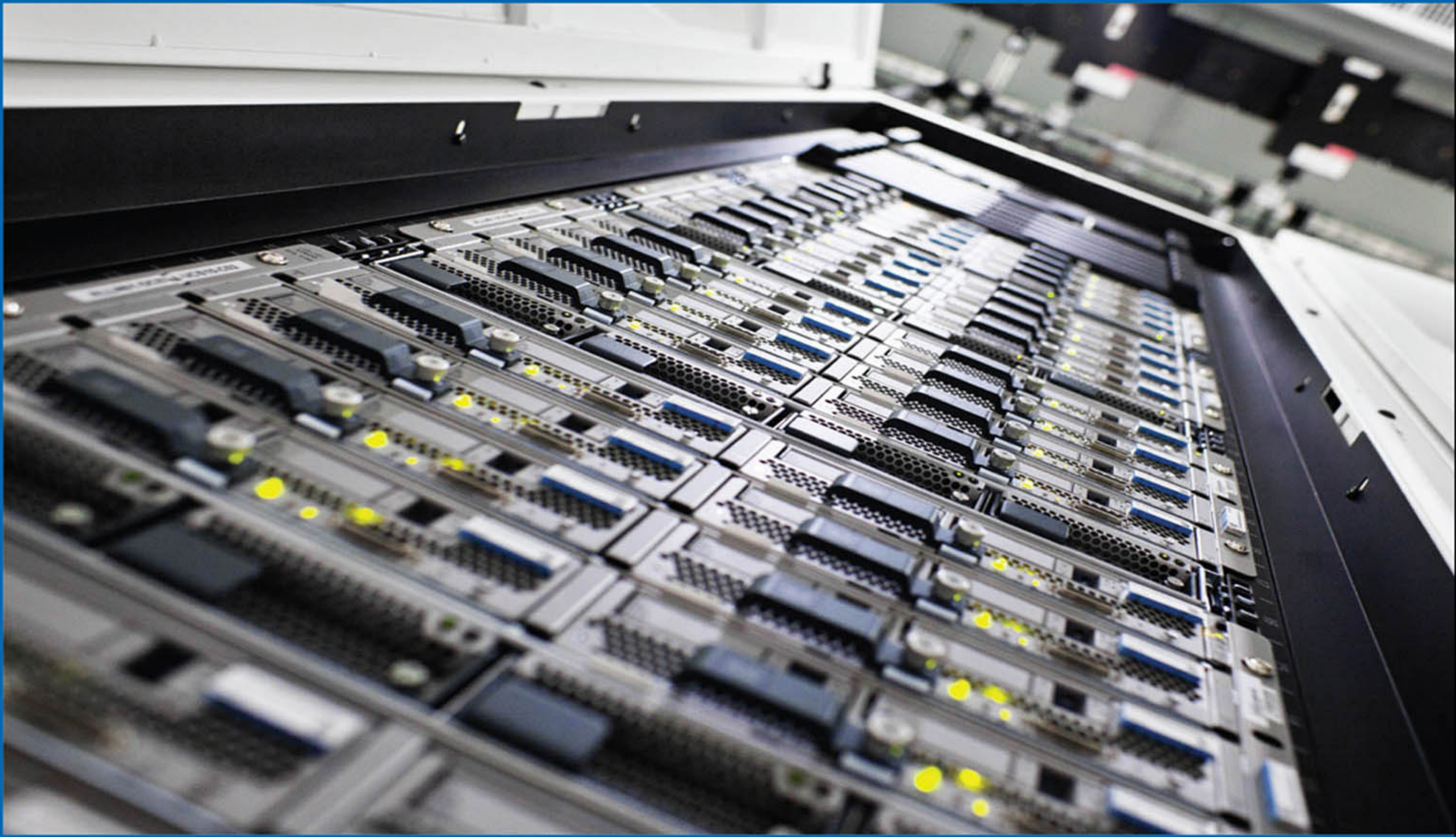
Introduction to Networks v6

Companion Guide



Cisco | Networking Academy®
Mind Wide Open™

Introduction to Networks v6

Companion Guide

Cisco Networking Academy

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

Introduction to Networks v6 Companion Guide

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 2016

Library of Congress Control Number: 2016946762

ISBN-13: 978-1-58713-360-2

ISBN-10: 1-58713-360-1

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.

Editor-in-Chief
Mark Taub

Product Line Manager
Brett Bartow

Business Operation Manager, Cisco Press
Ronald Fligge

Executive Editor
Mary Beth Ray

Managing Editor
Sandra Schroeder

Development Editor
Ellie C. Bru

Project Editor
Mandie Frank

Copy Editor
Celia McCoy

Technical Editor
Bob Vachon

Editorial Assistant
Vanessa Evans

Designer
Chuti Prasertsith

Composition
codeMantra

Indexer
Cheryl Lenser

Proofreader
Jaikumar

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.

Special Sales

For government sales inquiries, please contact governmentsales@pearsoned.com.

For questions about sales outside the U.S., please contact intlcs@pearson.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.

About the Contributing Authors

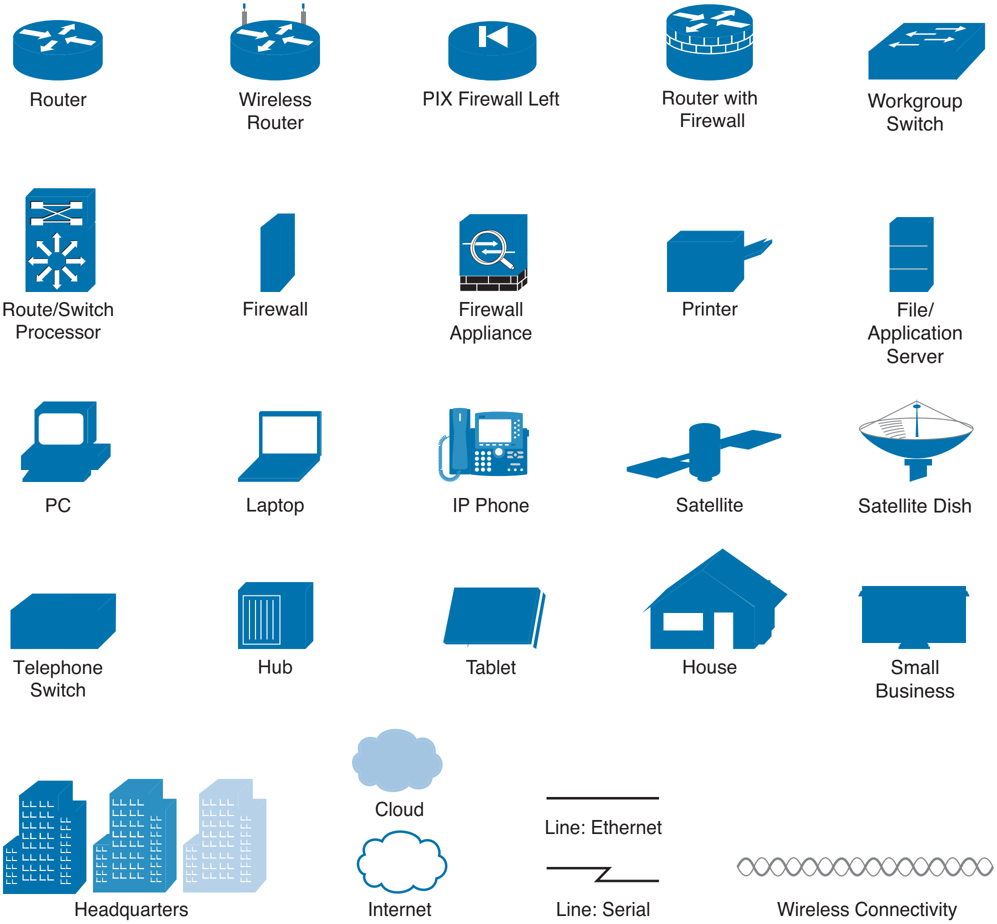
Rick Graziani teaches computer science and computer networking courses at Cabrillo College in Aptos, California. Prior to teaching Rick worked in the information technology field for Santa Cruz Operation, Tandem Computers, Lockheed Missiles and Space Corporation, and served in the U.S. Coast Guard. He holds an M.A. in Computer Science and Systems Theory from California State University Monterey Bay. Rick also works as a curriculum developer for the Cisco Networking Academy Curriculum Engineering team. When Rick is not working, he is most likely surfing at one of his favorite Santa Cruz surf breaks.

Allan Johnson entered the academic world in 1999 after 10 years as a business owner/operator to dedicate his efforts to his passion for teaching. He holds both an MBA and an M.Ed. in Occupational Training and Development. He taught CCNA courses at the high school level for seven years and has taught both CCNA and CCNP courses at Del Mar College in Corpus Christi, Texas. In 2003, Allan began to commit much of his time and energy to the CCNA Instructional Support Team, providing services to Networking Academy instructors worldwide and creating training materials. He now works full time for Cisco Networking Academy as a Curriculum Developer.

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

Introduction

Introduction to Networks: Companion Guide v6 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

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 Networking 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 question format in the Companion Guide encourages you to think about finding the answers as you read the chapter.

How To

- **"How-to" feature:** When this book covers a set of steps that you need to perform for certain tasks, the text lists the steps as a how-to list. When you are studying, the icon helps you easily refer to this feature as you skim through the book.
- **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 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 253 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

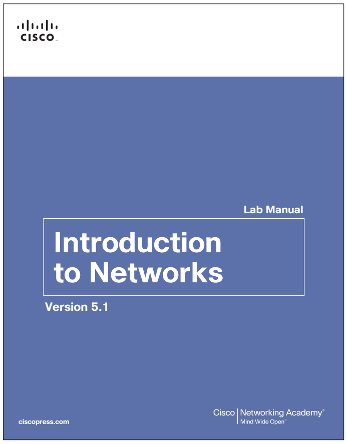
Video

- **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 Networking v6 Labs & Study Guide* [ISBN 978-1-58713-361-9]. 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.

Labs & Study Guide

The supplementary book *Introduction to Networking v6 Labs & Study Guide*, by Cisco Press (ISBN 978-1-58713-361-9), contains all the labs plus Packet Tracer activities from the course, a command reference, and additional study guide exercises and activities.



About Packet Tracer Software and Activities

Packet Tracer
□ Activity

Interspersed throughout the chapters you'll find many activities to work with the Cisco Packet Tracer tool. Packet Tracer 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 through the Cisco Networking Academy website. Ask your instructor for access to Packet Tracer.

Companion Website

Register this book to get information about Packet Tracer and access to other study materials plus additional bonus content to help you succeed with this course and the certification exam. Check this site regularly for any updates or errata that might become available for this book. Be sure to check the box that you would like to hear from us to receive news of updates and exclusive discounts on related products.

To access this companion website, follow the steps below:

1. Go to www.ciscopress.com/register and log in or create a new account.
2. Enter the ISBN: 9781587133602.

3. Answer the challenge question as proof of purchase.
4. Click the “Access Bonus Content” link in the Registered Products section of your account page, to be taken to the page where your downloadable content is available.

Please note that many of our companion content files can be very large, especially image and video files. If you are unable to locate the files for this title by following the steps, please visit www.ciscopress.com/contact and select the “Site Problems/Comments” option. Our customer service representatives will assist you.

How This Book Is Organized

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

- **Chapter 1, “Explore 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, “Configure 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, "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 8, "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 9, "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 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, "Build a Small 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

Explore 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?
- What ways can host devices be used as clients, servers, or both?
- How are network devices used?
- What are the differences between LAN and WAN devices?
- What are the differences between LAN and WAN topologies?
- What is the basic structure of the Internet?
- How do LANs and WANs interconnect to the Internet?
- What is a converged network?
- What are the four basic requirements of a converged network?
- How do trends such as BYOD, online collaboration, video, and cloud computing change the way we interact?
- How are networking technologies changing the home environment?
- What are some basic security threats and solutions for both small and large networks?
- Why is it important to understand the switching and routing infrastructure of a network?

Key Terms

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

Peer-to-Peer (P2P) file sharing   *Page 6*

Small Office/Home Office (SOHO) network   *Page 8*

Medium to large network   *Page 8*

Server   *Page 9*

Client   *Page 9*

End device   *Page 14*

Medium   *Page 8*

Network Interface Card (NIC)   *Page 18*

Physical port   *Page 18*

Interface   *Page 18*

Physical topology diagram   *Page 19*

Logical topology diagram   *Page 19*

Local area network (LAN)   *Page 20*

Wide area network (WAN)   *Page 20*

Internet   *Page 23*

Intranet   *Page 25*

Extranet   *Page 25*

Internet Service Provider (ISP)   *Page 26*

Converged network   *Page 29*

Network architecture *Page 31*

Scalable network *Page 32*

Quality of Service (QoS) *Page 32*

Bring Your Own Device (BYOD) *Page 35*

Collaboration *Page 36*

Cloud computing *Page 37*

Private cloud *Page 38*

Public cloud *Page 38*

Hybrid cloud *Page 38*

Custom cloud *Page 38*

Data center *Page 39*

Smart home technology *Page 40*

Powerline networking *Page 40*

Wireless Internet Service Provider (WISP) *Page 41*

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.

Class Activity 1.0.1.2: Draw Your Concept of the Internet

Refer to Lab Activity for this chapter

Welcome to a new component of our Networking Academy curriculum: 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!

Here is your first modeling activity:

Draw Your Concept of the Internet

Draw and label a map of the Internet as you interpret it now. Include your home or school/university location and its respective cabling, equipment, devices, etc. Some items you may wish to include

- Devices/Equipment
- Media (cabling)
- Link Addresses or Names
- Sources and Destinations
- Internet Service Providers

Upon completion, 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.

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

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.

Play the video to view how connected we are.

Video

Go to the online course to view this video.

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 button. 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.

Play the video to watch how the Internet emerged over the last 25 years and see a glimpse into the future! What else do you think we will be able to do using the network as the platform?

Video

Go to the online course to view this video.

No Boundaries (1.1.1.3)

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

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

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

How has the human network affected you?

Networks Support the Way We Learn (1.1.1.4)

Networks have changed 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. 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.

Play the video to see how the classroom is expanding.

Video

Go to the online course to view this video.

Networks Support the Way We Communicate (1.1.1.5)

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

- **Texting –** Texting enables instant real-time communication between two or more people.

- **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 –** Without the constraints of location or time zone, collaboration tools allow individuals to communicate with each other, often across real-time interactive video. The broad distribution of data networks means that people in remote locations can contribute on an equal basis with people in the heart of large population centers.
- **Blogs –** Blogs, which is an abbreviation of the word "weblogs," are web pages that are easy to update and edit. Unlike commercial websites, blogs give anyone a means to communicate their thoughts to a global audience without technical knowledge of web design.
- **Wikis –** Wikis are web pages that groups of people can edit and view together. Whereas a blog is more of an individual, personal journal, a wiki is a group creation. As such, it may be subject to more extensive review and editing. Many businesses use wikis as their internal collaboration tool.
- **Podcasting –** Podcasting allows people to deliver their audio 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. 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)

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

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

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

Networks Support the Way We Play (1.1.1.7)

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 as if we were all 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.

Whatever form of recreation we enjoy, networks are improving our experience.

How do you play on the Internet?

Lab 1.1.1.8: Researching Network Collaboration Tools

In this lab, you will complete the following objectives:

- Part 1: Use Collaboration Tools
- Part 2: Share Documents with Google Drive
- Part 3: Explore Conferencing and Web Meetings
- Part 4: Create Wiki Pages

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. They can range from simple networks consisting of two computers to networks connecting millions of devices. Figure 1-1 shows four classifications of networks based on size:

Small Home Networks

Small Office/Home Office Networks

Medium to Large Networks

World Wide Networks

Figure 1-1 Network Sizes

- Small home networks connect a few computers to each other and the Internet.
- The *Small Office/Home Office or SOHO network* enables computers within a home office or a remote office to connect to a corporate network or access centralized, shared resources.
- *Medium to large networks*, such as those used by corporations and schools, can have many locations with hundreds or thousands of interconnected computers.
- The Internet is a network of networks that connects hundreds of millions of computers world-wide.

Simple networks installed in homes enable sharing of resources, such as printers, documents, pictures, and music between a few local computers.

Home office networks and small office networks are often set up by individuals that work from a home or a 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.

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

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 those described above.

Clients and Servers (1.1.2.2)

All computers connected to a network that participate directly in network communication are classified as hosts. Hosts are also called end devices.

Servers are computers with software that enable them to provide information, like email or web pages, to other end devices on the network. Each service requires separate server software. For example, a server requires web server software in order to provide web services to the network. 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 may be necessary for one computer to act as a file server, a web server, and an email server.

Clients are computers with 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 Chrome or Firefox. A single computer can also run multiple types of client software. For example, a user can check email and view a web page while instant messaging and listening to Internet radio.

Figure 1-2 shows different client and server examples.

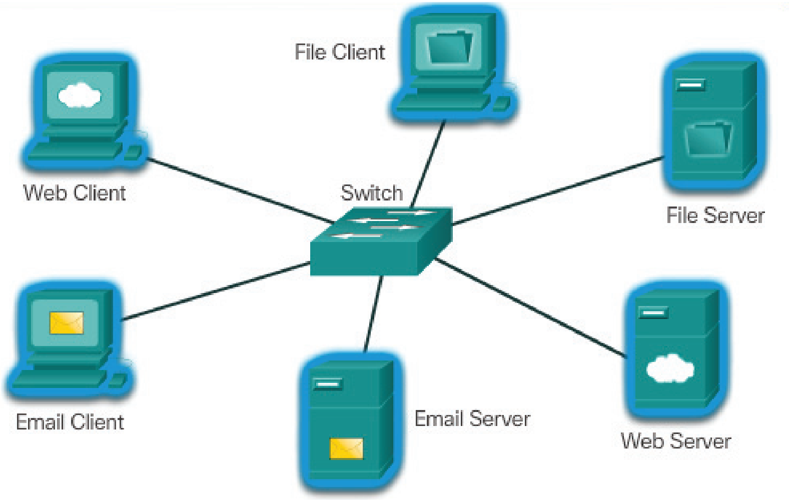


Figure 1-2 Client/Server Examples

- **Web Client and Server:** The Web Server runs web server software and clients use their browser software, such as Windows Internet Explorer, to access web pages on the server.
- **Email Client and Server:** The Email Server runs email server software and clients use their mail client software, such as Microsoft Outlook, to access email on the server.
- **File Client and Server:** The File Server stores corporate and user files in a central location. The client devices access these files with client software such as Windows Explorer.

Peer-to-Peer (1.1.2.3)

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*, as shown in Figure 1-3.

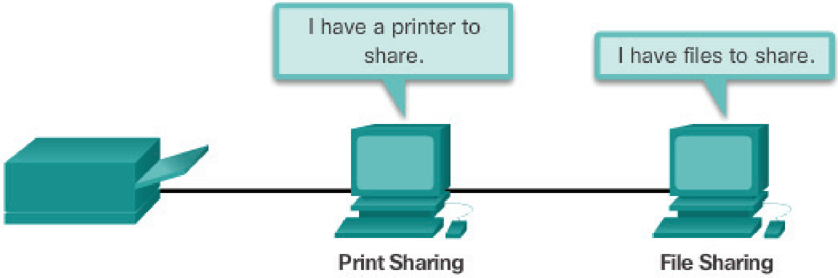


Figure 1-3 Peer-to-Peer Example

The advantages of peer-to-peer networking:

- Easy to set up
- Less complexity
- Lower cost since network devices and dedicated servers may not be required
- Can be used for simple tasks such as transferring files and sharing printers

The disadvantages of peer-to-peer networking:

- No centralized administration
- Not as secure
- Not scalable
- All devices may act as both clients and servers, which can slow their performance

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.

Network Components (1.2.1)

Different network components are used within the 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.

Overview of Network Components (1.2.1.1)

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

The network infrastructure contains three categories of network components, as shown in Figures 1-4, 1-5, and 1-6.

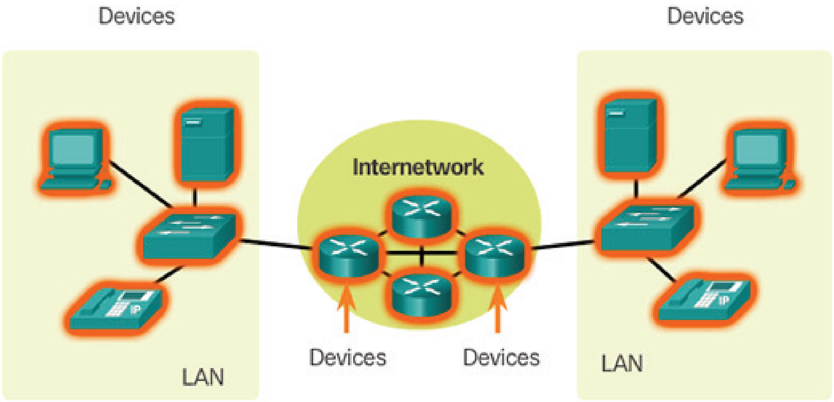


Figure 1-4 Devices

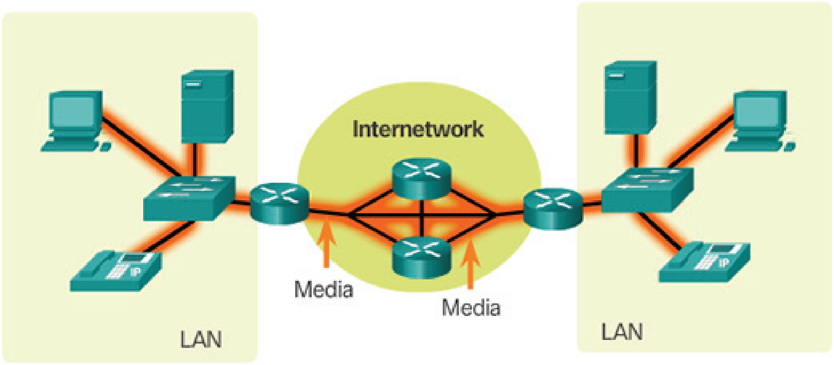


Figure 1-5 Media

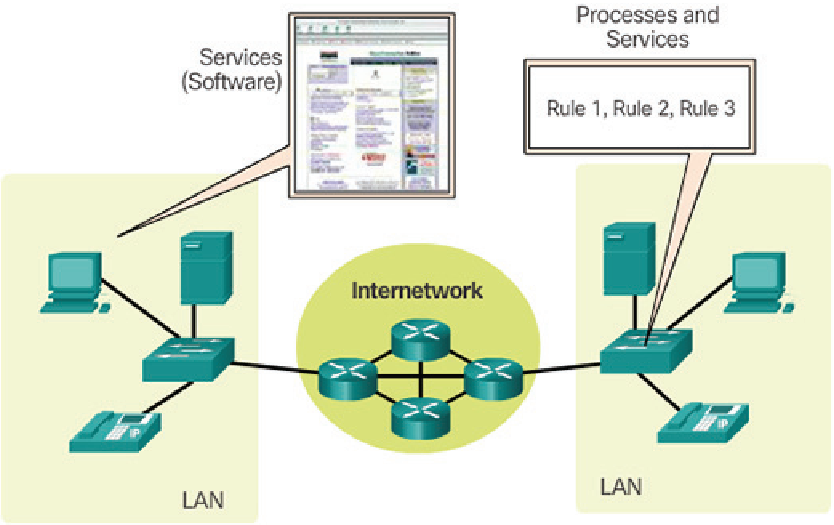


Figure 1-6 Services

Devices and media 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.

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. Some examples of end devices are shown in Figure 1-7.

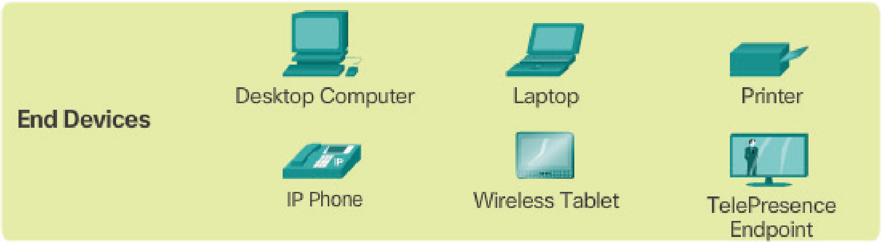


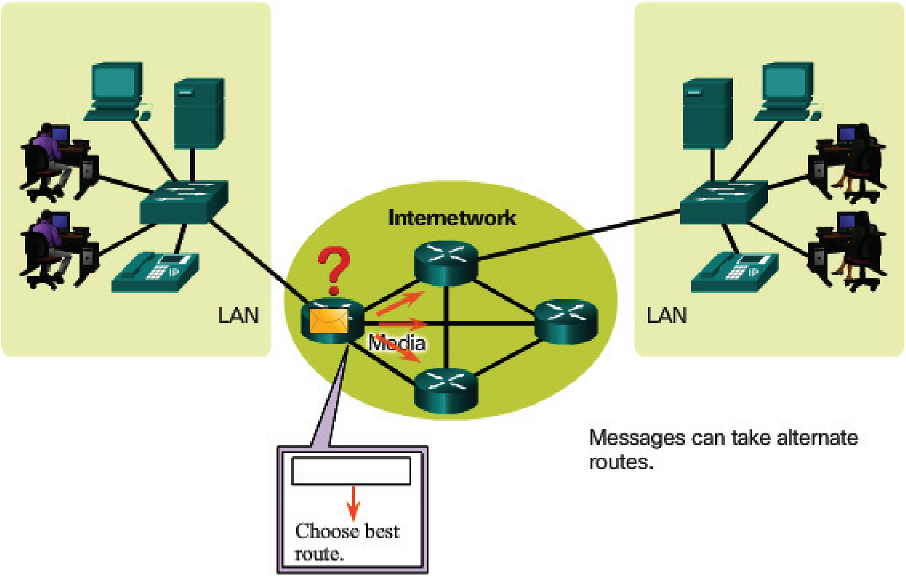
Figure 1-7 Examples of End Devices

An *end device* is either the source or destination of a message transmitted over the network. To distinguish one end device from another, each end device on a network is identified by an address. When an end device initiates communication, it uses the address of the destination end device to specify where the message should be sent. Devices between the source and destination are responsible for choosing the best path and forwarding messages sent between end devices, as shown in Figure 1-8.

Intermediary Network Devices (1.2.1.3)

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

Intermediary devices use the destination end device address, in conjunction with information about the network interconnections, to determine the path that messages should take through the network, as shown in Figure 1-8.



Messages can take alternate routes.

Data originates with an end device, flows through the network, and arrives at an end device.

Figure 1-8 End Devices Communicate Across the Internetwork

Examples of the more common intermediary devices are shown in Figure 1-9.

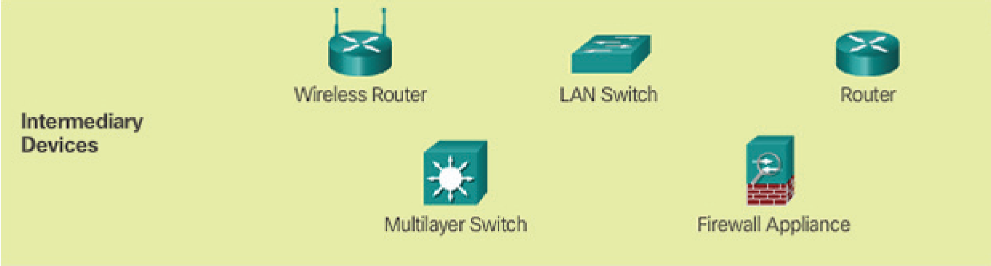


Figure 1-9 Examples of Intermediary Devices

Intermediary network devices perform some or all of 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 where there is a link failure
- Classify and direct messages according to 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 1-10, these media are

- **Metallic wires within cables –** data is encoded into electrical impulses
- **Glass or plastic fibers (fiber optic cable) –** data is encoded as pulses of light
- **Wireless transmission –** data is encoded using wavelengths from the electromagnetic spectrum

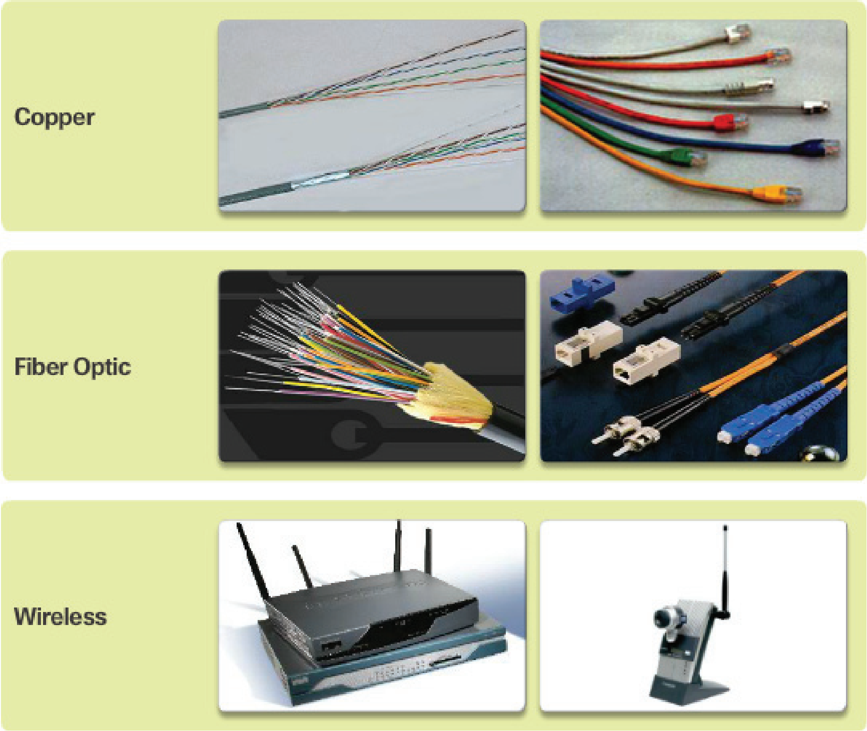


Figure 1-10 Examples of Network Media

Different types of network media have different features and benefits. Not all network media have the same characteristics, nor are they all appropriate for the same purpose.

Criteria to consider when choosing network media includes the following:

- What is the maximum distance that the media can successfully carry a signal?
- Into what type of environment will the media be installed?
- What is the amount of data and the speed at which it must be transmitted?
- What is the cost of the media and installation?

Network Representations (1.2.1.5)

Diagrams of networks often use symbols, like those shown in Figure 1-11, to represent the different devices and connections that make up a network.

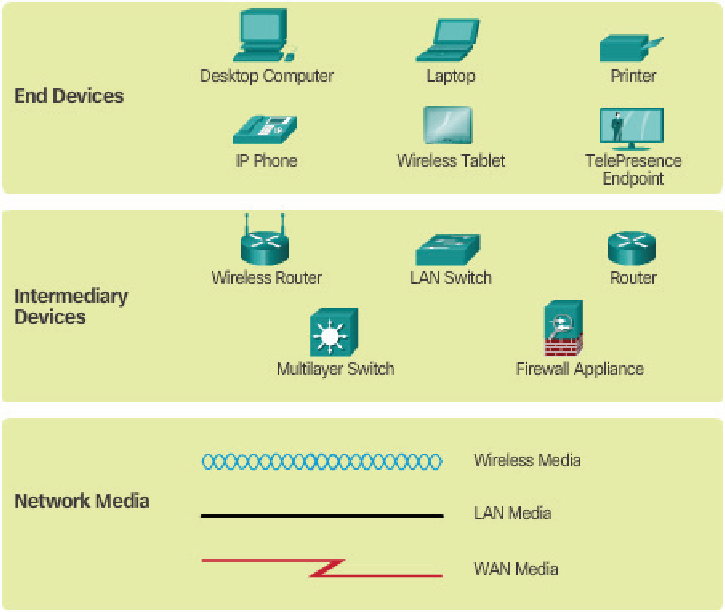


Figure 1-11 Common Icons Use to Represent Network Devices

A diagram provides an easy way to understand how devices in a large network are connected. This type of "picture" of a network is known as a topology diagram. 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.

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* – A NIC, or LAN adapter, provides the physical connection to the network at the PC or other end device. The media that are connecting the PC to the networking device plug directly into the NIC (Figure 1-12).

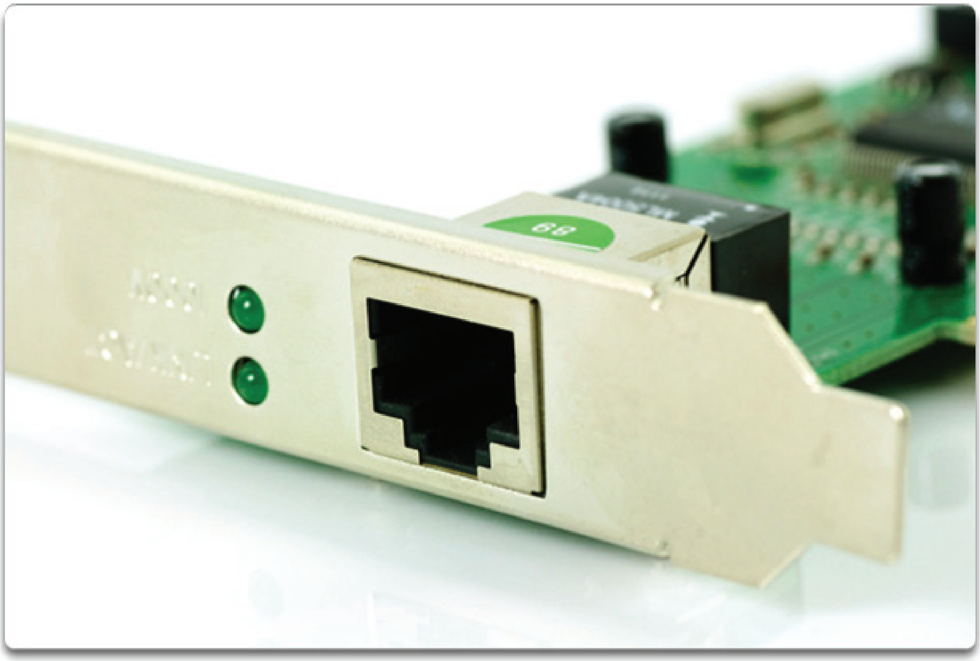


Figure 1-12 Network Interface Card

- *Physical Port* – A connector or outlet on a networking device where the media is connected to an end device or another networking device.
- *Interface* – Specialized ports on a networking device that connect to individual networks. Because routers are used to interconnect networks, the ports on a router are referred to as network interfaces.

Note

Often, the terms port and interface are often used interchangeably.

Topology Diagrams (1.2.1.6)

Topology diagrams 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* – Identify the physical location of intermediary devices and cable installation (Figure 1-13).

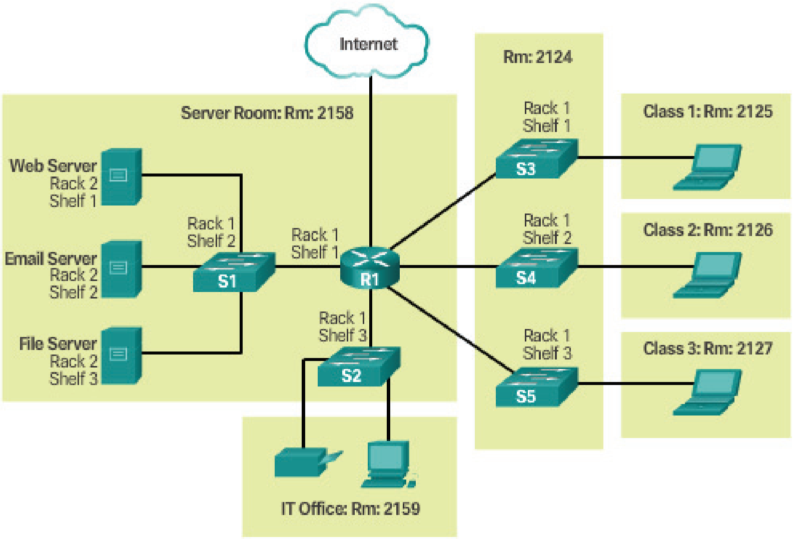


Figure 1-13 Physical Topology

- *Logical topology diagrams* – Identify devices, ports, and addressing scheme (Figure 1-14).

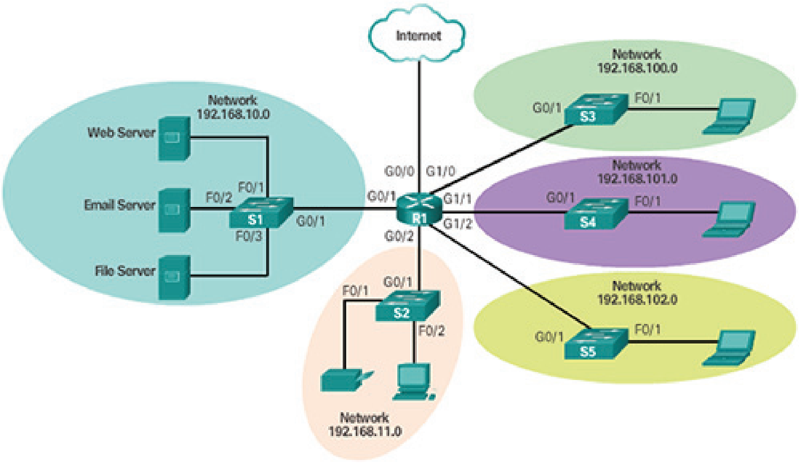


Figure 1-14 Logical Topology

The topologies shown in the physical and logical diagrams are appropriate for your level of understanding at this point in the course. Search the Internet for "network topology diagrams" to see some more complex examples. If you add the "Cisco" to your search phrase, you will find many topologies using similar icons to what you have seen in this chapter.

Interactive Graphic

Activity 1.2.1.7: Network Component Representations and Functions

Go to the online course to perform this practice activity.

LANs and WANs (1.2.2)

Network infrastructures can be differentiated is various ways. Two of the most common types of network infrastructures are LANs and WANs.

Types of Networks (1.2.2.1)

Network infrastructures can vary greatly in terms of

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

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

- *Local Area Network (LAN)* – A network infrastructure that provides access to users and end devices in a small geographical area, which is typically an enterprise, home, or small business network owned and managed by an individual or IT department.
- *Wide Area Network (WAN)* – A network infrastructure that provides access to other networks over a wide geographical area, which is typically owned and managed by a telecommunications service provider.

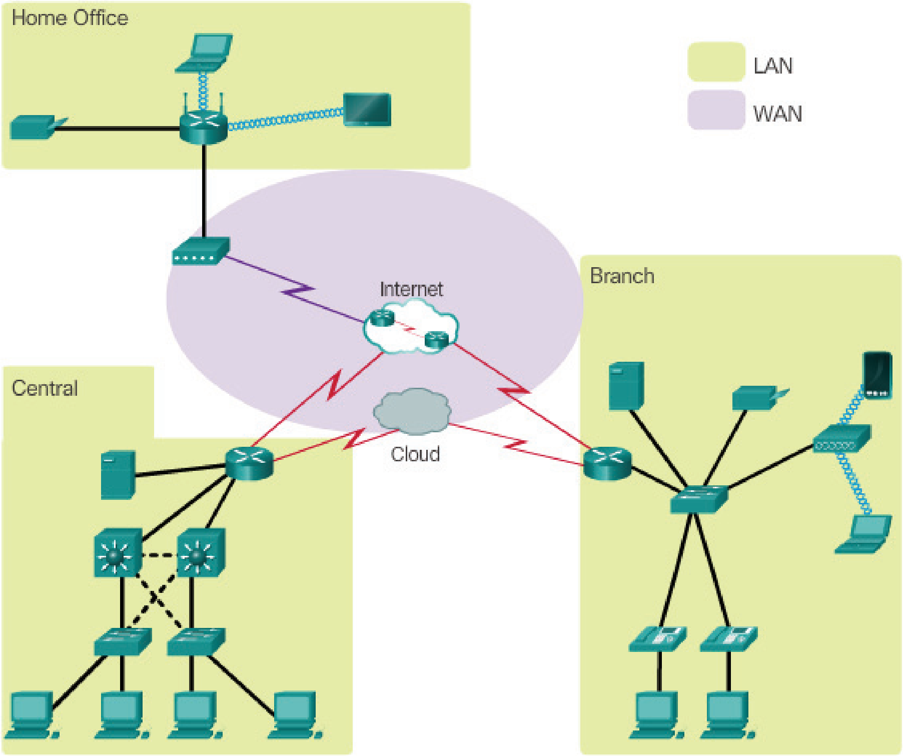


Figure 1-15 LANs and WANs

Video

Play the video to watch Cisco's Jimmy Ray Purser explains the difference between LAN and WAN.

Go to the online course to view this video.

Other types of networks include

- **Metropolitan Area Network (MAN) –** A network infrastructure that spans a physical area larger than a LAN but smaller than a WAN (e.g., a city). MANs are typically operated by a single entity such as a large organization.
- **Wireless LAN (WLAN) –** Similar to a LAN but wirelessly interconnects users and end points in a small geographical area.
- **Storage Area Network (SAN) –** A network infrastructure designed to support file servers and provide data storage, retrieval, and replication.

Local Area Networks (1.2.2.2)

LANs are a network infrastructure that spans a small geographical area, as shown in Figure 1-16.

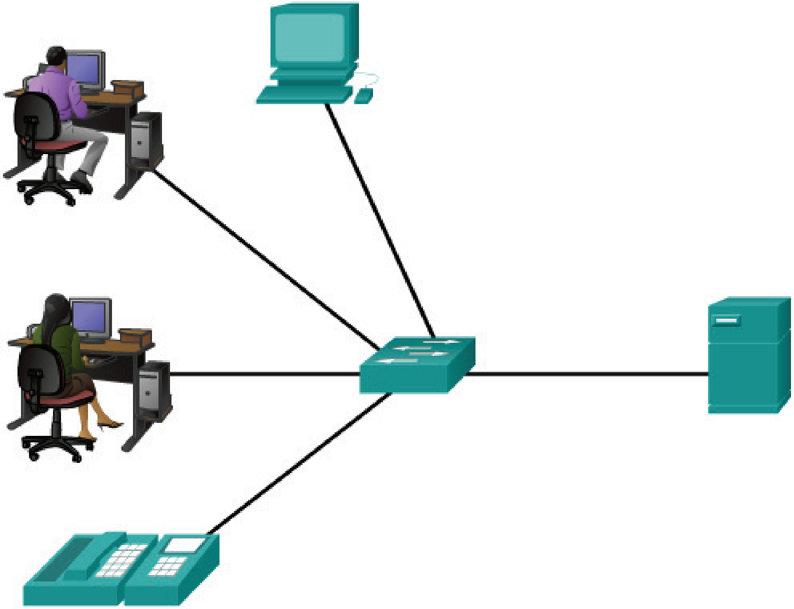


Figure 1-16 Example of a LAN

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.
- LANs provide high-speed bandwidth to internal end devices and intermediary devices.

Wide Area Networks (1.2.2.3)

WANs are a network infrastructure that spans a wide geographical area, as shown in Figure 1-17. WANs are typically managed by service providers (SP) or Internet Service Providers (ISP).

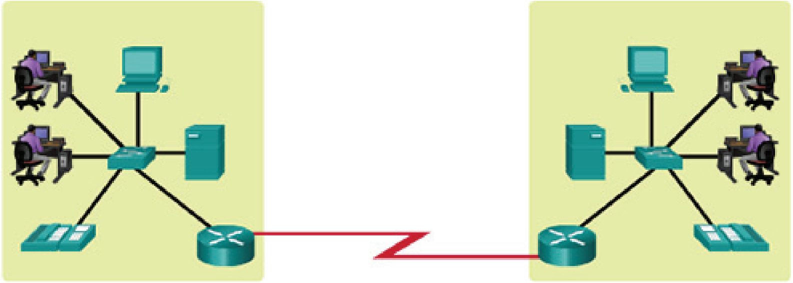


Figure 1-17 Example of a WAN

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, Intranets, and Extranets (1.2.3)

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.

The Internet (1.2.3.1)

The ***Internet*** is a worldwide collection of interconnected networks (internetworks or internet for short). Figure 1-18 one way to view the Internet as a collection of interconnected LANs and WANs.

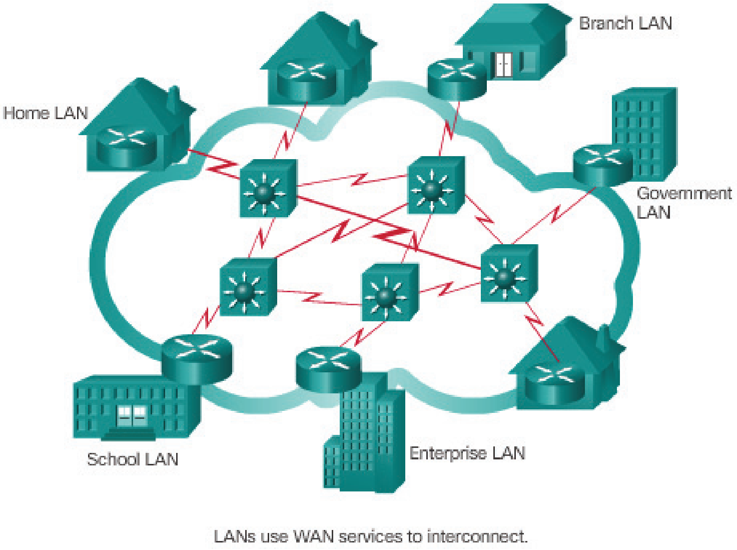


Figure 1-18 Collection of Interconnected LANs and WANs

Some of the LAN examples are connected to each other through a WAN connection. WANs are then connected to each other. The red WAN connection lines represent all the varieties of ways we connect networks. WANs can connect through copper wires, fiber optic cables, and wireless transmissions (not shown).

The Internet 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 structure and standardization of Internet protocols and processes. These organizations include the Internet Engineering Task Force (IETF), Internet Corporation for Assigned Names and Numbers (ICANN), and the Internet Architecture Board (IAB), plus many others.

Note

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

Intranets and Extranets (1.2.3.2)

There are two other terms that are similar to the term Internet:

- Intranet
- Extranet

Figure 1-19 shows the relationship of the Internet, extranets, and intranets.

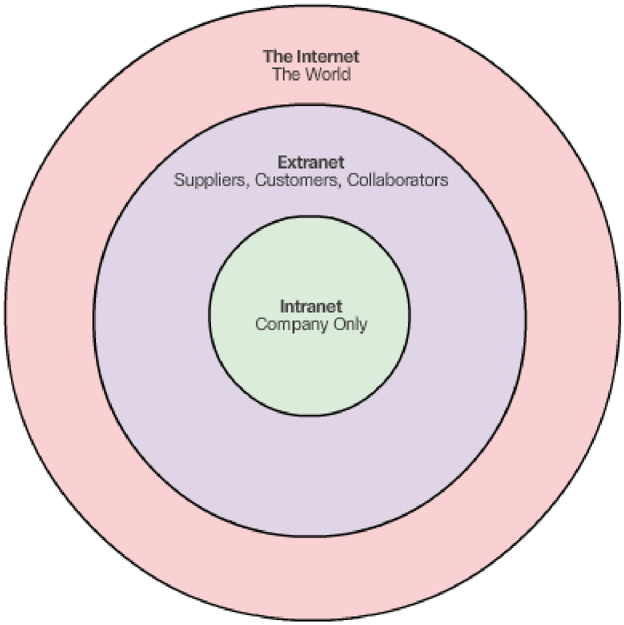


Figure 1-19 Internet, Extranet, and Intranet

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.

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

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

Internet Connections (1.2.4)

The type of connection to the Internet will depend on the type of network being connected. A business network will usually require a connection with more bandwidth than a home network.

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.

Home and Small Office Internet Connections (1.2.4.2)

Figure 1-20 illustrates common connection options for small office and home office users.

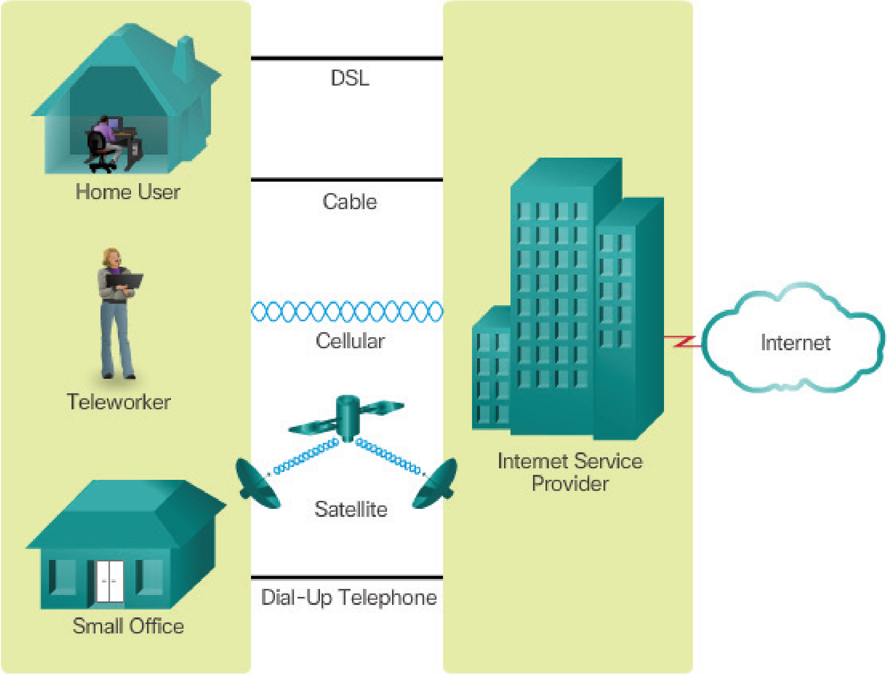


Figure 1-20 Connection Options

- **Cable –** Typically offered by cable television service providers, the Internet data signal is carried on the same cable that delivers cable television. It provides a high bandwidth, always on, connection to the Internet.

- **DSL –** Digital Subscriber Lines provide a high bandwidth, always on, connection to the Internet. DSL runs over a telephone line. In general, small office and home office users connect using Asymmetrical DSL (ADSL), which means that the download speed is faster than the upload speed.
- **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.
- **Satellite –** The availability of satellite Internet access is a real benefit in those areas that would otherwise have no Internet connectivity at all. Satellite dishes require a clear line of sight to the satellite.
- **Dial-up Telephone –** An inexpensive option that uses any phone line and a modem. The low bandwidth provided by a dial-up modem connection is usually not sufficient for large data transfer, although it is useful for mobile access while traveling.

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

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

Businesses Internet Connections (1.2.4.3)

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

Figure 1-21 illustrates common connection options for businesses.

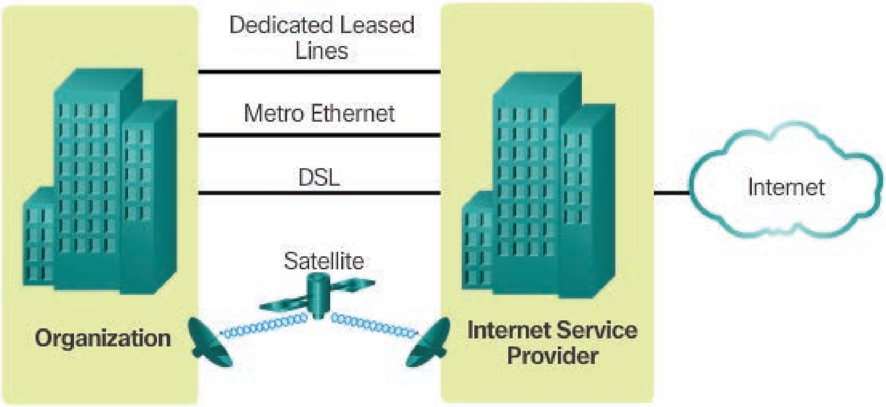


Figure 1-21 Typical Business Connection Options

- **Dedicated Leased Line –** Leased lines are actually reserved circuits within the service provider's network that connect geographically separated offices for private voice and/or data networking. The circuits are typically rented at a monthly or yearly rate. They can be expensive.
- **Ethernet WAN –** Ethernet WANs extend LAN access technology into the WAN. Ethernet is a LAN technology you will learn about in a later chapter. The benefits of Ethernet are now being extended into the WAN.
- **DSL –** Business DSL is available in various formats. A popular choice is Symmetric Digital Subscriber Lines (SDSL), which is similar to the consumer version of DSL but provides uploads and downloads at the same speeds.
- **Satellite –** Similar to small office and home office users, satellite service can provide a connection when a wired solution is not available.

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

Packet Tracer
□ **Activity**

Packet Tracer 1.2.4.4: Help and Navigation Tips

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 between various modes and workspaces.

Packet Tracer
□ **Activity**

Packet Tracer 1.2.4.5: Network Representation

In this activity, 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.

Converged Networks (1.3.1)

Modern networks are constantly evolving to meet user demands. Today's networks are used for data, phone, and video.

Traditional Separate Networks (1.3.1.1)

Consider a school built thirty years ago. Back then, some classrooms were cabled for the data network, telephone network, and video network for televisions. These separate networks could not communicate with each other, as shown in Figure 1-22.

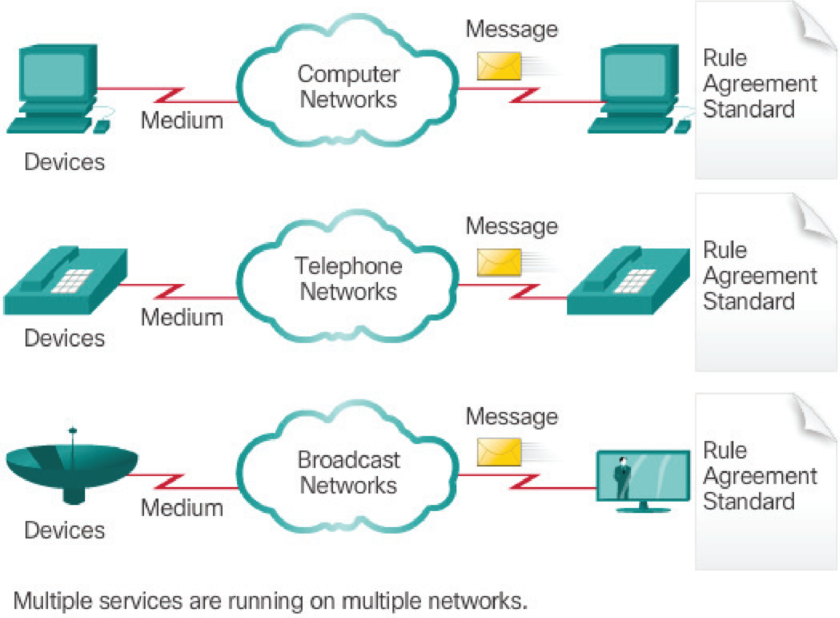
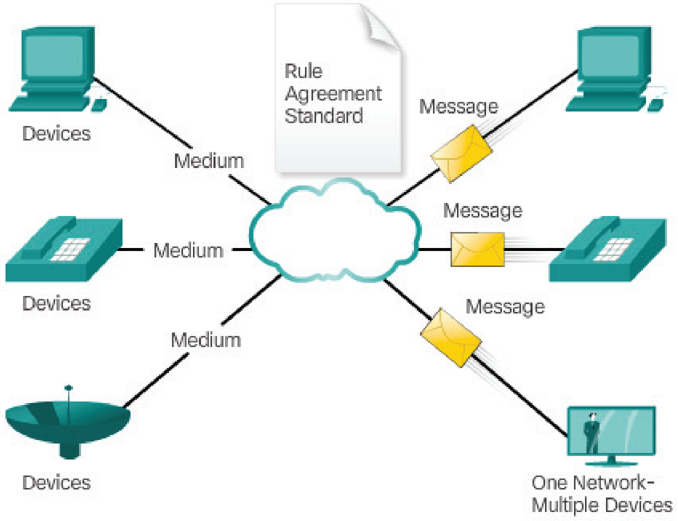


Figure 1-22 Multiple Networks

Each network used different technologies to carry the communication signal. Each network had its own set of rules and standards to ensure successful communication.

The Converging Network (1.3.1.2)

Today, the separate data, telephone, and video networks are converging. Unlike dedicated networks, *converged networks* are capable of delivering data, voice, and video between many different types of devices over the same network infrastructure, as shown in Figure 1-23. This network infrastructure uses the same set of rules, agreements, and implementation standards.



Converged data networks carry multiple services on one network.

Figure 1-23 Converged Networks

Lab 1.3.1.3: Researching Converged Network Services

In this lab, you will complete the following objectives:

- Part 1: Survey Your Understanding of Convergence
- Part 2: Research ISPs Offering Converged Services
- Part 3: Research Local ISPs Offering Converged Services
- Part 4: Select Best Local ISP Converged Service
- Part 5: Research Local Company or Public Institution Using Convergence Technologies

Reliable Network (1.3.2)

With our reliance on networks, certain precautions must be taken to ensure that the network functions as designed, even if things go wrong. Networks must be able to expand to meet the increased needs of an organization. The services provided by the network must be secure and provide the quality of service to meet the expectations of the organization.

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 data across the network.

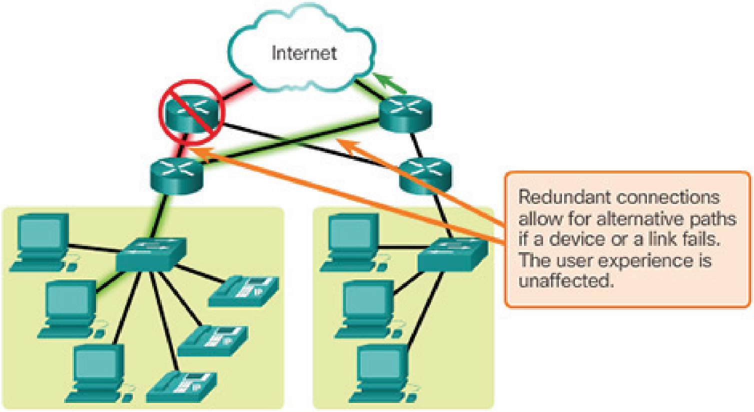
As networks evolve, we are discovering that there are four basic characteristics that the underlying architectures need to address in order to meet user expectations:

- Fault Tolerance
- Scalability
- Quality of Service (QoS)
- Security

Fault Tolerance (1.3.2.2)

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. 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.

One way reliable networks provide redundancy is by implementing a *packet-switched network*. Packet switching splits traffic into packets that are routed over a shared network. A single message, such as an email or a video stream, is broken into multiple message blocks, called packets. Each packet has the necessary addressing information of the source and destination of the message. The routers within the network switch the packets based on the condition of the network at that moment. This means that all the packets in a single message could take very different paths to the destination. In Figure 1-24, the user is not aware and is unaffected by the router dynamically changing the route when a link fails.



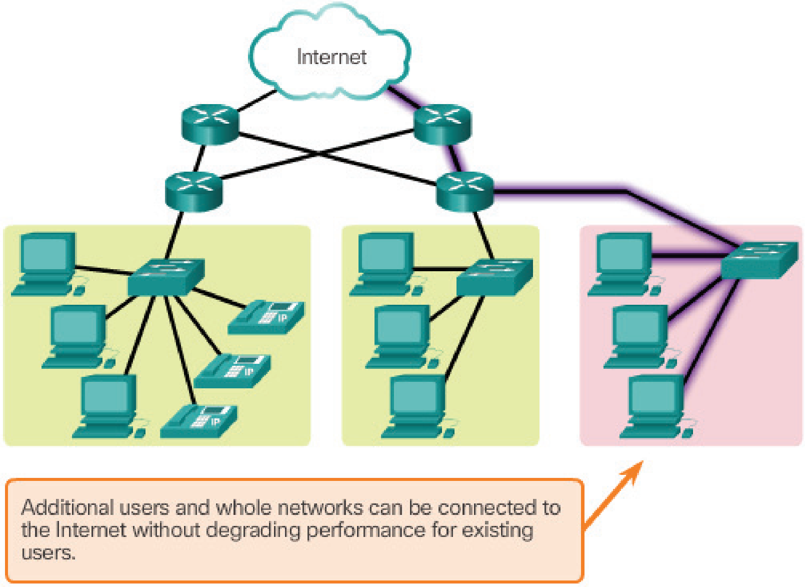
Redundant connections allow for alternative paths if a device or a link fails. The user experience is unaffected.

Figure 1-24 Fault Tolerance

This is not the case in circuit-switched networks traditionally used for voice communications. A *circuit-switched network* is one that establishes a dedicated circuit between the source and destination before the users may communicate. If the call is unexpectedly terminated, the users must initiate a new connection.

Scalability (1.3.2.3)

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 1-25 shows how a new network can be easily added to an existing network.



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

Figure 1-25 Scalability

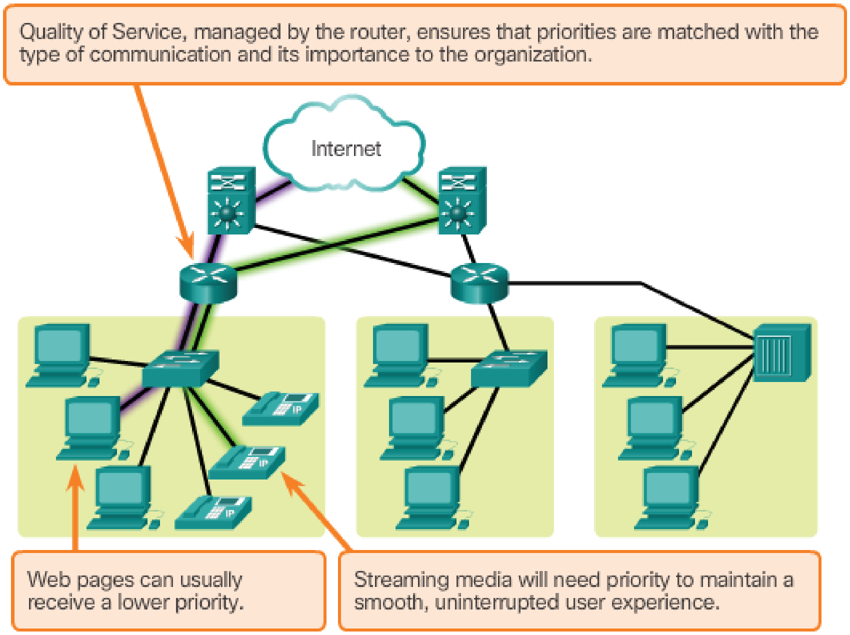
In addition, networks are scalable because the designers follow accepted standards and protocols. This allows software and hardware vendors to focus on improving products and services without worrying about designing a new set of rules for operating within the network.

Quality of Service (1.3.2.4)

Quality of Service (QoS) is also an ever-increasing requirement of networks today. New applications available to users over internetworks, such as voice and live video transmissions, create higher expectations for the quality of the delivered services. Have you ever tried to watch a video with constant breaks and pauses? As data, voice, and video content continue to converge onto the same network, QoS becomes a primary mechanism for managing congestion and ensuring reliable delivery of content to all users.

Congestion occurs when the demand for bandwidth exceeds the amount available. *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.

When the volume of traffic 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. In Figure 1-26, one user is requesting a web page and another is on a phone call. With a QoS policy in place, the router can manage the flow of data and voice traffic, giving priority to voice communications if the network experiences congestion.



Quality of Service, managed by the router, ensures that priorities are matched with the type of communication and its importance to the organization.

Web pages can usually receive a lower priority.

Streaming media will need priority to maintain a smooth, uninterrupted user experience.

Figure 1-26 Quality of Service (QoS)

Security (1.3.2.5)

The network infrastructure, services, and the data contained on network-attached devices are crucial personal and business assets. 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, as shown in Figure 1-27.

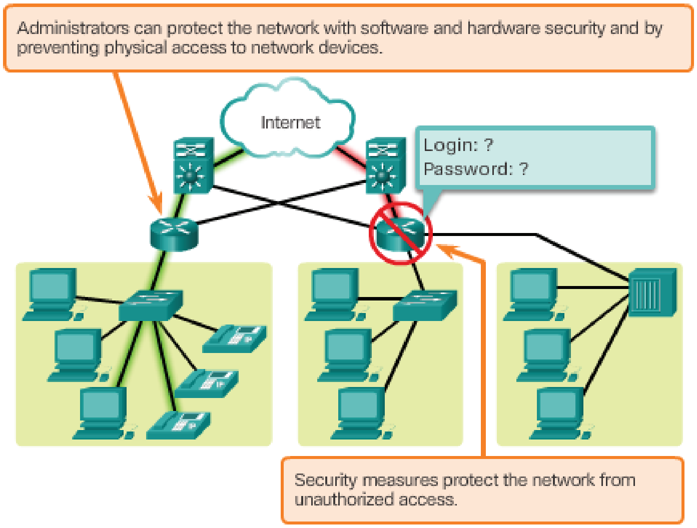

Administrators can protect the network with software and hardware security and by preventing physical access to network devices.
Internet
Login: ?
Password: ?
Security measures protect the network from unauthorized access.

Figure 1-27 Security

Information security refers to protecting the information contained within the packets being transmitted over the network and the information stored on network attached devices. In order to achieve the goals of network security, there are three primary requirements, as shown in Figure 1-28.

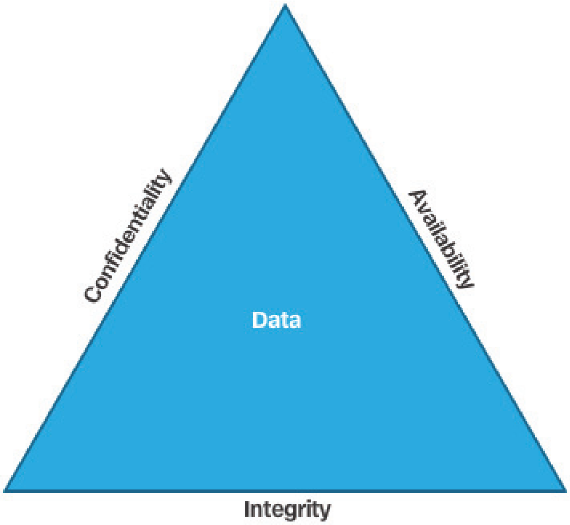


Figure 1-28 CIA Triad

- **Confidentiality –** Data confidentiality means that only the intended and authorized recipients can access and read data.
- **Integrity –** Data integrity means having the assurance that the information has not been altered in transmission, from origin to destination.
- **Availability –** Data availability means having the assurance of timely and reliable access to data services for authorized users.

Interactive Graphic

Activity 1.3.2.6: Reliable Networks

Go to the online course 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 couldn't be imagined years ago.

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)

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 between people, devices, and information. There are several new networking trends that will affect organizations and consumers. Some of the top trends include

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

Bring Your Own Device (1.4.1.2)

The concept of any device, to any content, in any manner, 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.

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." Collaboration tools, like Cisco WebEx shown in Figure 1-29, give employees, students, teachers, customers, and partners a way to instantly connect, interact, and achieve their objectives.

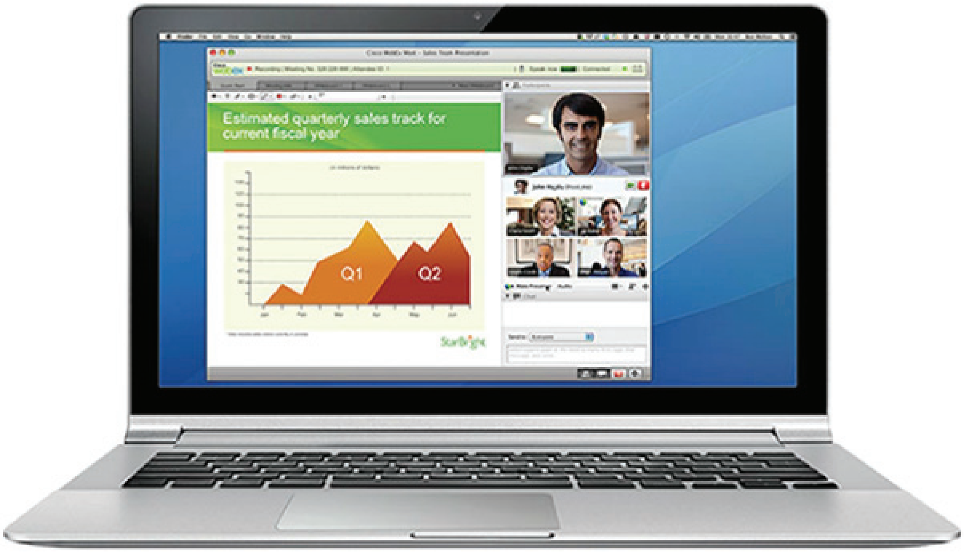


Figure 1-29 Cisco WebEx

For businesses, collaboration is a critical and strategic priority that organizations are using to remain competitive. Collaboration is also a priority in education. Students need to collaborate to assist each other in learning, to develop team skills used in the work force, and to work together on team-based projects.

Video Communication (1.4.1.4)

Another trend in networking that is critical to the communication and collaboration effort is video. Video is being used for communications, collaboration, and entertainment. Video calls can be made to and from anywhere with an Internet connection. Consider how many people are now using Skype or FaceTime to communicate with friends and family.

Video conferencing is a powerful tool for communicating with others at a distance, both locally and globally. Video is becoming a critical requirement for effective collaboration as organizations extend across geographic and cultural boundaries. Play the video to view how TelePresence can be incorporated into everyday life and business.

Video

Go to the online course to view this video.

Cloud Computing (1.4.1.5)

Cloud computing is another global trend changing the way we access and store data. Cloud computing allows us to store personal files, even backup our entire hard disk 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.

There are four primary types of Clouds, as shown in Figure 1-30.

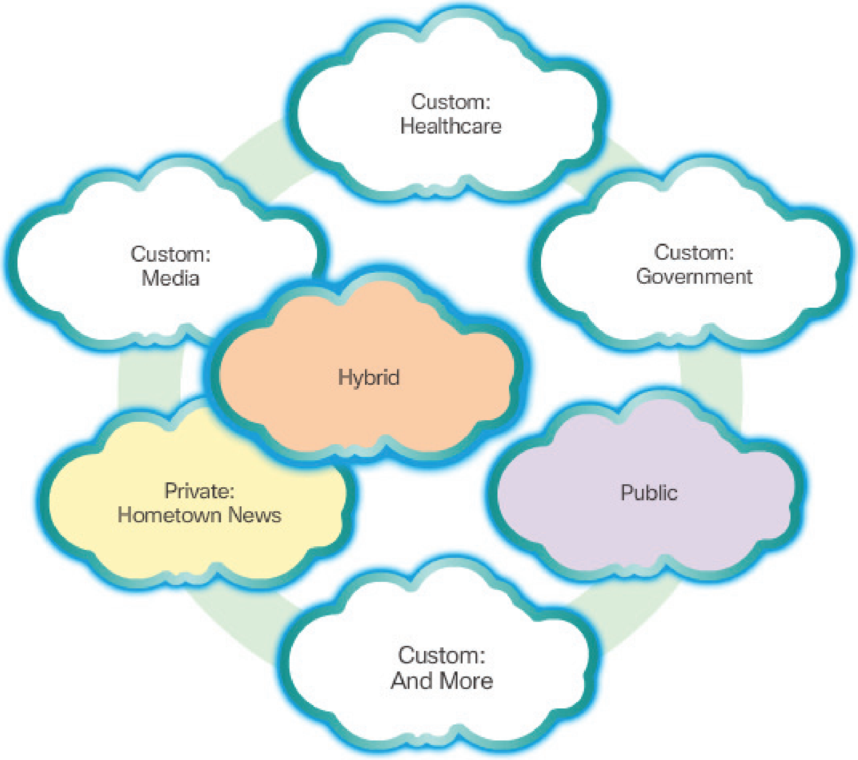


Figure 1-30 Types of Clouds

- *Private clouds* – Cloud-based applications and services offered in a private cloud are intended for a specific organization or entity, such as the government. A private cloud can be set up using the organization's private network, although this can be expensive to build and maintain. A private cloud can also be managed by an outside organization with strict access security.
- *Public clouds* – Cloud-based applications and services offered in a public cloud are made available to the general population. Services may 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* – A hybrid cloud is made up of two or more clouds (example: part custom, 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* – These are clouds built to meet the needs of a specific industry, such as healthcare or media. Custom clouds can be private or public.

Cloud computing is possible because of data centers. A *data center* is a facility used to house computer systems and associated components. A data center can occupy one room of a building, one or more floors, or an entire building. 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. Smaller organizations that cannot afford to maintain their own private data center can reduce the overall cost of ownership by leasing server and storage services from a larger data center organization in the Cloud.

Networking Technologies for the Home (1.4.2)

Today's home networks are used in every aspect of our daily lives, for entertainment, education, communications, and business.

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, as shown in Figure 1-31.

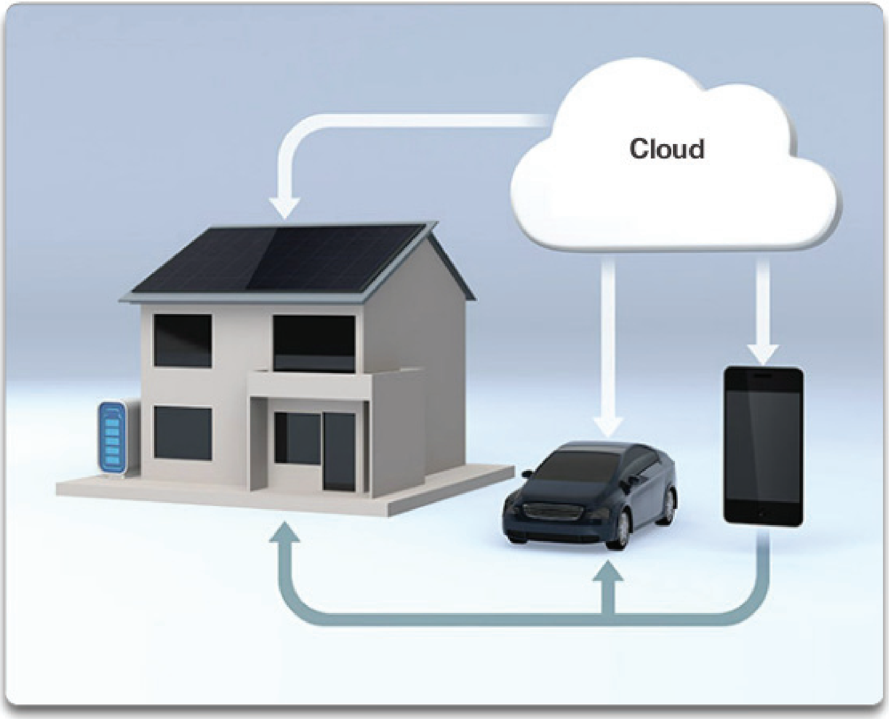


Figure 1-31 Smart Home Technology

The newest home trends include '*smart home technology*.' Smart home technology 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 if 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 allows 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 the future. 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 become more widespread. 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 1-32.

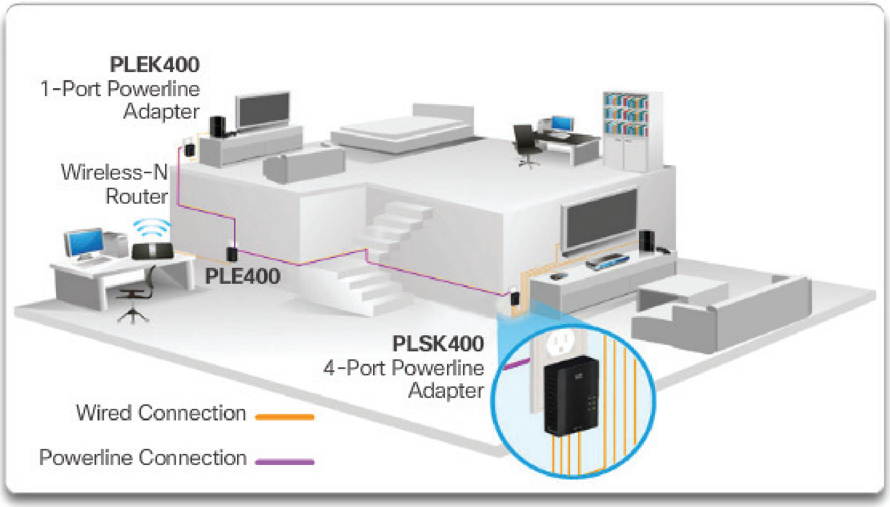


Figure 1-32 Powerline Networking

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 without any additional cost to the electrical bill. Using the same wiring that delivers electricity, powerline networking sends information by sending data on certain frequencies.

Using a 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 in 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 may be another option in many areas.

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 (WLANs). WISPs are more commonly found in rural environments where DSL or cable services are not available.

Although a separate transmission tower may 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 is not much different than DSL or cable service. The main difference is that the connection from the home to the ISP is wireless instead of a physical cable.

Another wireless solution for the home and small businesses is wireless broadband, as shown in Figure 1-33.

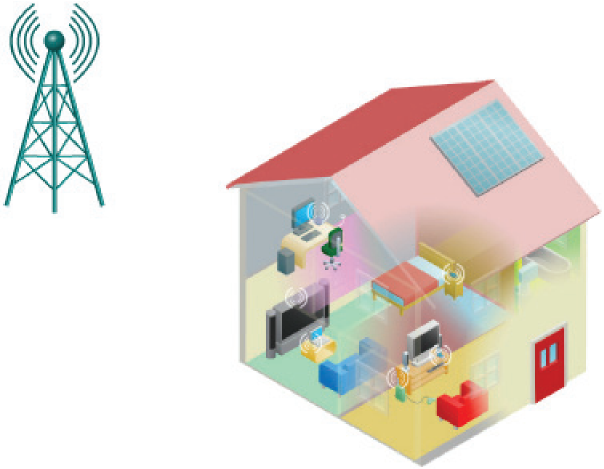


Figure 1-33 Wireless Broadband Service

This uses the same cellular technology used to access the Internet with a smart phone 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.

Network Security (1.4.3)

For a network to be entrusted with the communications of personal and business information, that network must be secure.

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 that is 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 allowing for 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. Threat vectors may be external or internal. 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 in order to access private data

It is equally important to consider internal threats. There have been many studies that show that the most common data breaches happen because of 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, both internal and external, as shown in Figure 1-34.

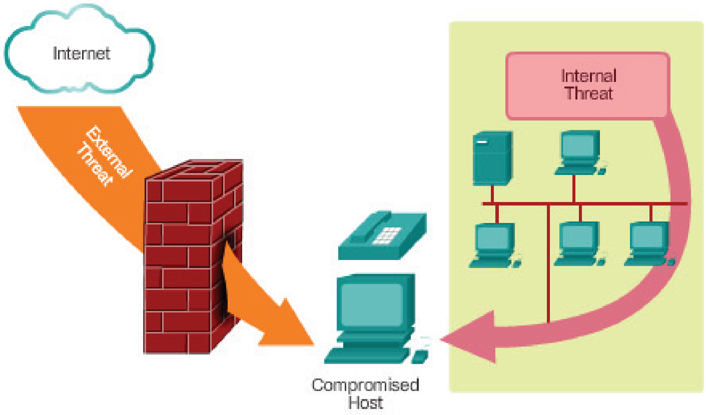


Figure 1-34 Threats to Networks

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 end 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 –** These are used to protect end devices from becoming infected with malicious software.
- **Firewall filtering –** This is used to block unauthorized access to the network. This may include a host-based firewall system that is implemented to prevent unauthorized access to the end 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 above, larger networks and corporate networks often have other security requirements:

- **Dedicated firewall systems –** These are used to provide more advanced firewall capabilities that can filter large amounts of traffic with more granularity.
- **Access control lists (ACL) –** These are used to further filter access and traffic forwarding.
- **Intrusion prevention systems (IPS) –** These are used to identify fast-spreading threats, such as zero-day or zero-hour attacks.
- **Virtual private networks (VPN) –** These are used 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 allowing for the quality of service that is expected of each technology. Additionally, the security solution implemented must be adaptable to the growing and changing trends of the network.

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

Interactive Graphic

Activity 1.4.3.3: Network Security Terminology

Go to the online course to perform this practice activity.

Network Architecture (1.4.4)

[The role of the network has changed from a data-only network to a system that enables the connections of people, devices, and information in a media-rich, converged network environment. In order for networks to function efficiently and grow in this type of environment, the network must be built upon a standard network architecture.

Cisco Network Architecture (1.4.4.1)

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 for wireless access, and provide for 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. Other certifications beyond the Associate are also available, as shown in Figure 1-35.

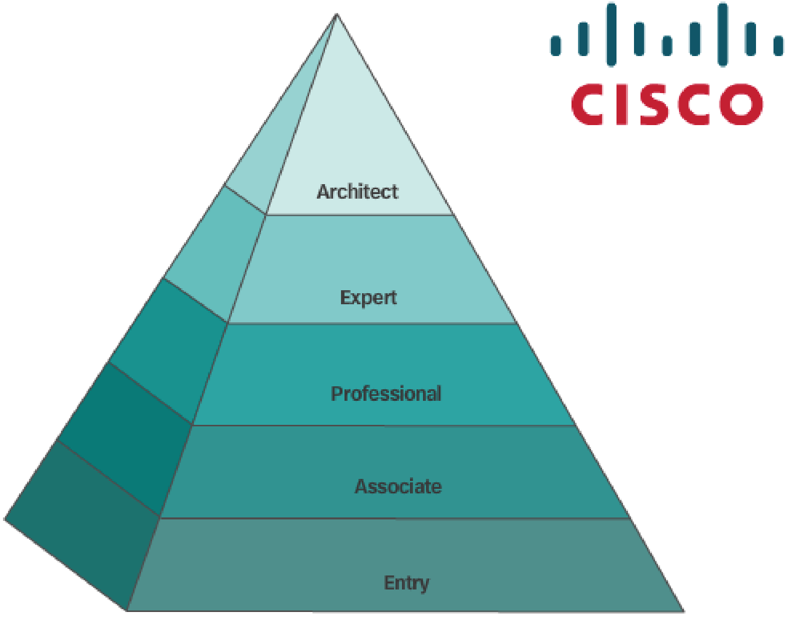


Figure 1-35 Cisco Certification Hierarchy

CCNA certification validates an individual's ability to install, configure, operate, and troubleshoot medium-size routed and switched networks, including implementation and verification of connections to remote sites in a WAN. 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 Ethernet, VLANs, IPv4, IPv6, Open Shortest Path First (OSPF), Enhanced Interior Gateway Routing Protocol (EIGRP), access control lists (ACLs) and others.

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

Lab 1.4.4.3: Researching IT and Networking Job Opportunities

In this lab, you will complete the following objectives:

- Part 1: Research Job Opportunities
- Part 2: Reflect on Research

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 may 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 may wish 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.

Warriors of the Net (1.5.1.2)

An entertaining resource to help you visualize networking concepts is the animated movie “Warriors of the Net” by TNG Media Lab. Before viewing the video, there are a few things to consider. In terms of concepts you have learned in this chapter, think about when, in the video, you are on the LAN, on the WAN, on the intranet, on the Internet, and what are end devices versus intermediate devices.

Although all animations often have simplifications in them, there is one outright error in the video. About 5 minutes in, the statement is made “What happens when Mr. IP doesn’t receive an acknowledgment, he simply sends a replacement packet.” This is not a function of the Layer 3 Internet Protocol, which is an “unreliable,” best effort delivery protocol, but rather a function of the transport layer TCP protocol. IP is explained in Chapter 6 and TCP is explained in Chapter 9.

Download the movie from http://www.warriorsofthe.net

Conclusion (1.5.1.3)

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 the network must be fault tolerant, 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. The network infrastructure must grow and adjust to support the way the network is used. The routing and switching platform is the foundation of any network infrastructure.

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

Practice

The following activities provide practice with the topics introduced in this chapter. The Labs and Class Activities are available in the companion Introduction to Networks v5.1 Lab Manual (ISBN 9781587133534). 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 Network Collaboration Tools

Lab 1.3.1.3: Researching Converged Network Services

Lab 1.4.4.3: Researching IT and Networking Job Opportunities

Packet Tracer
□ Activity

Packet Tracer Activities

Packet Tracer 1.2.4.4: Help and Navigation Tips

Packet Tracer 1.2.4.5: Network Representation

Check Your Understanding Questions

Complete all the review questions listed here to test your understanding of the topics and concepts in this chapter. The appendix "Answers to '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

   E. Access point

   F. TelePresence endpoint

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. Dial-up

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

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

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

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

12. In which scenario would the use of a WISP be recommended?

    A. an Internet cafe in a city
    B. a farm in a rural area without wired broadband access
    C. any home with multiple wireless devices
    D. an apartment in a building with cable access to the Internet

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?

This page intentionally left blank

Index