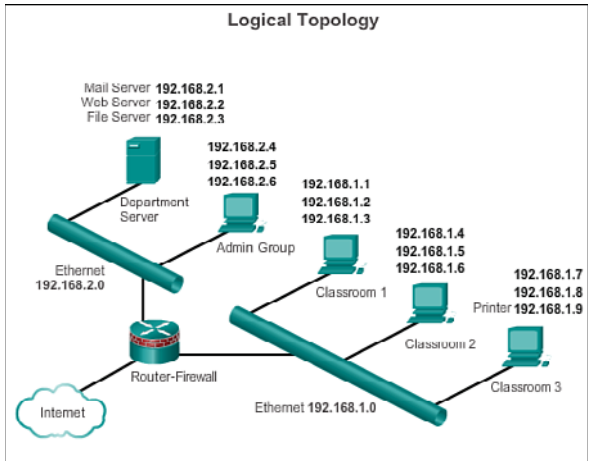


Figure 1-9 Network Topologies

Interactive Graphic

Activity 1.2.1.7: Network Component Representation and Functions

Go to the course online to perform this practice activity.

LANs and WANs (1.2.2)

Network infrastructures can vary greatly in terms of

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

For this reason, networks are often classified into various types based on a number of characteristics.

Types of Networks (1.2.2.1)

Figure 1-10 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.

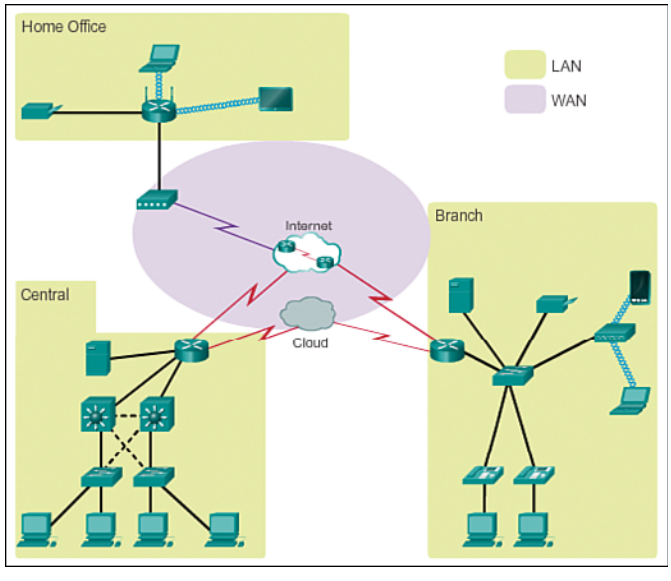


Figure 1-10 LANs and WANs

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 (for example, 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, and Fibre Channel interconnection technology.

Local-Area Networks (1.2.2.2)

Local-area networks (LAN) 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 are enforced on the network level.
- LANs provide high-speed bandwidth to internal end devices and intermediary devices.

Wide-Area Networks (1.2.2.3)

Wide-area networks (WAN) are a network infrastructure that spans a wide geographical area. WANs are typically managed by service providers (SP) or Internet service providers (ISP).

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 (1.2.3, 1.2.3.1)

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 1-11, the Internet is a worldwide collection of interconnected networks (internetworks or 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.

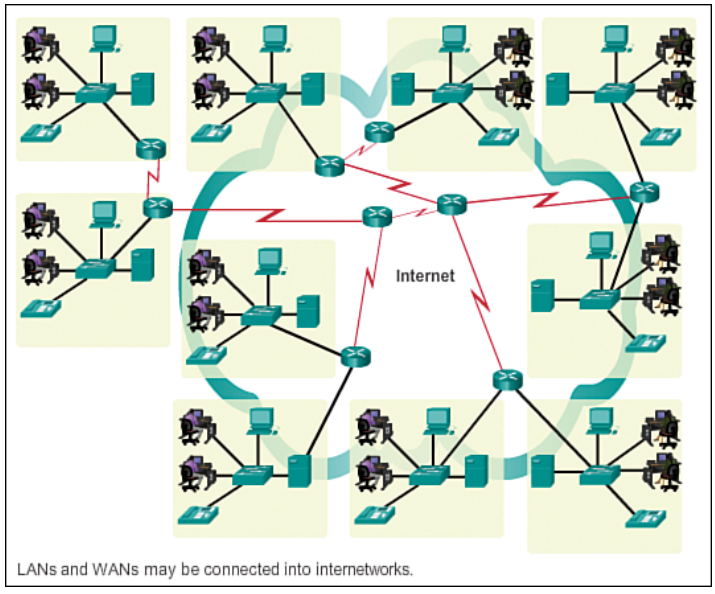


Figure 1-11 Internet

The Internet is a conglomerate of networks and is not 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 the structure and standardization of Internet protocols and processes. These organizations include the Internet Engineering Task Force (IETF), the Internet Corporation for Assigned Names and Numbers (ICANN), and the Internet Architecture Board (IAB), plus many others.

Note

The term *internet* (with a lowercase *i*) is used to describe multiple interconnected networks. When referring to the global system of interconnected computer networks, used by services such as the World Wide Web, the term *Internet* (with a capital *I*) is used.

Intranet and Extranet (1.2.3.2)

There are two other terms that 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 with authorization. Intranets are basically an internet that is usually only accessible from within the organization.

Organizations can publish web pages on an intranet about internal events, health and safety policies, staff newsletters, and staff phone directories. For example, schools can have intranets that include information on class schedules, online curricula, and discussion forums. Intranets usually help eliminate paperwork and speed workflows. The intranet can be accessible to staff working outside of the organization by using secure connections to the internal network.

An organization can use an extranet to provide secure and safe access to individuals who work for a different organization, 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 that they can make appointments for their patients
- A local office of education providing budget and personnel information to the schools in its district. Figure 1-12 shows how intranets, extranets, and the Internet relate.

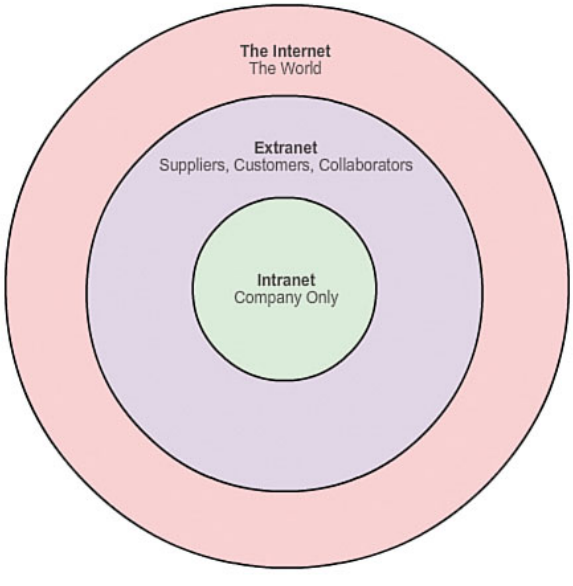


Figure 1-12 Intranets, Extranets, and the Internet

Lab 1.2.3.3: Researching Converged Network Services

Convergence in the context of networking is a term used to describe the process of combining voice, video, and data communications over a common network infrastructure. In this lab, you will survey your understanding of convergence and research ISPs that offer converged services. Based on your understanding of convergence, you will also select the best local ISP that offers converged services and research a local company that uses converged services.

Internet Access Technologies (1.2.4.1)

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 between ISP and 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 (SP). Popular business-class services include business DSL, leased lines, and Metro Ethernet.

Connecting Remote Users to the Internet (1.2.4.2)

Figure 1-13 illustrates some common 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 might

be 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, or for those constantly on the move.
- **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 service might be difficult 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.
- **Dialup 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 dialup modem connection is usually not sufficient for large data transfer, although it is useful for mobile access while traveling. A modem dialup connection should only be considered when higher-speed connection options are not available.

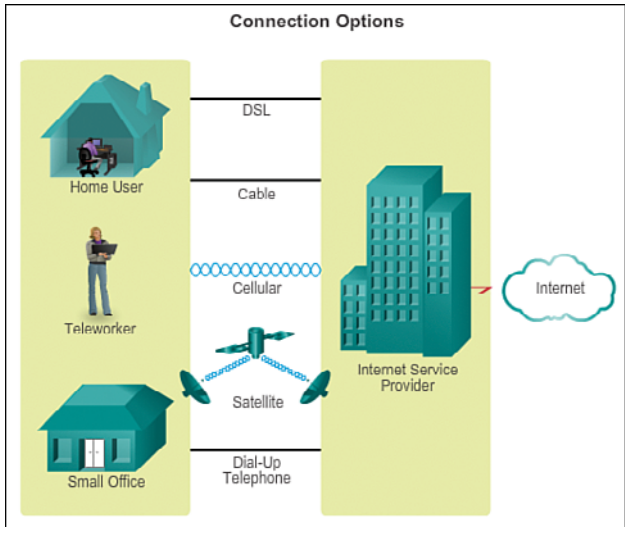


Figure 1-13 Common Internet Connection Options

Many homes and small offices are now being connected directly with fiber-optic cables. This enables an Internet service provider 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 (1.2.4.3)

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

Figure 1-14 illustrates common connection options for organizations, which 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 them expensive. In North America, common leased line circuits include T1 (1.54 Mbps) and T3 (44.7 Mbps), while 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 widely available, and reaches speeds of up to 40 Mbps. However, Ethernet over Copper is limited by distance. Fiber-optic Ethernet service delivers the fastest connections available at an economical megabit-per-second price. Unfortunately, there are still many areas where this service is unavailable.
- **DSL:** Business DSL is available in various formats. A popular choice is symmetric digital subscriber lines (SDSL), which are similar to asymmetric digital subscriber lines (ADSL), but provide 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 might 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 its terrestrial competition, which makes it less attractive than other alternatives.

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

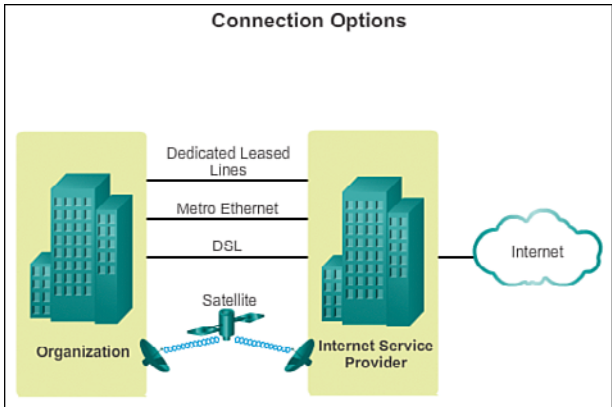


Figure 1-14 Internet Connectivity Options for Businesses

Packet Tracer Activity

Packet Tracer Activity 1.2.4.4: Network Representation

Packet Tracer is a fun, take-home, flexible software program that will help you with your Cisco Certified Network Associate (CCNA) studies. Packet Tracer allows you to experiment with network behavior, build network models, and ask "what if" questions. In this activity, 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. You will also learn how to switch among various modes and workspaces. Finally, you will explore how Packet Tracer serves as a modeling tool for network representations.

The Network as a Platform (1.3)

The network has become a platform for distributing a wide range of services to end users in a reliable, efficient, and secure manner.

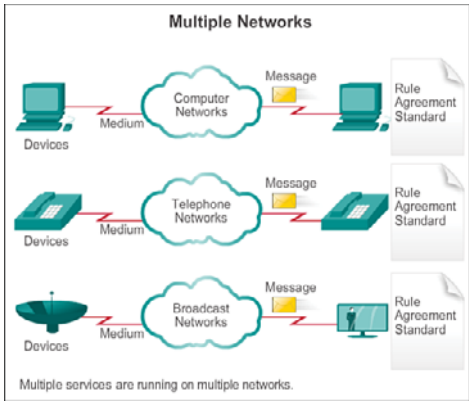
The Converging Network (1.3.1.1)

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, radio, and television networks were maintained separately from data networks. In the past, every one of these services required a dedicated network, with different communication 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 large school in the early 1990s. Back then, classrooms were cabled for the public announcement network, the telephone network, a video network for televisions, a data network, and perhaps a security network. These separate networks were disparate, meaning that they could not communicate with each other, as shown in Figure 1-15a.

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 among many different types of devices over the same communication channel and network structure, as shown in Figure 1-15b. 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.

a



b

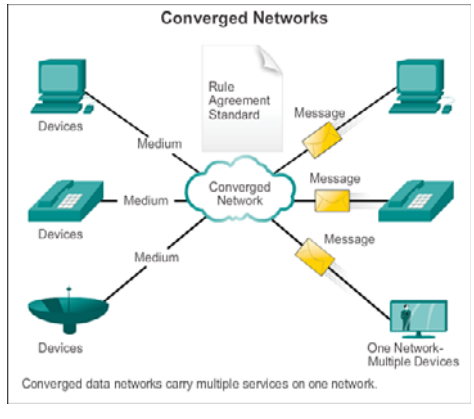


Figure 1-15 Multiple Networks Versus Converged Networks

In 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 (1.3.1.2)

The convergence of the different types of communications networks onto one platform represents the first phase in building the intelligent information network, as shown in Figure 1-16. We are currently in this phase of network evolution. The next phase will be to consolidate not only the different types of messages onto a single network but to also consolidate the applications that generate, transmit, and secure the messages onto integrated network devices.

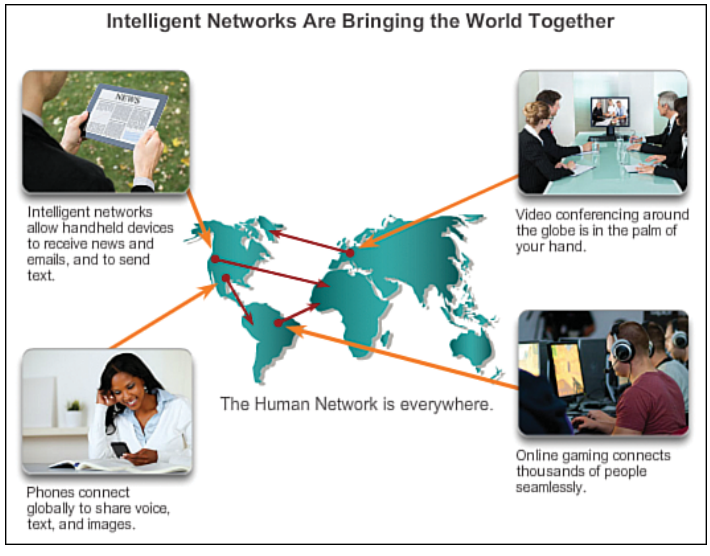


Figure 1-16 Intelligent Information Network

Not only will voice and video be transmitted over the same network, but the devices that perform the telephone switching and video broadcasting will also 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. With only about 10 billion of potentially 1.5 trillion things currently connected globally, there is vast potential to connect the unconnected through the IoE. 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 1.3.1.3: Mapping the Internet

In this lab, you will test network connectivity using ping and Windows tracert. Additionally, you will use web-based and software tools to trace a route to a remote server.

The Supporting Network Architecture (1.3.2.1)

Networks must support a wide range of applications and services, as well as operate over many different types of cables and devices, which 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, as shown in Figure 1-17, that the underlying architectures need to address in order to meet user expectations:

- Fault tolerance (Figure 1-17a)
- Scalability (Figure 1-17b)
- Quality of service (QoS) (Figure 1-17c)
- Security (Figure1-17d)

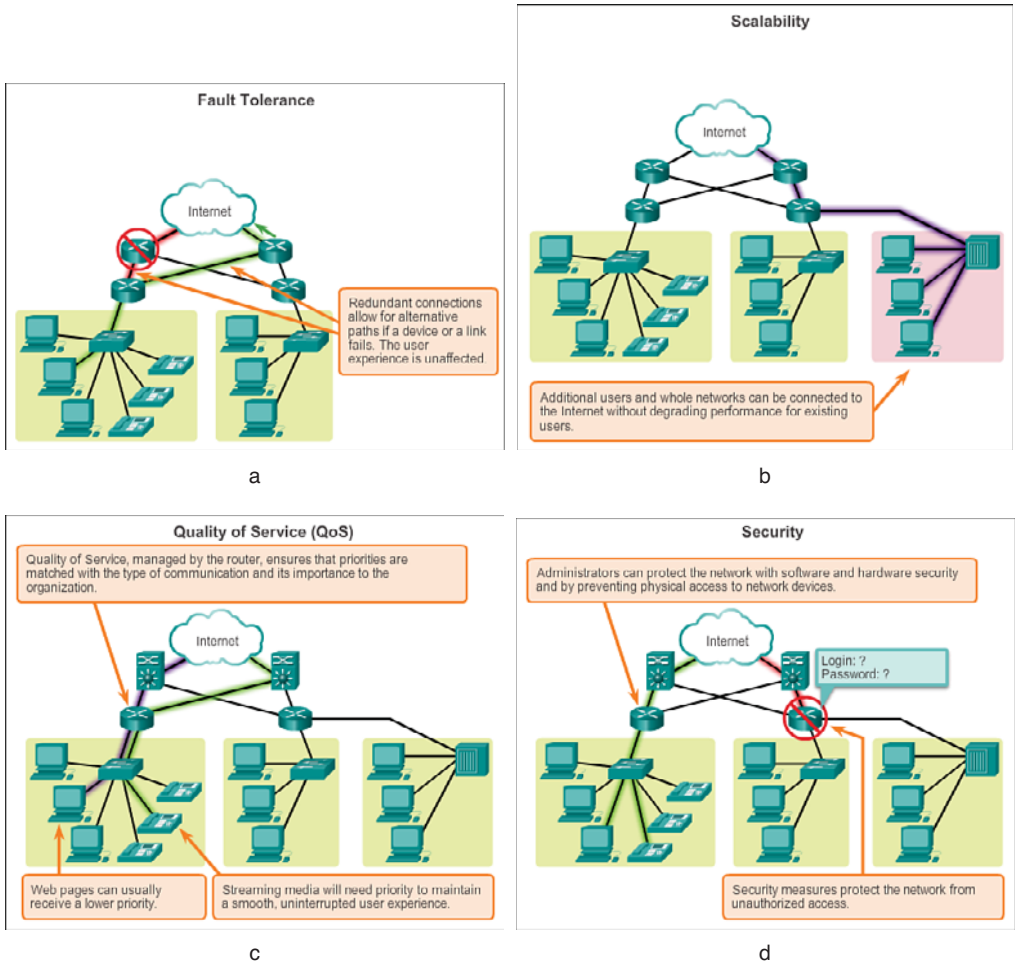


Figure 1-17 Characteristics of a Reliable Network

Fault Tolerance in Circuit-Switched Networks (1.3.2.2)

With our reliance on networks, certain precautions must be taken to ensure that the network functions as designed, even if things go wrong.

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 impact of a failure so that the fewest number of devices are affected by it. It is also built in a way that allows quick recovery when such a failure occurs. These 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*.

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 1-18.

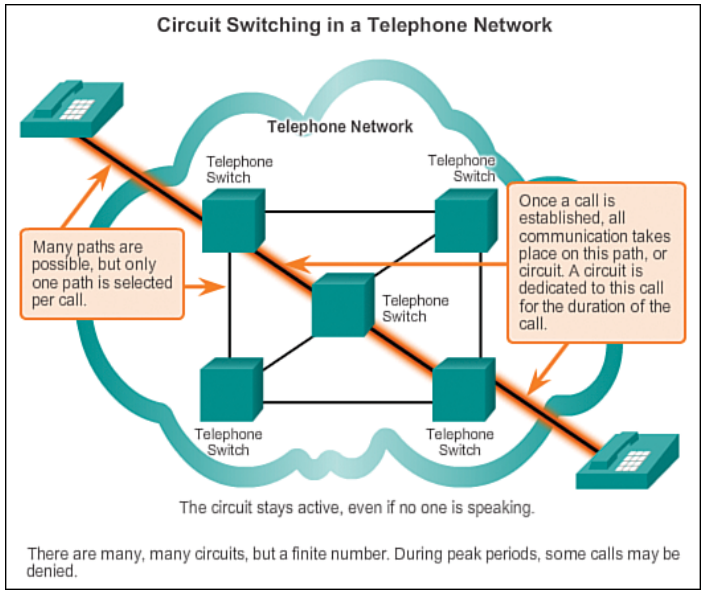


Figure 1-18 Circuit Switching in a Telephone Network

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 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 alternate 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, is why circuit-switched technology was not optimal for the Internet.

Fault Tolerance in Packet-Switched Networks (1.3.2.3)

Because of the technical issues and cost associated with building a fault-tolerant circuit-switched network, network designers turned their attention to packet-switched technologies.

Packet-Switched Networks

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 reaching their destination, as illustrated in Figure 1-19.

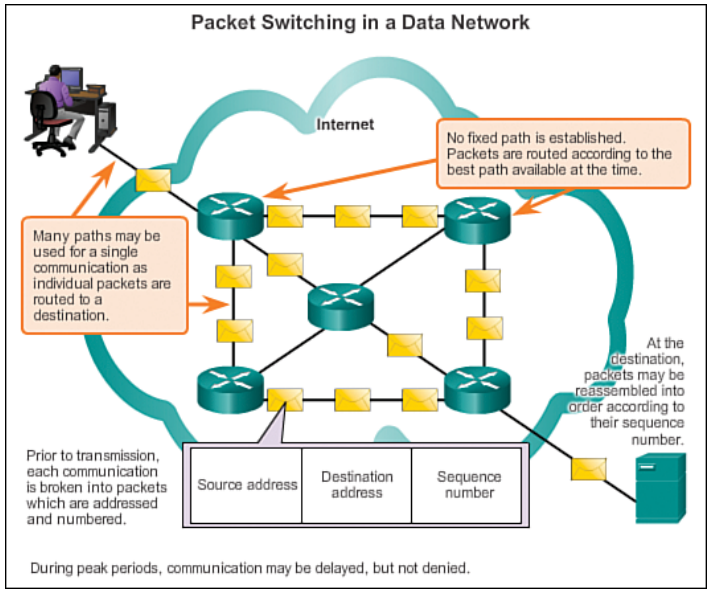


Figure 1-19 Packet Switching in a Data Network

The devices within the network itself are typically unaware of the content of the individual packets. Only visible is the address of the final destination. These addresses are often referred to as *IP addresses*, which can be 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. This would be like writing a long message to a friend using ten postcards. Each postcard has the destination address of the recipient. As the postcards are forwarded through the postal system, the destination address is used to determine the next path that postcard should take. Eventually, they will be delivered to the address on the postcards.

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 might 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. Using our postcard analogy, if one of the postcards is lost along the way, only that postcard needs to be mailed again.

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. In our mail analogy, as our postcard travels through the postal system, it will share transportation with other postcards, letters, and packages. For example, one of the postcards might be placed on an airplane, along with lots of other packages and letters that are being transported toward their final destination.

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 (1.3.2.4)

Not only must a network be fault tolerant, but it must also be able to grow to accommodate new users and services.

Scalability

Thousands of new users and service providers connect to the Internet each week. 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 impacting the performance of the service being delivered to existing users. Figure 1-20 shows the structure of the Internet.

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.

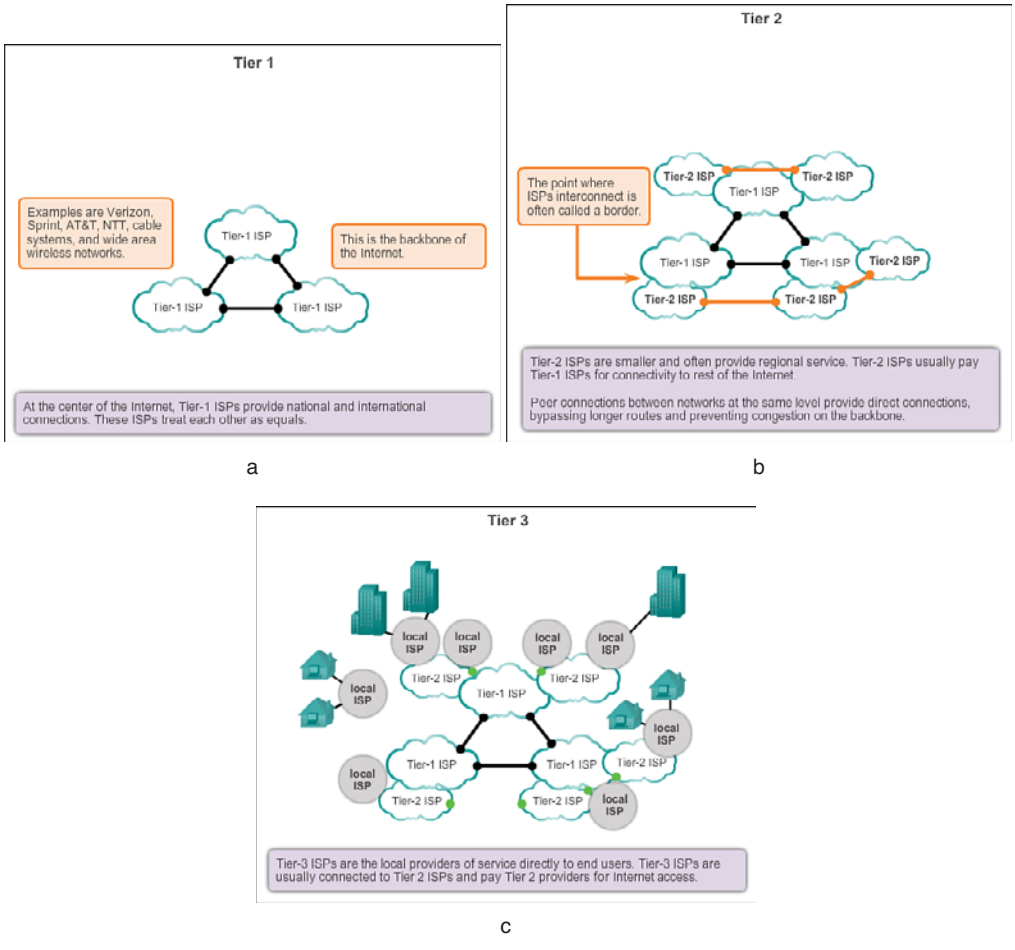


Figure 1-20 Internet as a Scalable Network

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, might 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 (1.3.2.5)

As new Internet applications and services are added, it becomes increasingly apparent that some mechanism is required to handle the different types of traffic encountered in a converged network.

Quality of Service

Quality of service (QoS) is 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 1-21, create higher expectations for the quality of the delivered services. Have you ever tried to watch a video with constant breaks and pauses?

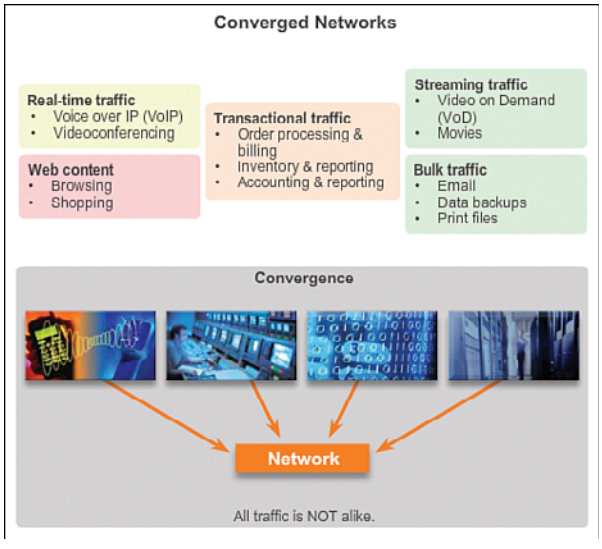


Figure 1-21 Types of Traffic Found in a Converged Network

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 communication 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 1-22. ***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.

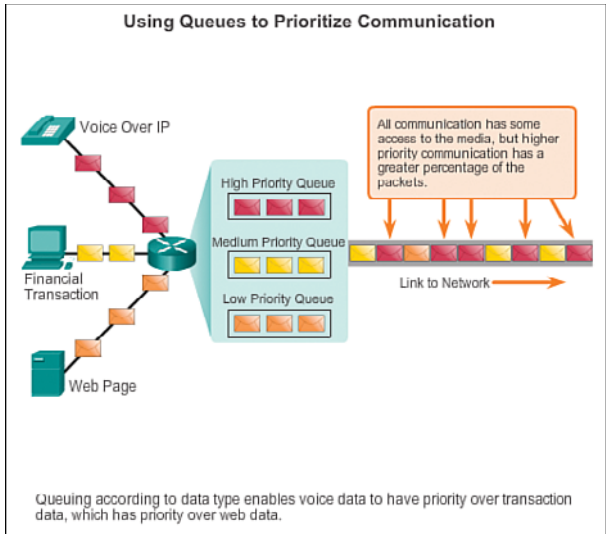


Figure 1-22 Using Queues to Prioritize Communication

Achieving the required QoS by managing the delay and packet loss parameters on a network becomes the secret to a successful end-to-end application quality solution. One way that 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, as shown in Figure 1-23. 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.

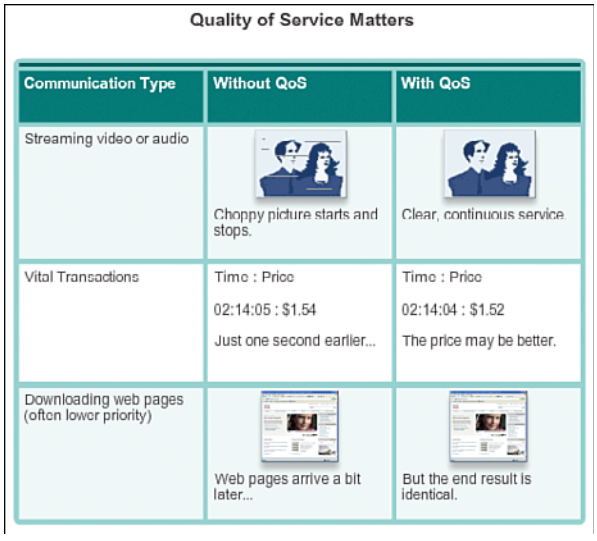


Figure 1-23 Importance of Quality of Service (QoS)

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 (1.3.2.6)

As new users and services are added to the network, it becomes important that measures be taken to ensure that information access is strictly controlled.

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 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 users' consent
- Misdirection and loss of personal or business funds
- Loss of important data that takes 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 the physical securing of devices that provide network connectivity and preventing unauthorized access to the management software that resides on them.

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 unauthorized disclosure
- Prevent theft of information
- Prevent unauthorized modification of information
- Prevent denial of service (DoS)

To achieve the goals of network security, there are three primary requirements, as shown in Figure 1-24:

- **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 the 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 as well as 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.

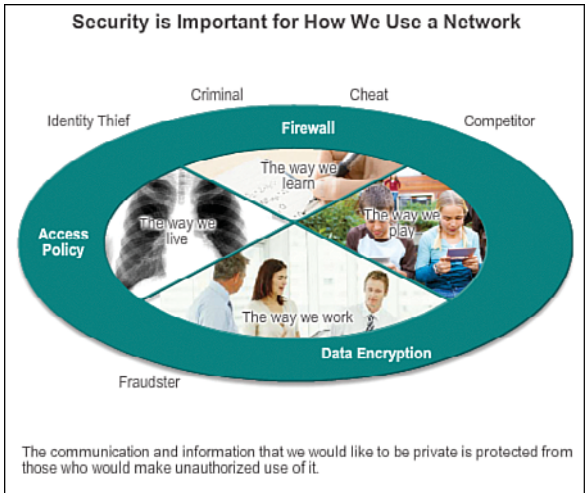


Figure 1-24 Importance of Network Security

Interactive Graphic

Activity 1.3.2.7: Reliable Networks

Go to the course online to perform this practice activity.

The Changing Network Environment (1.4)

The network environment continues to evolve, providing new experiences and opportunities for end users. The network is now capable of delivering services and applications in a manner that was once only dreamed about.

Network Trends (1.4.1)

Just as the way we work, play, and learn impacts the network, the availability of a robust reliable network has an impact on our daily lives.

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.

There are many predictions about the Internet in the near future, including the following:

- By 2014, traffic from wireless devices will exceed traffic from wired devices.
- By 2015, the amount of content traversing the Internet annually will be 540,000 times time the amount that traveled in 2003.
- By 2015, 90 percent of all content on the Internet will be video based.
- By 2015, a million video minutes will traverse the Internet every second.
- By 2016, the annual global IP traffic will surpass the zetabyte threshold (1,180,591,620,717,411,303,424 bytes).
- By 2016, the number of devices connected to IP networks will be nearly three times as high as the global population.
- By 2016, 1.2 million minutes of video content will cross the network every second.
- By 2020, 50 billion devices will be connected to the Internet.

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 effect organizations and consumers. Some of the top trends include

- Any device, to any content, in any way
- Online collaboration
- Video
- Cloud computing

These trends are interconnected and will continue to build on 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?

Video

Video 1.4.1.1: Click the second graphic in the online course to view a video that outlines some Cisco thoughts on future developments of the Internet.

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 that requires significant changes to the way devices are used. This trend is known as *Bring Your Own Device (BYOD)*.

BYOD is about end users having the freedom to use personal tools to access information and communicate across a business or campus network. With the growth of consumer devices, and the related drop in cost, employees and students can be expected to have some of the most advanced computing and networking tools for personal use. These personal tools include laptops, netbooks, tablets, smartphones, and e-readers. These can be devices purchased by the company or school, purchased by the individual, or both.

BYOD means any device, with any ownership, used anywhere. For example, in the past, a student who needed to access the campus network or the Internet had to use one of the school's computers. These devices were typically limited and seen as tools only for work done in the classroom or in the library. Extended connectivity through mobile and remote access to the campus network gives students tremendous flexibility and more learning opportunities for the student.

BYOD is an influential trend that has or will touch every IT organization.

Online Collaboration (1.4.1.3)

Individuals 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 a clear picture of the project?
- 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?

Collaboration is also a priority in education. Students need to collaborate with assist each other in learning, to develop team skills used in the workforce, and to work together on team-based projects.

One way to answer these questions and meet these demands in today's environment is through online collaboration tools. In traditional workspaces, and with BYOD environments alike, individuals 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. Individuals 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, students, teachers, customers, and partners a way to instantly connect, interact, and conduct business, through whatever communications channels they prefer, and achieve their objectives.

Video Communication (1.4.1.4)

Another trend in networking that is critical in the communication and collaboration effort is video. Video is being used for communications, collaboration, and entertainment. Video calls are becoming more popular, facilitating communications as part of the human network. Video calls can be made to and from anywhere with an Internet connection, including from home or at work.

Video calls and videoconferencing are proving particularly powerful for sales processes and for doing business. Video is a useful tool for conducting business at a distance, both locally and globally. Today, businesses are using video to transform the way they do business. Video helps businesses create a competitive advantage, lower costs, and reduce the impact on the environment by reducing the need to travel. Figure 1-25 shows the trend of video in communication.

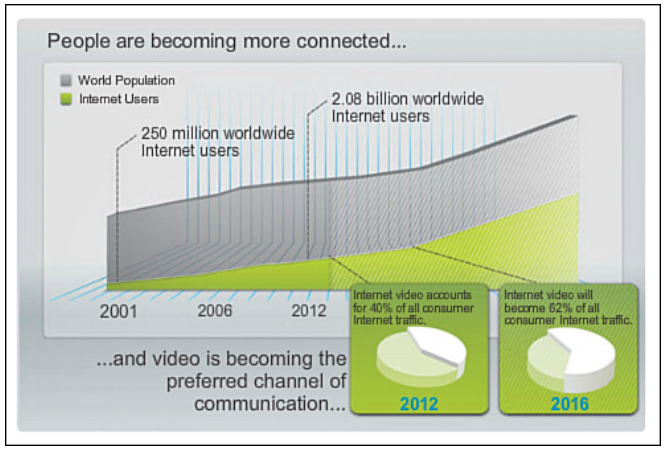


Figure 1-25 Trend of Video in Communication

Both consumers and businesses are driving this change. Video is becoming a key requirement for effective collaboration as organizations extend across geographic 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 audioconference will coexist with the videoconference. 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, might focus on globalization and fast-changing consumer tastes, while the chief information officer's (CIO) focus might be on cost savings by reducing travel costs of employees needing to meet face to face.

Some of the drivers for organizations to develop and implement a video solution strategy include

- **A global workforce and need for real-time collaboration:** Create collaborative teams that span corporate and national boundaries and geographies.
- **Reducing costs and green IT:** Avoiding travel reduces both cost and carbon emissions.
- **New opportunities for IP convergence:** These include converging video applications, such as high-definition video collaboration, video surveillance systems, and video advertising signage onto a single IP network.

- **Media explosion:** The plummeting cost of video cameras and a new generation of high-quality, low-cost devices have turned users into would-be movie producers.
- **Social networking:** The social networking phenomenon can be as effective in business as it is in a social setting. For example, employees are increasingly filming short videos to share best practices with colleagues and to brief peers about projects and initiatives.
- **Demands for universal media access:** Users are demanding to be able to access rich-media applications wherever they are and on any device. Participation in videoconferencing, viewing the latest executive communications, and collaborating with coworkers are applications that will need to be accessible to employees, regardless of their work location.

Video

Video 1.4.1.4: Click the third graphic in the online course for a closer look at how TelePresence using video can be incorporated into everyday life and business.

Another trend in video is video on demand and streaming live video. Delivering video over the network lets us see movies and television programs when we want and where we want.

Cloud Computing (1.4.1.5)

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 a service fee is charged.

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 can be a web browser, and the cloud's network takes care of the rest.

Cloud computing is another global trend that is changing the way we access and store data. Cloud computing encompasses any subscription-based or pay-per-use service, in real time over the Internet. Cloud computing allows us to store personal files and even back up our entire hard drive on servers over the Internet. Applications such as word processing and photo editing can be accessed using the cloud.

For businesses, cloud computing extends IT's capabilities 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.

The term *cloud computing* really refers to web-based computing. Online banking, online retail stores, and online music downloading are all examples of cloud computing. Cloud applications are usually delivered to the user through a web browser. Users do not need to have any software installed on their end device. This allows many different kinds of devices to connect to the cloud.

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:** The 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.

There are four primary types of clouds: private, public, hybrid, and custom. A private cloud offers applications and services intended only 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.

Cloud-based services offered in a public cloud are made available to the general population. Services can be free or are offered on a pay-per-use model, such as paying for online storage. The public cloud uses the Internet to provide services.

Hybrid clouds are made up of two or more clouds (for example part custom and part public), where each part remains a distinctive object, but both 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.

Custom clouds are built to meet the needs of a specific industry, such as healthcare or media. Custom clouds can be private or public.

Data Centers (1.4.1.6)

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 (for example, air conditioning and 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. While 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 might own a separate data center where patient records are maintained electronically. Smaller organizations, which 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.

Video

Video 1.4.1.6: View the video in the online course to learn about the growing use of cloud computing and data center services.

Technology Trends in the Home (1.4.2.1)

Networking trends are not only affecting the way we communicate at work and at school, but they are also changing just about every aspect of the home.

The newest home trends include “smart home technology.” This is technology that is integrated into everyday appliances, allowing them to interconnect with other devices, making them more “smart” or automated. For example, imagine being able to prepare a dish and place it in the oven for cooking prior to leaving the house for the day. Imagine that the oven was “aware” of the dish it was cooking and was connected to your calendar of events so that it could determine what time you should be available to eat, and adjust start times and length of cooking accordingly.

It could even adjust cooking times and temperatures based on changes in schedule. Additionally, a smartphone or tablet connection gives the user the ability to connect to the oven directly, to make any desired adjustments. When the dish is "available," the oven sends an alert message to a specified end-user device that the dish is done and warming.

This scenario is not far off. In fact, smart home technology is currently being developed for all rooms within a house. Smart home technology will become more of a reality as home networking and high-speed Internet technology becomes more widespread in homes. New home networking technologies are being developed daily to meet these types of growing technology needs.

Powerline Networking (1.4.2.2)

Powerline networking is an emerging trend for home networking that uses existing electrical wiring to connect devices, as shown in Figure 1-26. The concept of "no new wires" means the ability to connect a device to the network wherever there is an electrical outlet. This saves the cost of installing data cables and adds no cost to the electrical bill. Using the same wiring that delivers electricity, powerline networking sends information by sending data on certain frequencies similar to the technology used for DSL.

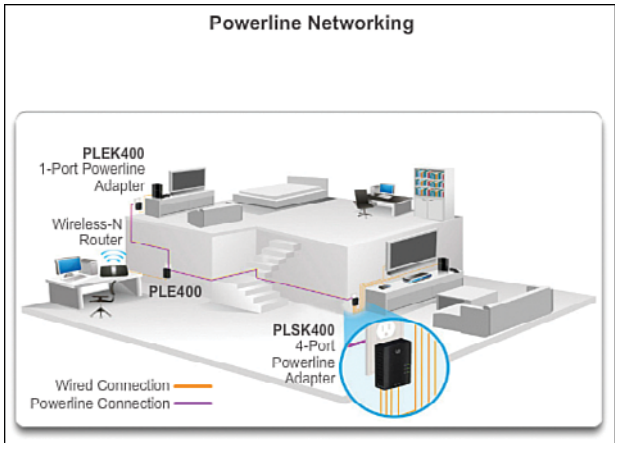


Figure 1-26 Powerline Networking

Using a HomePlug standard powerline adapter, devices can connect to the LAN wherever there is an electrical outlet. Powerline networking is especially useful when wireless access points cannot be used or cannot reach all the devices in the home. Powerline networking is not designed to be a substitute for dedicated cabling for data networks. However, it is an alternative when data network cables or wireless communications are not a viable option.

Wireless Broadband (1.4.2.3)

Connecting to the Internet is vital in smart home technology. DSL and cable are common technologies used to connect homes and small businesses to the Internet. However, wireless can be another option in many areas.

Wireless Internet Service Provider (WISP)

A wireless Internet service provider (WISP) is an ISP that connects subscribers to a designated access point or hot spot using similar wireless technologies found in home wireless local-area networks (WLAN). WISPs are more commonly found in rural environments where DSL or cable services are not available.

Although a separate transmission tower might be installed for the antenna, it is common that the antenna is attached to an existing elevated structure such as a water tower or a radio tower. A small dish or antenna is installed on the subscriber's roof in range of the WISP transmitter. The subscriber's access unit is connected to the wired network inside the home. From the perspective of the home user, the setup isn't much different than DSL or cable service. The main difference is that the connection from the home to the ISP is wireless instead of using a physical cable.

Wireless Broadband Service

Another wireless solution for the home and small businesses is wireless broadband. This uses the same cellular technology used to access the Internet with a smartphone or tablet. An antenna is installed outside the house, providing either wireless or wired connectivity for devices in the home. In many areas, home wireless broadband is competing directly with DSL and cable services.

Security Threats (1.4.3.1)

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 as large as a corporation with thousands of users. The network security implemented must take into account the environment, as well as the tools and requirements of the network. It must be able to secure data while still providing the quality of service that is expected of the network.

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 attacks, also called zero-hour attacks:** An attack that occurs on the first day that a vulnerability becomes known
- **Hacker attacks:** An attack by a knowledgeable person to user devices or network resources
- **Denial of service attacks:** Attacks 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 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 internal users of the network. This can be attributed to lost or stolen devices, accidental misuse by employees, and in the business environment, even malicious employees. 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.

Security Solutions (1.4.3.2)

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.

A home network security implementation is usually rather basic. It is generally implemented on the connecting host devices, as well as at the point of connection to the Internet, and can even rely on contracted services from the ISP.

In contrast, 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:

- **Antivirus and antispyware:** To protect user devices from malicious software.

- **Firewall filtering:** To block unauthorized access to the network. This can 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.

In addition to the these items, larger networks and corporate networks often have other security requirements:

- **Dedicated firewall systems:** 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 systems (IPS):** To identify fast-spreading threats, such as zero-day or zero-hour attacks
- **Virtual Private Networks (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 computing requirements. Both home environments and businesses must be able to secure their data while still providing 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 1.4.3.3: Network Security Terminology

Go to the course online to perform this practice activity.

Cisco Network Architectures (1.4.4.1)

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. For networks to function efficiently and grow in this type of environment, the network must be built upon a standard network 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 ensure the connection of any device across any combination of networks. While ensuring connectivity, it also increases cost

efficiency by integrating network security and management, and improves business processes. At the foundation of all network architectures, and in fact, at the foundation of the Internet itself, are routers and switches. Routers and switches transport data, voice, and video communications, as well as allow wireless access and provide security.

Building networks that support our needs of today and the needs and trends of the future starts with a clear understanding of the underlying switching and routing infrastructure. After a basic routing and switching network infrastructure is built, individuals, small businesses, and organizations can grow their network over time, adding features and functionality in an integrated solution.

CCNA (1.4.4.2)

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 route and switched networks, including implementation and verification of connections to remote sites in a WAN. The CCNA curriculum also includes basic mitigation of security threats, introduction to wireless networking concepts and terminology, and performance-based skills. This CCNA curriculum includes the use of various protocols, such as IP, Open Shortest Path First (OSPF), Serial Line Interface Protocol, Frame Relay, VLANs, Ethernet, access control lists (ACL), 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 1.4.4.3: Researching IT and Networking Job Opportunities

In this lab, you will research the current networking jobs and hiring trends in IT/networking. You will also examine the value of career certifications, especially those offered by Cisco Systems.

Summary (1.5)

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. You can also refer to the other activities completed in this chapter, including Packet Tracer activities.

Draw a map of the Internet as you see it now. Use the icons presented in the chapter for media, end devices, and intermediary devices.

In your revised drawing, you might want to include some of the following:

- WANs
- LANs
- Cloud computing
- Internet service providers (tiers)

Save your drawing in hard-copy format. If it is an electronic document, save it to a server location provided by your instructor. Be prepared to share and explain your revised work in class.

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, work, and interests.

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 that the network must be fault tolerant, be 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 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 Internet Operating System (IOS), which is 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 *The Introduction to Networking Lab Manual* (ISBN 978-1-58713-312-1). 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 1.1.1.8: Researching Collaboration Tools
- Lab 1.2.3.3: Researching Converged Network Services
- Lab 1.3.1.3: Mapping the Internet
- Lab 1.4.4.3: Researching IT Networking Jobs and Hiring Trends in IT/Networking

Packet Tracer Activities

- Packet Tracer Activity 1.2.4.4: 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. What is a group of web pages that groups of individuals can edit and view together called?

   A. Podcasting
   B. Wiki
   C. Weblog (blog)
   D. Instant messaging

2. Which of the following are disadvantages of peer-to-peer networking? (Choose two.)

   A. Expensive to set up and maintain
   B. No centralized administration
   C. Complex configuration
   D. Scalability

3. Which devices would be considered end devices on a network? (Choose four.)

   A. Switch
   B. Printer
   C. IP phone
   D. Server
   E. Tablet computer
   F. Wireless access point

4. What type of information would be found on a logical topology diagram?

   A. Location of departmental printer
   B. Length and type of all cable runs
   C. IP addressing scheme
   D. Location of departmental switch

5. What is a network infrastructure that provides access to other networks over a wide geographic area?

   A. LAN
   B. WLAN
   C. MAN
   D. WAN
   E. SAN

6. Which of the following are business-class Internet connection technologies normally supplied by a service provider? (Choose two.)

   A. Leased lines
   B. Broadband cable
   C. Metro Ethernet
   D. Mobile services
   E. Cellular

7. Which technology would be best to provide a home user with a high-speed, always-on Internet connection?

   A. Dialup
   B. DSL
   C. Satellite
   D. Cellular

8. What is a converged network?

   A. A network that makes use of both fiber-optic and copper connections
   B. A network where voice, video, and data move over the same infrastructure
   C. A network that makes use of both wired and wireless technology
   D. A network that makes use of both satellite and terrestrial connections to move data

9. What is a fault-tolerant network?

   A. A network that can provide priority treatment of voice and video traffic
   B. A network that offers secure transactions
   C. A network that can reroute traffic in case of device failure
   D. A network that is incapable of failing

10. What is true of Tier 3 ISPs?

A. They act as local providers of service directly to end users.
B. They connect directly to Tier 1 ISPs.
C. They interconnect with other Tier 1 ISPs.
D. They provide high-speed redundant services to other ISPs.

11. Which type of traffic must receive the highest priority from QoS?

A. Web traffic
B. Email
C. VoIP
D. Order processing

12. What are the primary requirements of information security? (Choose three.)

A. Confidentiality
B. Integrity
C. Availability
D. QoS
E. Scalability

13. List four current network trends.

14. Describe some common everyday uses of a modern-day network.

15. In what ways has the network transformed the way we learn?

Index

Symbols

NUMERICS

A

B

C

D

E

F

G

H

I

J-K

L

M

N

O

P

Q-R

S

T

U

V

W

X-Z