"All-in-One Is All You Need."

ALL-IN-ONE

CompTIA IT Fundamentals+®

EXAM GUIDE

EXAM FC0-U61

SECOND EDITION

Save 10% on any CompTIA exam voucher! Coupon code inside.

Online Content Includes:

- 130 practice exam questions in a customizable test engine
- Link to over an hour of free video training from Mike Meyers

Complete coverage of all current objectives for the CompTIA IT Fundamentals+ exam

Ideal as both a study tool and an on-the-job reference

Filled with practice exam questions and in-depth explanations

SCOTT JERNIGAN
CompTIA A+®, CompTIA Network+®

MIKE MEYERS
CompTIA A+, CompTIA Network+, CompTIA Security+®

DANIEL LACHANCE
CompTIA A+, CompTIA Network+, CompTIA Cloud+®, CompTIA Server+®, CompTIA Security+, MCSA

Mc Graw Hill Education

https://t.me/learningnets

https://t.me/learningnets

"All-in-One Is All You Need."

ALL-IN-ONE

CompTIA IT Fundamentals+®

EXAM GUIDE

EXAM FC0-U61

SECOND EDITION

Save 10% on any CompTIA exam voucher! Coupon code inside.

Online Content Includes:

- 130 practice exam questions in a customizable test engine
- Link to over an hour of free video training from Mike Meyers

Complete coverage of all current objectives for the CompTIA IT Fundamentals+ exam

Ideal as both a study tool and an on-the-job reference

Filled with practice exam questions and in-depth explanations

SCOTT JERNIGAN
CompTIA A+®, CompTIA Network+®

MIKE MEYERS
CompTIA A+, CompTIA Network+, CompTIA Security+®

DANIEL LACHANCE
CompTIA A+, CompTIA Network+, CompTIA Cloud+®, CompTIA Server+®, CompTIA Security+, MCSA

https://t.me/learningnets

https://t.me/learningnets

ALL ■ IN ■ ONE

CompTIA IT Fundamentals+®

EXAM GUIDE

Second Edition
(Exam FC0-U61)

Mike Meyers
Scott Jernigan
Dan Lachance



New York Chicago San Francisco
Athens London Madrid Mexico City
Milan New Delhi Singapore Sydney Toronto

McGraw-Hill Education is an independent entity from CompTIA® and is not affiliated with CompTIA in any manner. This publication and online content may be used in assisting students to prepare for the CompTIA IT Fundamentals+ exam. Neither CompTIA nor McGraw-Hill Education warrants that use of this publication and online content will ensure passing any exam. CompTIA and IT Fundamentals+ are registered trademarks of CompTIA in the United States and/or other countries. All other trademarks are trademarks of their respective owners.

https://t.me/learningnets

Copyright © 2019 by McGraw-Hill Education. All rights reserved. Except as permitted under the United States Copyright Act of 1976, no part of this publication may be reproduced or distributed in any form or by any means, or stored in a database or retrieval system, without the prior written permission of the publisher, with the exception that the program listings may be entered, stored, and executed in a computer system, but they may not be reproduced for publication.

ISBN: 978-1-26-044188-8
MHID: 1-26-044188-1

The material in this eBook also appears in the print version of this title: ISBN: 978-1-26-044187-1, MHID: 1-26-044187-3.

eBook conversion by codeMantra
Version 1.0

All trademarks are trademarks of their respective owners. Rather than put a trademark symbol after every occurrence of a trademarked name, we use names in an editorial fashion only, and to the benefit of the trademark owner, with no intention of infringement of the trademark. Where such designations appear in this book, they have been printed with initial caps.

McGraw-Hill Education eBooks are available at special quantity discounts to use as premiums and sales promotions or for use in corporate training programs. To contact a representative, please visit the Contact Us page at www.mhprofessional.com.

All trademarks or copyrights mentioned herein are the possession of their respective owners and McGraw-Hill Education makes no claim of ownership by the mention of products that contain these marks.

Information has been obtained by McGraw-Hill Education from sources believed to be reliable. However, because of the possibility of human or mechanical error by our sources, McGraw-Hill Education, or others, McGraw-Hill Education does not guarantee the accuracy, adequacy, or completeness of any information and is not responsible for any errors or omissions or the results obtained from the use of such information.

https://t.me/learningnets

TERMS OF USE

This is a copyrighted work and McGraw-Hill Education and its licensors reserve all rights in and to the work. Use of this work is subject to these terms. Except as permitted under the Copyright Act of 1976 and the right to store and retrieve one copy of the work, you may not decompile, disassemble, reverse engineer, reproduce, modify, create derivative works based upon, transmit, distribute, disseminate, sell, publish or sublicense the work or any part of it without McGraw-Hill Education's prior consent. You may use the work for your own noncommercial and personal use; any other use of the work is strictly prohibited. Your right to use the work may be terminated if you fail to comply with these terms.

THE WORK IS PROVIDED "AS IS." McGRAW-HILL EDUCATION AND ITS LICENSORS MAKE NO GUARANTEES OR WARRANTIES AS TO THE ACCURACY, ADEQUACY OR COMPLETENESS OF OR RESULTS TO BE OBTAINED FROM USING THE WORK, INCLUDING ANY INFORMATION THAT CAN BE ACCESSED THROUGH THE WORK VIA HYPERLINK OR OTHERWISE, AND EXPRESSLY DISCLAIM ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. McGraw-Hill Education and its licensors do not warrant or guarantee that the functions contained in the work will meet your requirements or that its operation will be uninterrupted or error free. Neither McGraw-Hill Education nor its licensors shall be liable to you or anyone else for any inaccuracy, error or omission, regardless of cause, in the work or for any damages resulting therefrom. McGraw-Hill Education has no responsibility for the content of any information accessed through the work. Under no circumstances shall McGraw-Hill Education and/or its licensors be liable for any indirect, incidental, special, punitive, consequential or similar damages that result from the use of or inability to use the work, even if any of them has been advised of the possibility of such damages. This limitation of liability shall apply to any claim or cause whatsoever whether such claim or cause arises in contract, tort or otherwise.

https://t.me/learningnets

This book is for all the teachers out there snatched from English, social studies, and more, and thrust into teaching IT. You'll do great things!

—Scott Jernigan

https://t.me/learningnets

ABOUT THE AUTHORS

Mike Meyers is the best-selling author of numerous books on computer literacy and certifications, including *CompTIA A+® Certification All-in-One Exam Guide, CompTIA Network+® Certification All-in-One Exam Guide, CompTIA Network+® Guide to Managing and Troubleshooting Networks,* and *Mike Meyers' CompTIA Security+ Certification Guide*. Most consider Mike the leading expert on computer industry certifications. He is the president and founder of Total Seminars, LLC, a major provider of PC and network repair seminars for thousands of organizations throughout the world.
E-mail: michaelm@totalsem.com

Scott Jernigan wields a mighty red pen as the editor in chief of Total Seminars, LLC. With a master of arts degree in medieval history, Scott feels as much at home in the musty archives of London as he does in the crisp monitor glow of Total Seminars' Houston HQ. After fleeing a purely academic life, he dove headfirst into IT, working as an instructor, editor, and writer.

Scott has written, edited, and contributed to dozens of books on computer literacy, hardware, operating systems, networking, and certification, including *Computer Literacy: Your Ticket to IC^3 Certification*. Scott has also taught computer classes all over the United States, including stints at the United Nations in New York and the FBI Academy in Quantico. Practicing what he preaches, Scott has numerous IT certs: CompTIA IT Fundamentals, CompTIA A+, CompTIA Network+, and CompTIA Security+; Microsoft Certified Professional; Microsoft Office User Specialist; and Certiport IC^3.
E-mail: scottj@totalsem.com

Daniel Lachance, CompTIA Cloud+, CompTIA Server+, CompTIA A+, CompTIA Network+, CompTIA Security+, MCT, MCSA, MCITP, MCTS, is the owner of Lachance IT Consulting, Inc., based in Halifax, Nova Scotia. Dan has delivered technical IT training for a wide variety of products for more than 20 years. He has recorded IT support videos related to security and various cloud-computing platforms. Dan has developed custom applications and planned,

https://t.me/learningnets

implemented, troubleshot, and documented various network configurations and conducted network security audits. Dan has worked as a technical editor on a number of certification books and has authored books including *CompTIA Server+ Certification All-in-One Exam Guide (Exam SK0-004)* and *CompTIA Security+ Certification Practice Exams, Second Edition (Exam SY0-401)*.

When not performing with the Halifax-based cover band Clusterfunk, Dan loves being around family and spending time outdoors.

About the Technical Editor

Kenneth "Ken" Hess is a practicing senior system administrator and a technology author, blogger, columnist, editor, and podcaster. Ken has written hundreds of technology articles on topics that cover Linux, open source software, Windows, Mac, mobile devices, databases, and cryptocurrencies. He also reviews technology products and is an avid photographer and filmmaker.

https://t.me/learningnets



Becoming a CompTIA Certified IT Professional Is Easy

Not only is becoming certified easy, it’s the best way to reach greater professional opportunities and rewards.

Why Get CompTIA Certified?

In fact, there are many benefits.

Growing Demand

Some technology fields will experience growth of more than 20 percent by the year 2020, according to a CompTIA information security trends study (“500 U.S. IT and Business Executives Responsible for Security”). CompTIA certification qualifies the skills required to join this workforce.

Higher Salaries

IT professionals with certifications on their résumés command better jobs, earn higher salaries, and have more doors open to new multi-industry opportunities.

Verified Strengths

Ninety-one percent of hiring managers indicate CompTIA certifications are valuable in validating IT expertise, making certification the best way to demonstrate your competency and knowledge to employers (according to CompTIA’s “Employer Perceptions of IT Training and Certification” report).

Universal Skills

CompTIA certifications are vendor neutral, which means certified professionals can proficiently work with an extensive variety of hardware and software found

https://t.me/learningnets

in most organizations.



You can learn more about certification at http://certification.CompTIA.org/certifications/it-fundamentals.

CompTIA Disclaimer

© 2019 CompTIA Properties, LLC, used under license by CompTIA Certifications, LLC. All rights reserved. All certification programs and education related to such programs are operated exclusively by CompTIA Certifications, LLC. CompTIA is a registered trademark of CompTIA Properties, LLC in the U.S. and internationally. Other brands and company names mentioned herein may be trademarks or service marks of CompTIA Properties, LLC or of their respective owners. Reproduction or dissemination of this courseware sheet is prohibited without written consent of CompTIA Properties, LLC. Printed in the U.S. 02544-Mar2016.

The logo of the CompTIA Approved Quality Curriculum Program and the status of this or other training material as “Approved” under the CompTIA Approved Curriculum Program signifies that, in CompTIA’s opinion, such training material covers the content of CompTIA’s related certification exam. CompTIA has not reviewed or approved the accuracy of the contents of this training material and specifically disclaims any warranties of merchantability or fitness for a particular purpose. CompTIA makes no guarantee concerning the success of persons using any such “Approved” or other training material in order

https://t.me/learningnets

to prepare for any CompTIA certification exam.

https://t.me/learningnets

CONTENTS AT A GLANCE

Part I Computer Basics

Chapter 1 How People Use Computers

Chapter 2 System Hardware

Chapter 3 Device Ports and Peripherals

Chapter 4 Data Storage and Sharing

Part II Setting Up and Using Computers

Chapter 5 Understanding Operating Systems

Chapter 6 Setting Up and Configuring a PC

Chapter 7 Setting Up and Configuring a Mobile Device

Chapter 8 Managing Files

Chapter 9 Using and Managing Application Software

Part III Networking, Security, and Maintenance

Chapter 10 Configuring Network and Internet Connectivity

Chapter 11 IT Security Threat Mitigation

Chapter 12 Computer Maintenance and Management

Chapter 13 IT Troubleshooting

Part IV Databases and Software Development

Chapter 14 Understanding Databases

Chapter 15 Developing and Implementing Software

Part V Appendixes

https://t.me/learningnets

Appendix A Exam Objective Reference
Appendix B About the Online Content
Glossary
Index

https://t.me/learningnets

CONTENTS

Acknowledgments
Introduction

Part I Computer Basics

Chapter 1 How People Use Computers

Features Common to Computing Devices
- Internet of Things Devices
- Processors
- Programming
- Data Storage
- Data Assets
- Examples and Two More Definitions

Common General-Purpose Computing Devices
- Multi-user Computers
- Dedicated Computers

Networks: Hooking It All Together
- Servers
- Resource Sharing

Remotely Accessed Computer Systems
- Mobile Apps
- Streaming Media
- Web Apps
- Cloud Computing
- Virtualization

Specialized Computer Systems
- Point-of-Sale Terminals
- ATMs
- GPS

https://t.me/learningnets

VoIP/Telepresence
Chapter Review
Questions
Answers

Chapter 2 System Hardware

CPUs
Speed
Features
Power and Heat Management
RAM
Different Types of RAM in a Computer
RAM Capacity
RAM Technologies and Speeds
Motherboards
Motherboard Form Factors
Motherboard Features
Power Supplies
Chapter Review
Questions
Answers

Chapter 3 Device Ports and Peripherals

Expansion Cards and Slots
Expansion Cards
Expansion Slot Types
Common Ports and Connectors
USB
Other Peripheral Ports and Connectors
Monitors
Monitor Types
Monitor Ports and Connectors
Touchscreens
Standard Input Devices
Keyboards
Pointing Devices

https://t.me/learningnets

Other Common I/O Devices
Audio Devices
Imaging Peripherals
Printers and Fax Machines
Chapter Review
Questions
Answers

Chapter 4 Data Storage and Sharing

Storage Technologies
Magnetic Storage
Optical Storage
Solid-State Storage
Local Storage
Network Storage
Online Storage
Chapter Review
Questions
Answers

Part II Setting Up and Using Computers

Chapter 5 Understanding Operating Systems

The Functions of an Operating System
Operating System Characteristics
Licensing
Software Compatibility
Complexity
Comparing OS Interfaces
The Windows Interface
The macOS Interface
The Linux Interface
The Chrome OS Interface
Cross-Referencing Features
Common Features of Operating Systems
Executing Programs

https://t.me/learningnets

Services
Managing Files
Connecting to Hardware
Connecting to the Internet
Navigating with Hotkeys
Creating Screen Captures
Configuring Accessibility Options
Chapter Review
Questions
Answers

Chapter 6 Setting Up and Configuring a PC

Preparing the Work Area
Evaluating Room Conditions
Choosing Where to Set Up the PC
Making a Work Area More Comfortable
Avoiding ESD and EMI Problems
Ensuring Reliable AC Power
Setting Up a Desktop PC
Physical Connections
Cable Management
Operating System Setup
Completing Post-Setup Tasks
Verify and Configure the Internet Connection
Install Security Software
Run Software and Security Updates
Configure Peripherals
Uninstall Unneeded Software
Install Additional Software
Create More User Accounts
Chapter Review
Questions
Answers

Chapter 7 Setting Up and Configuring a Mobile Device

Mobile Devices: A Quick Overview

https://t.me/learningnets

Setting Up the Device
Understanding the Interface
Using Gestures
Understanding Kinetics
Controlling Screen Orientation
Security Features
Setting and Changing a Lock Passcode
Configuring Account IDs and Passwords
Managing Lost Device Security
Wireless Connectivity
Verifying Wireless Capabilities
Pairing via Bluetooth Devices
Transferring Data with Bluetooth
Connecting to a WiFi Network
Sharing a Phone's Cellular Connection with Other Devices
Disabling All Wireless Connections with Airplane Mode
Configuring Mobile E-mail
Configuring Synchronization
Synchronizing with a Cloud Service
Synchronizing Photos
Synchronizing with a Computer
Installing and Removing Apps
Finding and Installing an App
Removing an App
Resetting a Mobile Device
Performing a Soft Reset
Performing a Hard Reset
Getting Your Data Back After a Hard Reset
Chapter Review
Questions
Answers
Chapter 8 Managing Files
Managing File Storage
Understanding Folders and Paths

https://t.me/learningnets

File Management Tools
Navigating a File Structure
File and Folder Properties
Manipulating Files and Folders
Opening, Editing, and Saving Files
Moving and Copying Files and Folders
Renaming Files and Folders
Deleting and Undeleting Files and Folders
Searching, Sorting, and Displaying Files
Protecting Files
File and Folder Permissions
Backing Up and Restoring Data
Chapter Review
Questions
Answers

Chapter 9 Using and Managing Application Software

Running an Application
Running an Application in Windows
Running an Application in macOS
Running an Application in Linux
Running an Application in Chrome OS
Running an Application on a Smartphone
Switching Between Applications
Saving Your Work
Exiting an Application
Installing, Updating, and Removing Applications
Installing Applications
Updating Applications
Removing Applications
Common Applications and Their Uses
Platforms
Types
Common File Types
Software Licensing

https://t.me/learningnets

Single and Multi-use Licenses
Product Keys and Activation
Chapter Review
Questions
Answers

Part III Networking, Security, and Maintenance

Chapter 10 Configuring Network and Internet Connectivity

Understanding Network Basics
LANs and WANs
Clients and Servers
Switches and Routers
Local Ad Hoc Networks and Direct Links
Setting Up and Configuring a SOHO Router
Choosing an Appropriate Router
Setting Up a SOHO Router
Making a Wired Connection
Checking for Basic Internet Connectivity
Accessing the SOHO Router Configuration Utility
Logging In and Changing the Password
Updating the SOHO Router Firmware
Changing the SSID
Setting Up Wireless Security
Connecting Wireless Clients
Wired, Radio Frequency, Satellite, and Cellular: Making the Right Choice
Mobility
Availability
Throughput/Bandwidth
Connection Delay (Latency)
Reliability
Number of Concurrent Connections
Level of Security
Using a LAN to Share Files and Printers
Enabling File and Printer Sharing

https://t.me/learningnets

Network Organization
Sharing
Installing and Sharing a Printer
Chapter Review
Questions
Answers

Chapter 11 IT Security Threat Mitigation

Understanding Local Security Threats
Unauthorized Access
Data Destruction
Theft
Malware
Physical Security
Access Control
Device Hardening
Users and Passwords
Using Appropriate Account Types
Authenticating Users
User Account Control
Malicious Software
Adware
Spyware
Spam
Social Engineering
Viruses
Trojan Horses
Worms
Ransomware
Protecting Against Malware
Windows Update
Anti-malware Programs
Malware Prevention Tips
Malware Recovery Tips
Network Threats

https://t.me/learningnets

Eavesdropping
Man-in-the-Middle Attacks
Denial-of-Service Attacks
Being a Smart Web User
Understanding the Risks of Public Workstations
Playing Smart with Secure Web Sites
Configuring Browser Security and Privacy Settings
Firewalls
Chapter Review
Questions
Answers

Chapter 12 Computer Maintenance and Management

Power Management Basics
Choose Energy-Efficient Devices
Leave the PC Running
Shut Down the PC
Low-Power Modes
Power Plans
Choosing Actions for Power Buttons or Closing the Lid
Cleaning and Maintaining Computer Hardware
Proper Cleaning Materials
Cleaning Monitors and Removable Media
Cleaning Inside a Desktop PC
Ventilation, Dust, and Moisture Control
Environmentally Aware Computer Disposal
Disaster Recovery
Incident Response
Disaster Recovery Plans
Chapter Review
Questions
Answers

Chapter 13 IT Troubleshooting

Troubleshooting Methodology
Solvable Common Computer Problems

https://t.me/learningnets

No Power
Physical Damage
Won’t Start Up Normally
A Certain App Won’t Install or Run
Apps Run but Sometimes Freeze
Peripherals Won’t Work
Getting Help
Manufacturer Documentation and Web Sites
Technical Support
Internet Searches and Community Groups
Chapter Review
Questions
Answers

Part IV Databases and Software Development

Chapter 14 Understanding Databases

Database Concepts
Database Table Structure
Database Scalability
Database Structures
Relational Databases
NoSQL Databases
Database Creation and Management
Database Connectivity
Database Security
Manipulating Data
Chapter Review
Questions
Answers

Chapter 15 Developing and Implementing Software

Software Development Life Cycle
Requirement Analysis and Planning
Design
Coding

https://t.me/learningnets

Testing
Deployment
Maintenance
Data Types
Constants
Variables
Object-Oriented Programming
Properties
Methods
Program Flow
Conditional Execution
Getting Loopy
Functions
Chapter Review
Questions
Answers

Part V Appendixes

Appendix A Exam Objective Reference

CompTIA IT Fundamentals+

Appendix B About the Online Content

System Requirements
Your Total Seminars Training Hub Account
Single User License Terms and Conditions
TotalTester Online
Mike's Video Training
Technical Support

Glossary

Index

https://t.me/learningnets

ACKNOWLEDGMENTS

Our acquisitions editor, Tim Green, knocked another project out of the park. Thank you for the kind reminders, thoughtful pokes, and occasional thumps on the back of the head. It was truly a pleasure working with you!

Ken Hess caught every little technical error and kept us honest. His knowledge and attention to detail were invaluable.

Claire Yee, our acquisitions coordinator, peppered the days between our Friday meetings with gentle reminders . . . and yes, I promise I'll get that file to you today . . . how about end of day? Nice working with you!

Janet Walden was the editorial supervisor. It was great working with you again.

Rachel Fogelberg did a great job running the team that turned copyedited chapters into the final book. We enjoyed working with you on this and look forward to the next project as well.

To the copy editor, Kim Wimpsett; proofreader, Richard Camp; indexer, Jack Lewis; and layout folks at Cenveo Publisher Services—superb work in every facet. Thank you for being the best.

https://t.me/learningnets

INTRODUCTION

People use computers or computing devices every day to accomplish certain goals. You probably use a smartphone, such as an iPhone or Android device, to make telephone calls, text friends and family, and surf the Internet. You might use a desktop computer, such as a Windows PC, to write papers for school, create documents for work, and e-mail people around the country.

Computers are so common in everything we do that you could argue the modern world would not function without them. Software provides applications that make computers do useful things such as manipulate numbers, store customer records in databases, or predict future weather trends. A general knowledge of software design principles and how databases work goes hand in hand with knowing how to configure computers to meet your needs.

Should people living in a world that can't function without computers know basics such as what computers can do? Should they know how computing devices work and how to set one up once they get home from the store? Should they have a handle on how computers connect to networks such as the Internet? We think the answer is an unqualified *yes*.

This basic body of knowledge about computers and the role they play in our modern lives has various names.

- Information technology (IT) fundamentals
- Computer literacy
- Digital literacy

In many fields, people demonstrate knowledge of subjects by passing tests, passing classes, and getting degrees. In computing, people get certificates (or, more commonly, *certifications*) to prove their skills. The most important general certifying body for computing is CompTIA.

What Is CompTIA?

The Computer Technology Industry Association (CompTIA) is a nonprofit

https://t.me/learningnets

industry trade association based in Oakbrook Terrace, Illinois. It consists of more than 20,000 members in 102 countries. You'll find CompTIA offices in such diverse locales as Amsterdam, Dubai, Johannesburg, Tokyo, and São Paulo.

Virtually every company of consequence in the IT industry is a member of CompTIA. Here are a few of the biggies:

Adobe Systems	AMD	Best Buy	Brother International
Canon	Cisco Systems	Facebook	Fujitsu
Hewlett-Packard	IBM	Intel	Kyocera
McAfee	Microsoft	NCR	Symantec
Toshiba	Total Seminars, LLC (that's our company!)	Xerox	*Plus many thousands more*

CompTIA provides a forum for people in these industries to network (as in meeting people), represents the interests of its members to the government, and provides certifications for many aspects of the computer industry. CompTIA watches the IT industry closely and provides new and updated certifications to meet the ongoing demand from its membership.

CompTIA Certifications

CompTIA certifications enable techs to offer proof of competency in a variety of technology fields. Attaining the CompTIA A+ certification, for example, proves that you're a PC technician of some skill. You know how to build and fix PCs, and you know the basics of networking because modern PCs almost always connect to some network. The CompTIA Network+ certification, in contrast, goes pretty deep into networking. It's designed for network technicians.

Earning a CompTIA A+ or CompTIA Network+ certification takes time and commitment. Most commonly, the successful candidate is a working tech already and wants to prove his or her merit to an employer. But what about people who might want to become a tech but aren't there already?

CompTIA IT Fundamentals+

The CompTIA IT Fundamentals+ certification covers entry-level IT subjects and demonstrates a solid, general knowledge of modern computing devices. The successful candidate can discuss basic computer components and put together a personal computer (PC). The candidate can install software for productivity,

https://t.me/learningnets

connect the computer to a network, and explain basic security. The candidate can communicate the essentials of safety and maintenance. In short, a successful CompTIA IT Fundamentals+ certification recipient can handle a variety of computing devices competently.

People pursue the CompTIA IT Fundamentals+ certification for a couple of reasons. First, CompTIA IT Fundamentals+ establishes a baseline core of computing knowledge for everyone. The certification explores computing devices of all types and thus helps the student learn what is possible.

CompTIA IT Fundamentals+ also creates an entry point for people who think they might want to become a tech. To take the exam successfully, you'll need to understand the concepts and terminology that go with PCs and networks. You'll need a working knowledge of computer components, operating systems, and networks. This is an essential starting point for techs.

The CompTIA IT Fundamentals+ certification, therefore, applies to these two groups:

- People who want to understand modern technology and function well in today's digital world
- Those thinking about becoming a tech

About the Book

We designed the *CompTIA IT Fundamentals+ Certification All-in-One Exam Guide* to address the needs of both sets of these people who want to get the CompTIA IT Fundamentals+ certification. The book approaches topics in plain language, gradually introducing you to terminology and technology.

The chapters in this book are split into four parts.

I. Computer Basics
II. Setting Up and Using Computers
III. Networking, Security, and Maintenance
IV. Databases and Software Development

"Computer Basics" covers what you might expect: the basic components and workings of personal computing devices. Chapters 1–4 teach you how computers work. We cover important jargon, tools, and concepts. You'll learn about the basic hardware and software and how everything works together.

"Setting Up and Using Computers" discusses topics such as how to set up a

https://t.me/learningnets

new PC and work with modern operating systems. In Chapters 5–9, you'll look at working with applications for productivity and managing files and folders. The section also explores the setup and configuration of mobile devices, such as smartphones and tablets.

"Network, Security, and Maintenance" gets at the heart of how to connect devices to the outside world and keep them safely running. Chapter 10 explores local area networking and both wired and wireless Internet connections. Chapter 11 examines local security and online security, where you'll learn about how to protect systems from malware and mad hackers. Chapter 12 focuses on computer maintenance and management including hardware and software updates, and Chapter 13 is all about solving computer-related problems.

"Databases and Software Development" introduces database and software design principles. Chapter 14 discusses relational and NoSQL databases. Chapter 15 shines the spotlight on planning how to build a software solution and dives into some computer programming examples.

Getting the CompTIA IT Fundamentals+ Certification

To get CompTIA IT Fundamentals+ certified, you need to take and pass one 75-question exam within 60 minutes. That's it. Whether you are in London or Los Angeles, you can sign up for the exam online, where you will schedule a time and place to take it. Go to Pearson VUE to get started: www.vue.com.

You'll need to create an account with VUE first. VUE has testing sites all over the world, in cities large and small. You should be able to find one that's convenient to you.

As of this writing, the CompTIA IT Fundamentals+ exam costs USD $119 for non-CompTIA members. You can also purchase discount vouchers from several companies, including our own. Do a Google search for *CompTIA IT Fundamentals+ discount voucher,* or go to our company's site: www.totalsem.com/vouchers.

Once you pass the exam, you'll be CompTIA IT Fundamentals+ certified. If you decide to pursue a career in IT, your next step should be pursuing the CompTIA A+ certification. That's the industry-standard entry point for techs.

If you've studied CompTIA IT Fundamentals+ for knowledge and language but want more user-oriented training, then a lot of other options emerge. Certiport offers an excellent Computer Literacy certification, for example, called IC^3. Microsoft has certifications for each of its Office products, such as Word,

https://t.me/learningnets

Excel, and PowerPoint. You can find many other application-specific certifications as well.

The CompTIA Certification Roadmap makes a great starting point with explanations about tech certifications and some of the suggested pathways to take. The document shows career choices on the right with links to certs along the way. Putting web site links in a printed book means adding lots of corrections over time. Do a Google search for *it-certification-roadmap.pdf* to get the latest version.

Studying for the Exam

We suggest you read the book twice. The first time, read it like a novel. Enjoy the new terms and fun illustrations. Don't try to memorize things yet. On the second read-through, make sure you have a copy of the CompTIA IT Fundamentals+ objectives printed out or on-screen. Read carefully, and check off topics as you cover them.



NOTE There's a map in Appendix A so you know where we cover each objective in the book.

If you have questions or comments, good or bad, feel free to contact us. Here are our e-mail addresses:

scottj@totalsem.com

michaelm@totalsem.com

Good luck with your studies and with the CompTIA IT Fundamentals+ exam!

https://t.me/learningnets

PART I

Computer Basics

- **Chapter 1** How People Use Computers
- **Chapter 2** System Hardware
- **Chapter 3** Device Ports and Peripherals
- **Chapter 4** Data Storage and Sharing

https://t.me/learningnets

CHAPTER 1

How People Use Computers

In this chapter, you will learn how to

- Explain features common to all computing devices
- Describe different types of general-purpose computers
- Explain how computer networks work
- Describe methods of remotely accessing computer systems
- Identify specialized computer systems and their purposes

The marvels that make up life in the 21st century, such as the International Space Station, driverless cars, stunning special effects in movies, and nearly instant access to the collective knowledge of the human race (through the Internet), rely on sophisticated machines called *computers*. A *computer,* or *computing device,* does math breathtakingly fast.

Over the years, some smart people have figured out how to represent just about anything you can see or hear as a series of numbers. Others like them are hard at work on doing the same with anything you can smell, touch, taste, and even think. More specifically, the vast majority of these representations (which we call *data*) are built from massive sequences of ones and zeros.

A fancy calculator that creates stunning movie effects may sound like something out of *Jack and the Beanstalk,* at least before you know that this "data" stuff is really just numbers. Since the sounds and images a computer creates are made of numbers, the computer can change them (or even create them from scratch) by doing a little (okay, a lot of) math.

All of this math is how computers can turn a recording of a bunch of kids pretending to cast spells into a *Harry Potter* film. The wizards better known as *programmers* write commands that use math to change data according to some pattern and collect them into *programs*. In turn, special effects artists (and anyone else who does work on a computer) use programs full of useful commands to coax computing devices into making one kind of magic or another.

https://t.me/learningnets

This chapter first discusses the features of all computing devices and some important terms and labels used to talk about them. Next, the chapter explains common, general-purpose computing devices and then dives into how you and they can work together to do some seriously *Star Trek*–level magic. The chapter finishes with a discussion on specialized computing devices. Knowing computing devices and connections of all types is your first step on the journey to getting CompTIA IT Fundamentals certified. Let's start with magic.

Features Common to Computing Devices

A few practical examples demonstrate the magic you can work with a smartphone (Figure 1-1), such as an Apple iPhone or a Samsung Galaxy. It can cast spells that enable you to do the following:

https://t.me/learningnets



Figure 1-1 Typical smartphones

- Speak with people all around the world from comfortable places like your bed, or a bathroom stall
- Play an awesome, visually stunning game, like *Alto's Adventure* (Figure 1-2)

https://t.me/learningnets



Figure 1-2 *Alto's Adventure* on an Apple iPhone

- Take a high-resolution photograph or video, the latter including pictures and sound, and then send it to anyone with an Internet-connected computing device
- Run a small business
- Join a full-motion, real-time video call (Figure 1-3)

https://t.me/learningnets



Figure 1-3 Making a video call in a program called FaceTime

- View and set residential or commercial environmental conditions through a smartphone app

Not even a century ago, anyone shown a modern smartphone would have *known* it was a magical device. What does this awesome smartphone magic have to do with passing the CompTIA IT Fundamentals exam? The point is that you use computing devices all the time, and while it's fine for users to see them as a little bit magical, IT is all about dispelling this magic and replacing it with knowledge.

When you pay for fuel or groceries, you interact with computers. When you get in a car, for that matter, you're relying on its computer to get you safely from point A to point B. When you sit down in front of a screen running Windows and open Microsoft Word to type a paper for school or a report for work, you're clearly interacting with a computing device (Figure 1-4).

https://t.me/learningnets

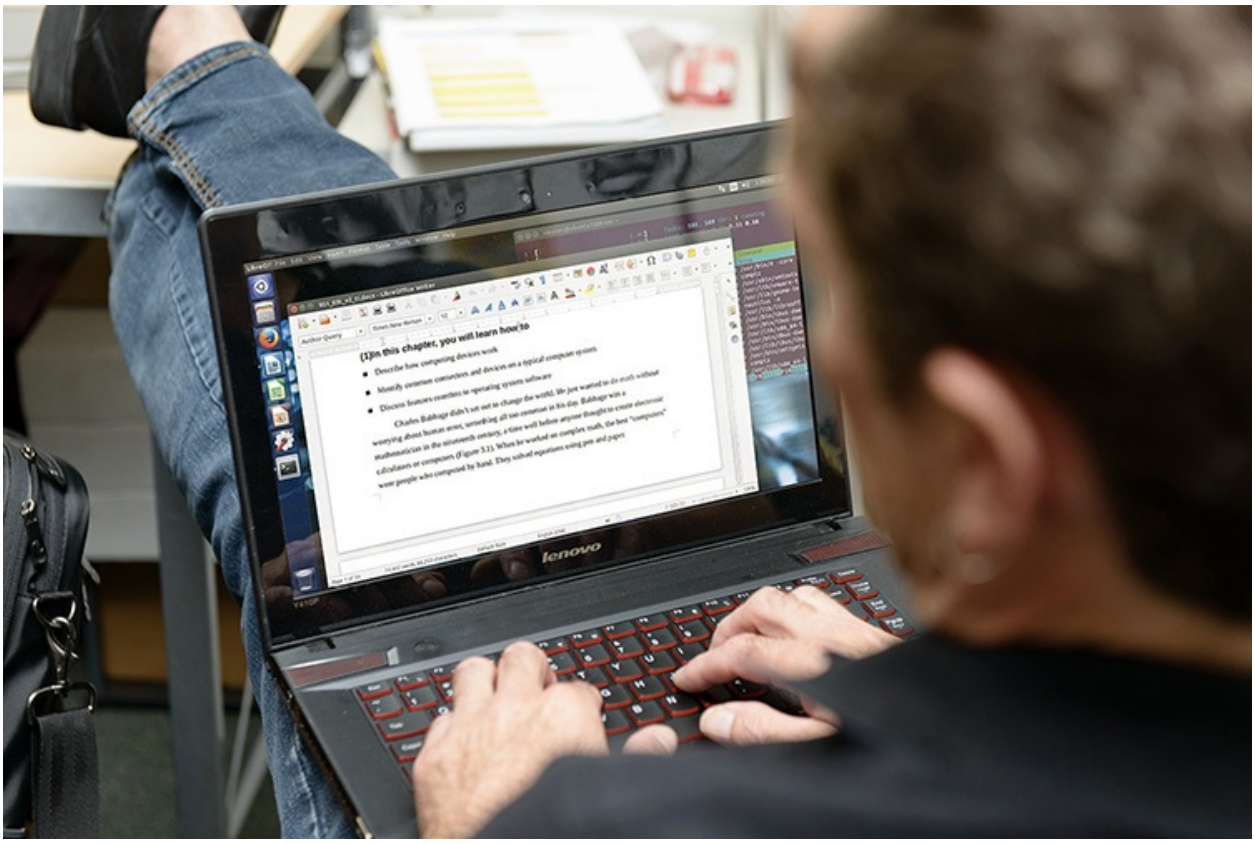


Figure 1-4 Typical computer for school or office work

Where else will you find computers?

- Game systems, such as PlayStation, Wii, and Xbox
- Tablets (like an Apple iPad) and phablets (phone/tablet combinations)
- Digital cameras
- Entertainment hardware, such as digital video recorders (DVRs) and televisions
- Clocks and watches
- Motorcycles
- Appliances, such as refrigerators and washing machines
- Cash registers
- Automatic teller machines (ATMs)
- Manufacturing equipment in factories
- Inventory management systems in warehouses
- Internet of Things (IoT) devices

https://t.me/learningnets

Internet of Things Devices

IoT devices are specialized computing devices that communicate data over the Internet, excluding standard desktops, laptops, servers, and smartphones. These are all IoT device examples:

- Medical devices used for patient monitoring
- Residential and commercial security cameras including doorbell cams
- Smart cars
- Baby monitors
- Residential and commercial environmental control
- Home appliances such as refrigerators
- Amazon Echo/Google Home/Apple HomePod voice-controlled speakers

Sending data from IoT devices can present some security challenges, including the possibility of remote attacker control of an IoT device, but we'll dive into security details in Chapter 11.

Processors

Despite the different roles these devices play, each is driven by one or more super-fast electronic calculators—*processors*—that carry out (or *execute*) computations specified by the device's *programming*. We could go into gory details on how processors work at the microscopic level, but the main things you need to know are that they're all fairly similar and all of these devices use processors to perform work.

Programming

Programming is how programmers control what kind of work these computations accomplish. Programming comes in two forms for computers: operating systems and applications. An *operating system* (OS) enables people to interact with the computing machine. It defines both what commands the system can perform and how you can click, speak, tap, or type to run them. *Applications* (or *apps*) are examples of specialized programming (or *programs*) that enable the computer to accomplish specific tasks.

Data Storage

https://t.me/learningnets

The ability to store huge programs and save vast amounts of data for later use is so foundational to modern computing that it's hard to imagine what the first computers looked like. In the decades before large, high-quality internal *data storage* devices were common, programs and data were often entered by hand, built directly into the device, or recorded as a series of holes punched in paper cards or tape.

These limitations kept programs small and simple for a long time. A *small* modern smartphone app (or even just a picture taken with one) would have easily filled the first commercial data storage systems of the early 1950s and, in today's money, cost thousands of dollars a month to store.



NOTE Data is typically organized into *files*. Each picture, song, movie, or document usually has its own file, though these are often created from many individual files. This book started as a separate file for every chapter and image, and all of these files are later edited together. Programs *can* be a single file, but most modern applications have many files, in which case their programming tells the computer how to combine all of the parts.

Data Assets

Individuals and organizations tend to assign the most value, after people, to their data assets. Data are raw items that can be processed and presented in meaningful ways (called *information* at this point), such as with summaries and reports. Reports can provide a quick way to analyze data that can result in more informed business decisions.

Replacing a failed operating system is easy, but without backups, how do you replace research data, customer transaction data, service sales information, and so on? Not only must enterprises protect the confidentiality of data, but they must also ensure data is available when needed, and when disaster strikes, that data must be quickly recoverable. In many cases, companies must comply with laws and regulations that relate to data capture, collection, and use. An example of this is the Canadian privacy law called the Personal Information Protection and Electronics Documents Act (PIPEDA). Most countries have their own forms of privacy laws.

Some data has unique or artistic properties. This type of data is called *intellectual property* (IP). Examples include the book you are reading right now,

https://t.me/learningnets

car designs, and original music compositions, to name just a few. Authors can protect their artistic expressions with copyrights, whereas inventions can be protected with patents. The primary purpose of some IP is to sell many copies, such as of a digital music file or movie; these are called *digital products*. Trademarks are another aspect of IP; they are a unique design or phrase that identifies a company or product.

Examples and Two More Definitions

There are a few more terms you should understand before we move on, so let's see how they apply to a popular smartphone, the iPhone.

- The iPhone is a computer. It's a device, a piece of *hardware*, meaning it's something you can throw out a window.
- Inside the iPhone is a *processor* that does a lot of the computing/processing work.
- The iPhone runs Apple iOS as its operating system. That's the programming or *software* that gives you screen icons to click, and so on. The operating system provides structure or a framework for everything else.
- FaceTime is an *app*, a program that enables you to accomplish a specific task.

We realize we've already thrown a zillion terms at you, but at least you have a handy reference going forward. Refer to this section as needed until the terms *hardware*, *software*, *processing*, *processor*, *programs*, *programming*, *computing*, and *computing device* have crystallized in your mind. Let's go on.

Common General-Purpose Computing Devices

General-purpose computing devices (those that enable you to do a whole bunch of different things) come in many shapes and sizes. This section looks at multiuser computers and dedicated computers and then goes into detail on the variations among dedicated computers. We'll examine operating systems and mobile variations as well.

Multi-user Computers

A *multi-user computer* can serve more than one person at a time. Mainframes,

https://t.me/learningnets

minicomputers, and supercomputers all fall into this category. Most people use dedicated computing devices these days, but multi-user computers are still useful. All the computerized cash registers in a large retail store, for example, typically connect to a multi-user computer that records transactions and adjusts the store's inventory database so individual registers can't get out of sync.

From their introduction in the 1940s into the 1970s, powerful computers called *mainframes* were widely used in the academic, banking, industrial, and scientific fields. Figure 1-5 shows a military mainframe from the 1960s. Mainframes specialize in multitasking, supporting dozens or even thousands of user sessions (each with its own programs and files) at the same time. Smaller versions of mainframes called *minicomputers* were also popular with businesses that didn't need the full power (and expense) of a mainframe. Mainframes and minicomputers aren't as popular these days because there are cheaper, smaller options available.



Figure 1-5 Military mainframe computer from the 1960s

Supercomputers focus the power of a mainframe computer on a single task, making them arguably the most powerful computers on the planet. Most

https://t.me/learningnets

supercomputers are single large machines with hundreds or thousands of processors working in tandem. Supercomputers tackle big-brained tasks like the following:

- Tallying census results
- Compiling geothermal imaging data
- Determining the answer to life, the universe, and everything

Supercomputers also handle other *essential* processing chores, such as rendering the sophisticated *computer generated imagery* (CGI) effects for movies. CGI enables dinosaurs to roam Jurassic Park, and Spiderman to soar through the skyscrapers of Manhattan using nothing more than webs and spider-enhanced muscle. Like we said, it's *essential* processing.

Dedicated Computers

For decades, multi-user computers enabled users to perform computing chores from the simple, such as composing documents, to the complex. Starting in the 1970s, *dedicated computers*—those meant for one user at a time—gradually replaced multi-user computers for just about every computing task. The most common dedicated computer these days is called a PC.

A typical *personal computer* (PC) runs the Microsoft Windows operating system, for example, and comes with certain *peripherals*—devices that enable you to interact with the machine, such as a keyboard, mouse, and monitor (Figure 1-6). PCs have their own computing power and storage capabilities, so you can do work without connecting to any other computing device. Even though a PC is dedicated computer, multiple users can certainly take turns.

https://t.me/learningnets



Figure 1-6 Typical PC with a few peripherals



NOTE PCs are sometimes referred to as *microcomputers* because they're so much smaller than mainframes and minicomputers.

Personal computers can be linked together in a computer *network* that enables them to communicate and share resources. In a network environment, processing power is still in the hands of each networked device, but data storage can be centralized on a single computer that all the other computers can access called a *file server,* making it easier for each PC to manage and back up data files.

PCs vary according to capabilities but also in their level of portability. This relates to both the size and the ease with which the entire computer can be packed up and transported.

Desktop and Laptop Computers

PCs that aren't easily transportable are known as *desktop computers* or *desktops PCs,* and PCs that are transportable are called *laptops* (or *notebooks*). A desktop computer typically has a separate display (though some have built-in monitors), with its own power cord and separate keyboard and mouse components. You can also connect other devices (or *peripherals*) such as a printer, a webcam, or a

https://t.me/learningnets

scanner.

Desktop PCs come in many shapes and sizes, from the metal box you've seen in offices, schools, and homes (see Figure 1-7) to exotic-looking creations with blinking lights, transparent cases, custom paint jobs, and other stylistic touches (see Figure 1-8).



Figure 1-7 Regular PC

https://t.me/learningnets



Figure 1-8 Fancy PC

A *laptop* computer typically has all essential components built into a single package. The laptop monitor, for example, folds down to cover the keyboard for transport. Instead of a mouse, most laptops have a touchpad or some other built-in pointing device. Some of them also have a touch-sensitive screen (a *touchscreen*) that enables users to control the device with their fingertips. Laptops PCs are often called *notebooks* because they approximate the size and shape of a paper notebook.

There are many related terms for variations on this theme. Small laptop PCs are sometimes called *subnotebooks*, for example, and thin, powerful, high-quality laptop PCs are called *ultrabooks*. Figure 1-9 shows a standard-sized laptop, and Figure 1-10 shows an ultrabook.

https://t.me/learningnets



Figure 1-9 Laptop



Figure 1-10 Ultrabook

Chapters 2, 3, and 4 cover specific hardware components in desktop and laptop PCs, and Chapter 6 explains how to set up and configure desktop and laptop PCs.

Operating Systems for Desktop and Laptop PCs

A computer's OS runs the device, supports its applications, and defines how users can interact with it. You can think about an OS as a *software foundation*, the piece of the computing device upon which everything else builds. With more than 90 percent of the market, the most popular OS for desktop and laptop PCs is

https://t.me/learningnets

by far Microsoft Windows. You can find several other operating systems in the market that offer contrasting strengths.

Hardware Platform Your choice of OS depends on the capabilities of your computer's hardware; not every PC can run every operating system. The hardware on which an OS runs is known as the *platform* (though the term *platform* applies to more than just hardware).

The standard platform that runs the Windows OS has a lot of nicknames: *IBM-compatible platform, IBM platform,* or *Intel platform.* IBM was the company that made the first popular personal computers (that used a text-based operating system called MS-DOS). Intel provided the processors for the platform. This platform today can also run a free OS known as Linux or a small and efficient variant of it called Google Chrome OS.

Apple makes both the hardware and the OS for the *Macintosh platform*. Early Macs had proprietary hardware that would run only Apple's OS, but today most Macs use the same Intel-manufactured CPUs as Intel-platform PCs. As a consequence, most Macs can also use a utility called Boot Camp to run Windows.

GUI vs. Command Line Most common operating systems have both a *graphical user interface* (GUI) and a *command-line interface* (CLI). A graphical user interface displays pictures on a monitor, and the user interacts with the pictures by moving a mouse or other pointing device. GUIs are popular because they are easy to use and require little training or memorization of commands. Users interact with a CLI by typing commands at a text-based on-screen prompt.

In operating systems where both interfaces are available, the CLI appears in a window within the GUI. Figure 1-11 shows command prompt windows in Windows (top) and Linux (bottom). The commands used to perform the same actions differ between Linux and Windows, although you can accomplish the same tasks in each OS.

https://t.me/learningnets

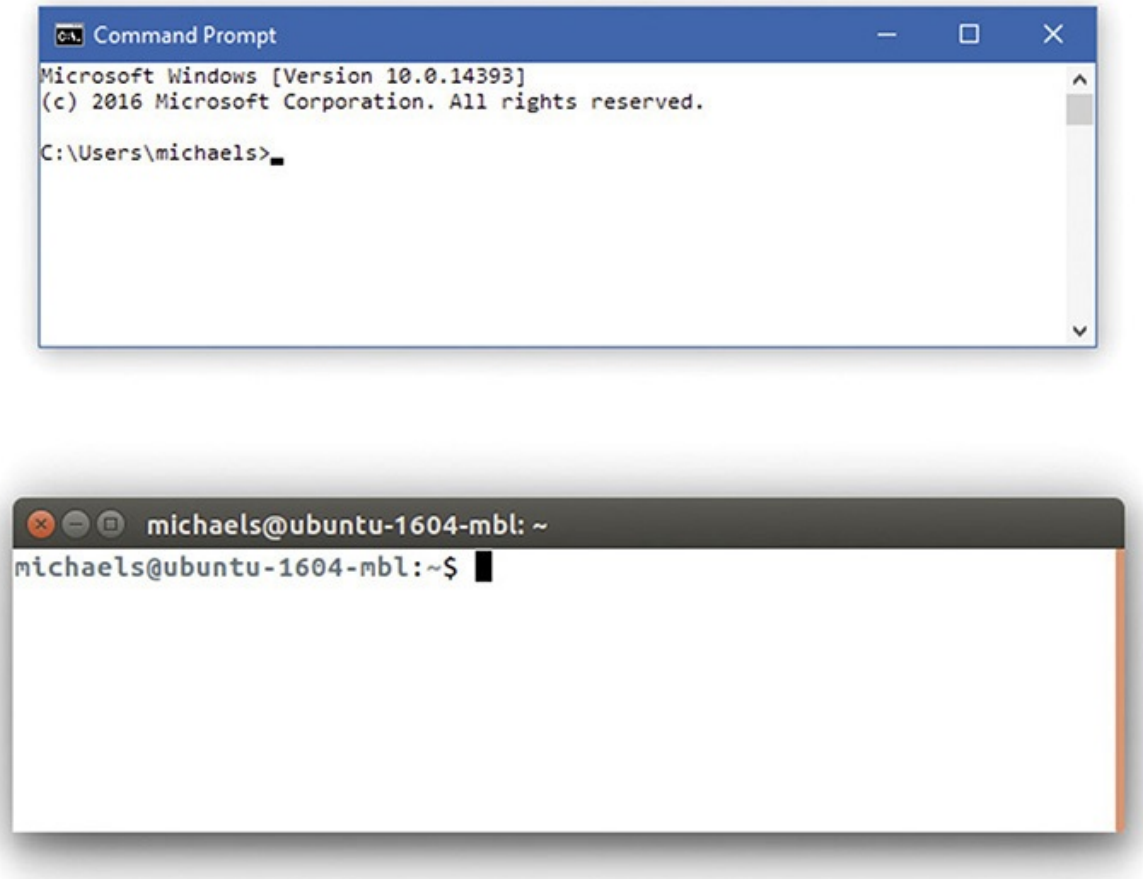


Figure 1-11 Windows (top) and Linux (bottom) command-line interfaces



NOTE macOS has a command-line interface that uses the same basic command set as Linux.

The following sections introduce the major operating systems available today. Chapter 5 looks at them in more detail.

Microsoft Windows The Microsoft Windows OS, shown in Figure 1-12, runs on both desktops and laptops. Microsoft makes Windows editions for smaller devices such as tablets and smartphones; these are "Windows" in name, but they differ a lot from the desktop versions (we'll look at them later in the chapter).

https://t.me/learningnets

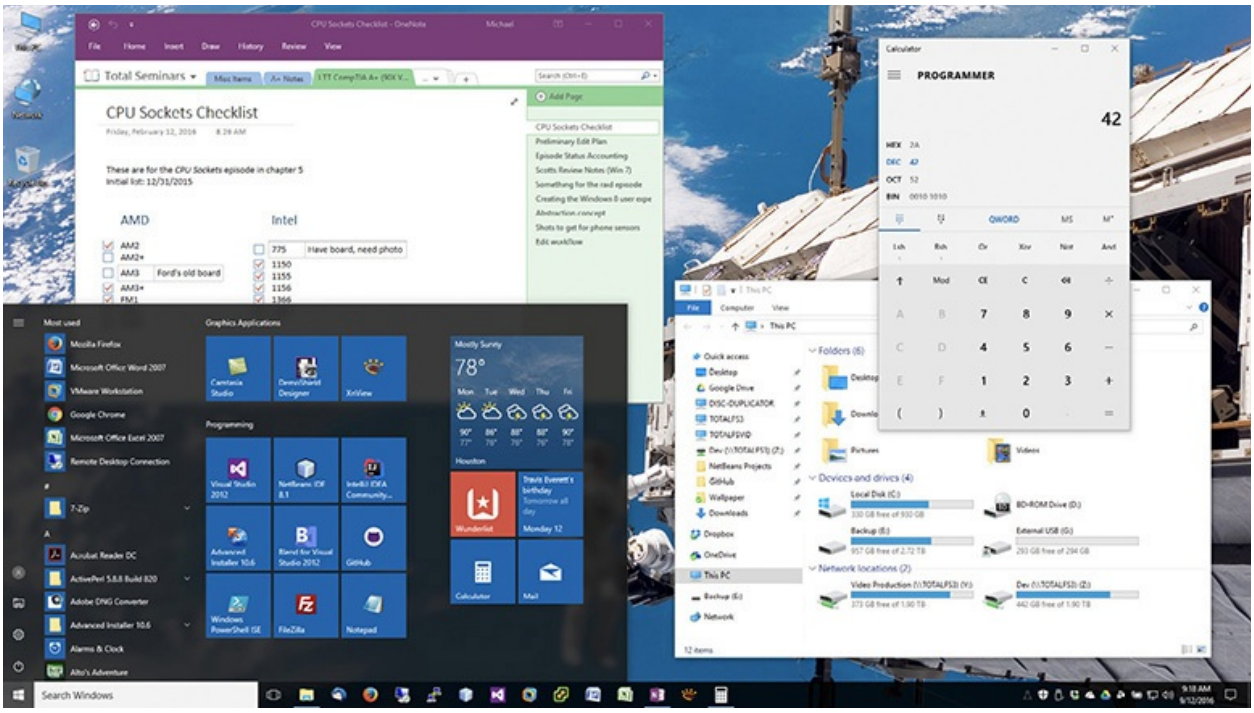


Figure 1-12 Microsoft Windows 10

Windows enables you to connect to the Internet and other networks, run applications, manage files, and do just about anything you might want to do with a computer. The current version is Windows 10, but you may encounter other, older versions as well, including Windows Vista, Windows 7, and Windows 8.1.

Apple macOS The *Apple Mac* (formerly *Macintosh*) computer offers an alternative to Windows-based computers. Figure 1-13 shows a typical Apple Mac. Macs use Apple's own operating system, which Apple renamed from *OS X* (see Figure 1-14) to *macOS* in 2016. Macs can tackle the same tasks as PCs but are more common in creative fields such as music, video, and the graphic arts.

https://t.me/learningnets



Figure 1-13 Apple iMac

https://t.me/learningnets

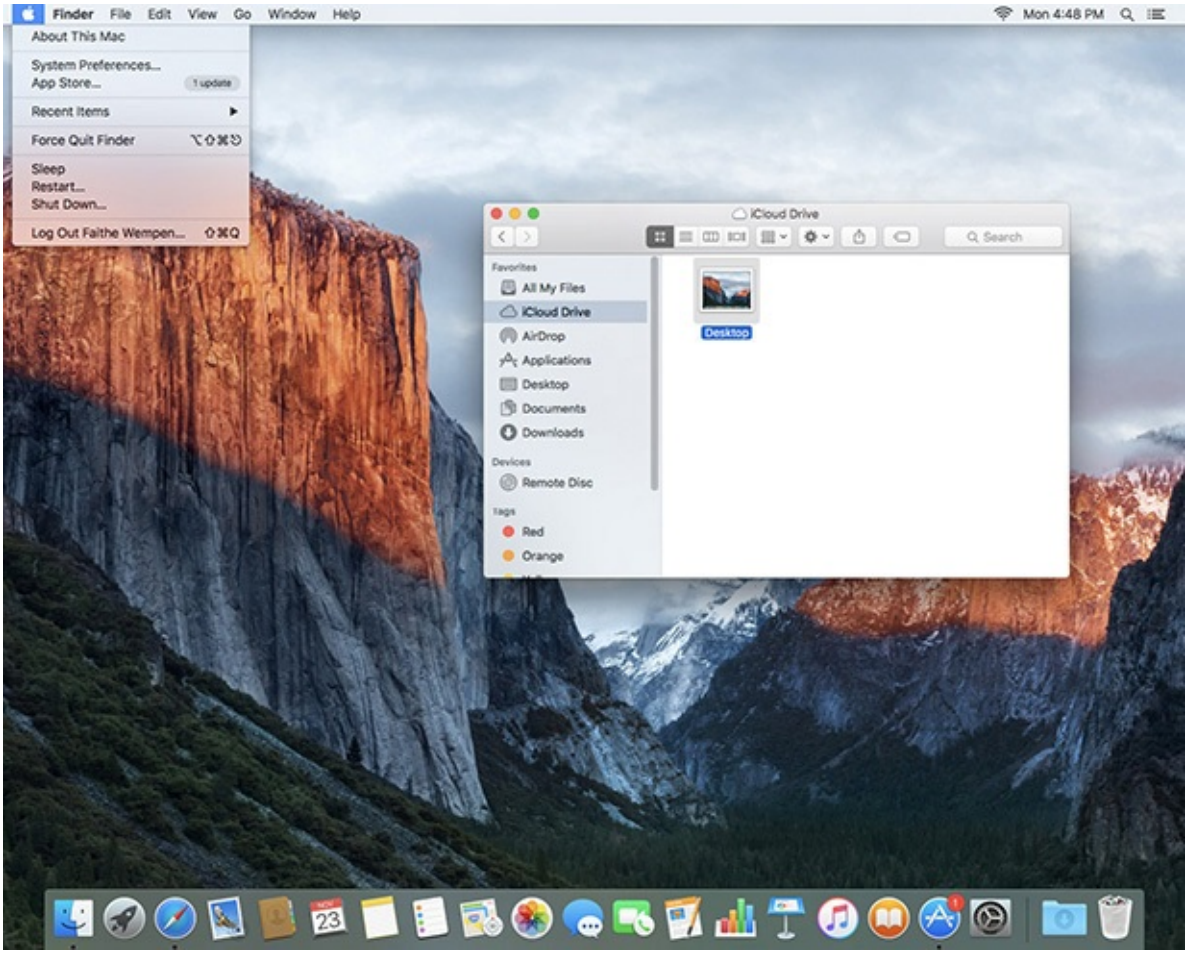


Figure 1-14 OS X desktop

Macs require macOS-specific software. You can't run (or even install) an app designed for Windows in macOS. Programming companies often make apps for both platforms; you need to install the compatible version. Figure 1-15 shows OS-specific versions of an application.

https://t.me/learningnets

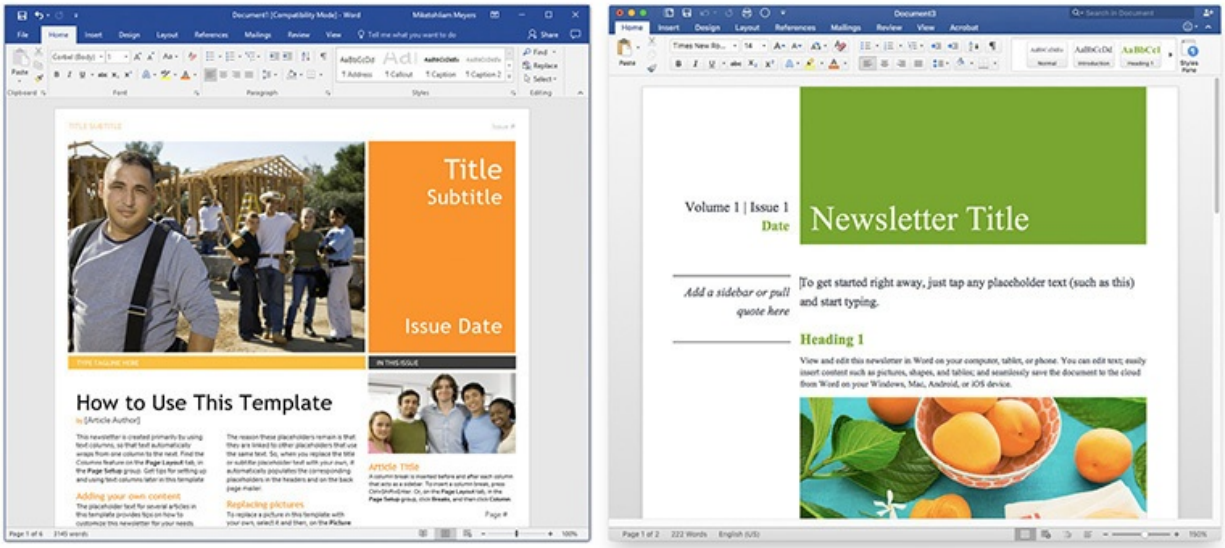


Figure 1-15 Microsoft Word comes in both Windows and macOS versions.

Linux Linux is a variant of a much older operating system, UNIX, which started as a command-line operating system used on servers. It is a free, *open source* operating system, meaning that anyone can download and modify the source code (assuming you know how to program). You can find versions of Linux tailored for just about any kind of computer system.



EXAM TIP Open source software is usually free (you may have to pay to license some software for business use), but the important part is that anyone can make changes and release this new version to the public. In contrast, commercial software like Windows is owned by a company or individual who retains all rights to make, modify, and sell it.

A version of Linux packaged with add-ons and utilities suitable for a particular purpose is called a distribution, or *distro*. Different distros have their own user interface known as a *desktop environment* (DE). One of the most popular distros for personal computers is Ubuntu Linux; you can download it for free online. Figure 1-16 shows the Ubuntu Linux graphical interface. Other popular operating systems such as Chrome OS are based on Linux, but these typically come with their own unique interface and many other modifications.

https://t.me/learningnets

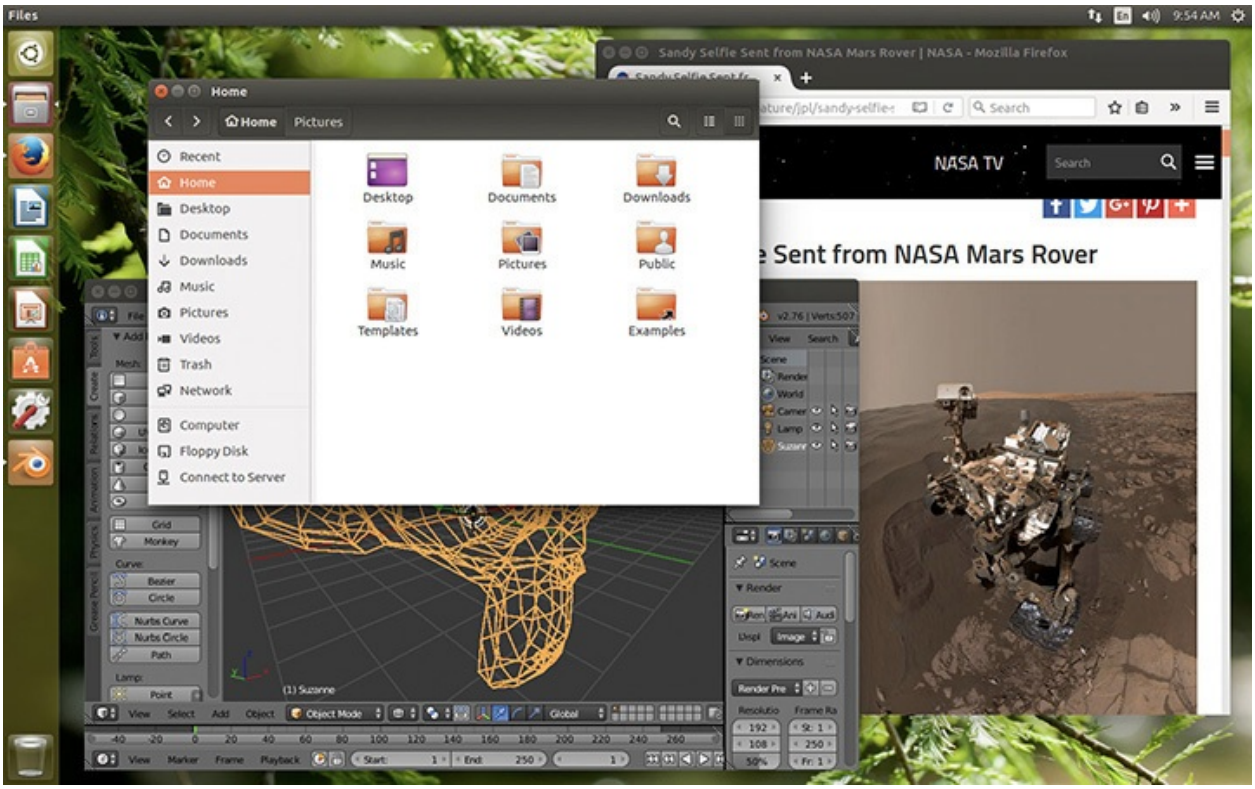


Figure 1-16 The Ubuntu Linux GUI



NOTE Check out Ubuntu's web site (www.ubuntu.com) to download a free version of Ubuntu Linux.

Chrome OS Chrome OS is a Linux variant designed by Google for *thin client* systems (minimally equipped PCs designed primarily for Internet usage, in contrast with fully equipped *thick clients*). Chrome OS is not a viable replacement for a full-featured operating system like Microsoft Windows because it lacks the ability to run desktop applications such as Microsoft Office. If you want to run applications under Chrome OS, you have to use web-based versions of them, such as the Office Online apps at www.office.com.

Mobile Computing Devices

Mobile devices, as the name implies, are made for use on the go and are therefore smaller and lighter than desktop and laptop systems. (Technically, yes, laptops are mobile too, but since they run desktop operating systems and have

https://t.me/learningnets

similar capabilities, we addressed them earlier in the chapter along with desktops.)

Handheld devices have a small touch-sensitive screen that acts as both an input and output device. Modern devices often have touchscreens with virtual keyboards that pop up on-screen when needed, though a few devices (such as the BlackBerry in Figure 1-17) still use integrated hardware keyboards.



Figure 1-17 BlackBerry

The two major types of mobile device available today are smartphones and tablets. Other kinds of device (such as digital music players, e-book readers, and personal organizers) have been popular in the past, but their popularity faded when smartphones and tablets got good enough at their jobs.

Smartphones Smartphones are not just mobile phones; they're tiny computers

https://t.me/learningnets

that help you stay connected by enabling you to access the Internet on the go. They also help you stay organized by giving you a way to copy and carry around data that you'd normally store on your PC, such as your address book, calendar, task lists, and so on.

Most smartphones have enough processing power to allow you to play games, edit text documents and spreadsheets, read books, listen to music, and do many other computing tasks on the go. The most common way to categorize smartphones is by OS (more on each in a moment), leaving us with iPhones (iOS), Androids, and Windows Phones. Figure 1-18 shows an iPhone.



Figure 1-18 Apple iPhone

Tablets A *tablet* is a digital slate with a touchscreen (see Figure 1-19). It resembles an extra-large smartphone, but most don't have cell phone functionality. (A tablet that does have cell phone capability is called a *phablet*.)

https://t.me/learningnets

A tablet fills a niche between the pocket-size portability of a smartphone and the computing power of a laptop. The iPad is the world's most popular tablet, using the same iOS operating system as the iPhone; other 20alternatives include a variety of tablets that use the Android operating system, such as the Samsung Galaxy Tab.

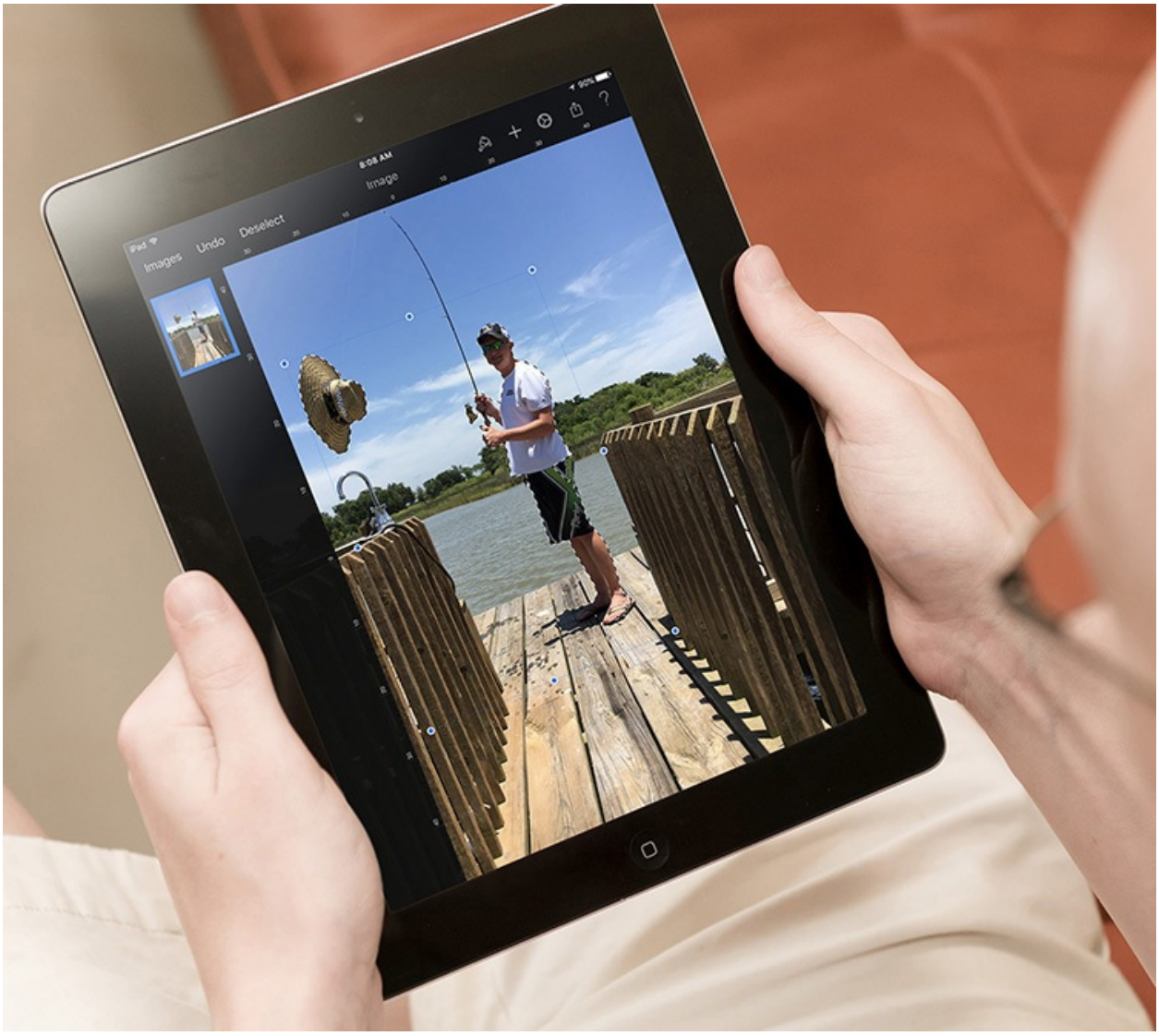


Figure 1-19 Apple iPad



NOTE Microsoft's Surface and Surface Pro tablets feature a detachable keyboard, blurring the line between laptop and tablet (inspiring some to call

https://t.me/learningnets

them *laplets*). These still use the full workstation (desktop and laptop) version of Windows, so it's best to think of them as laptops that can pass as tablets.

Specialty Mobile Devices The trick with specialty mobile devices is that they tend to be popular for some specific task until the hardware and apps on generic mobile devices like smartphones or tablets get *good enough* for the average user to prefer the app over carrying another device.

E-book readers (such as Amazon Kindle or Barnes & Noble Nook), which are basically tablets specialized for reading e-books, enable you to carry the equivalent of a small library in your pocket. They have nice touches like long battery life and screens that cause less eye strain and don't wash out in sunlight.

If number crunching is your thing, a modern *scientific calculator* puts more raw processing power into an index card–sized shell than the first mainframes could boast. Calculators are available with video screens that enable you to graph complex equations, but so can a smartphone app.

Devices with *global positioning system* (GPS) receivers enable you to pinpoint your physical location and help you find your way around. Many smartphones and automobiles now offer GPS capabilities, so having a separate GPS device has become less desirable for navigating roads and cities on foot or by car. Some separate GPS devices have features that make them essential for activities such as sailing or extended backpacking trips.

Operating Systems for Mobile Devices

Many companies make smartphones and tablets, but almost all models use one of four operating systems optimized for mobile use: Apple iOS, Android, Windows Phone, and BlackBerry OS.

Whereas most desktop and laptop operating system interfaces have icons, menus, and windows that you access with a mouse, most mobile operating system interfaces have icons and full-screen applications that you access by tapping the touch-sensitive screen.

Operating systems are built into mobile devices, stored in *nonvolatile memory* (memory that retains its content when the computer is off). A mobile device ships with a dedicated OS and you cannot change to a different OS, although you can install updates.

Apple iOS Apple iOS (shown in Figure 1-20) works the same way across the iPhone and iPad, even though the screen sizes differ. iOS is available only on Apple hardware; it does not run on any third-party devices.

https://t.me/learningnets

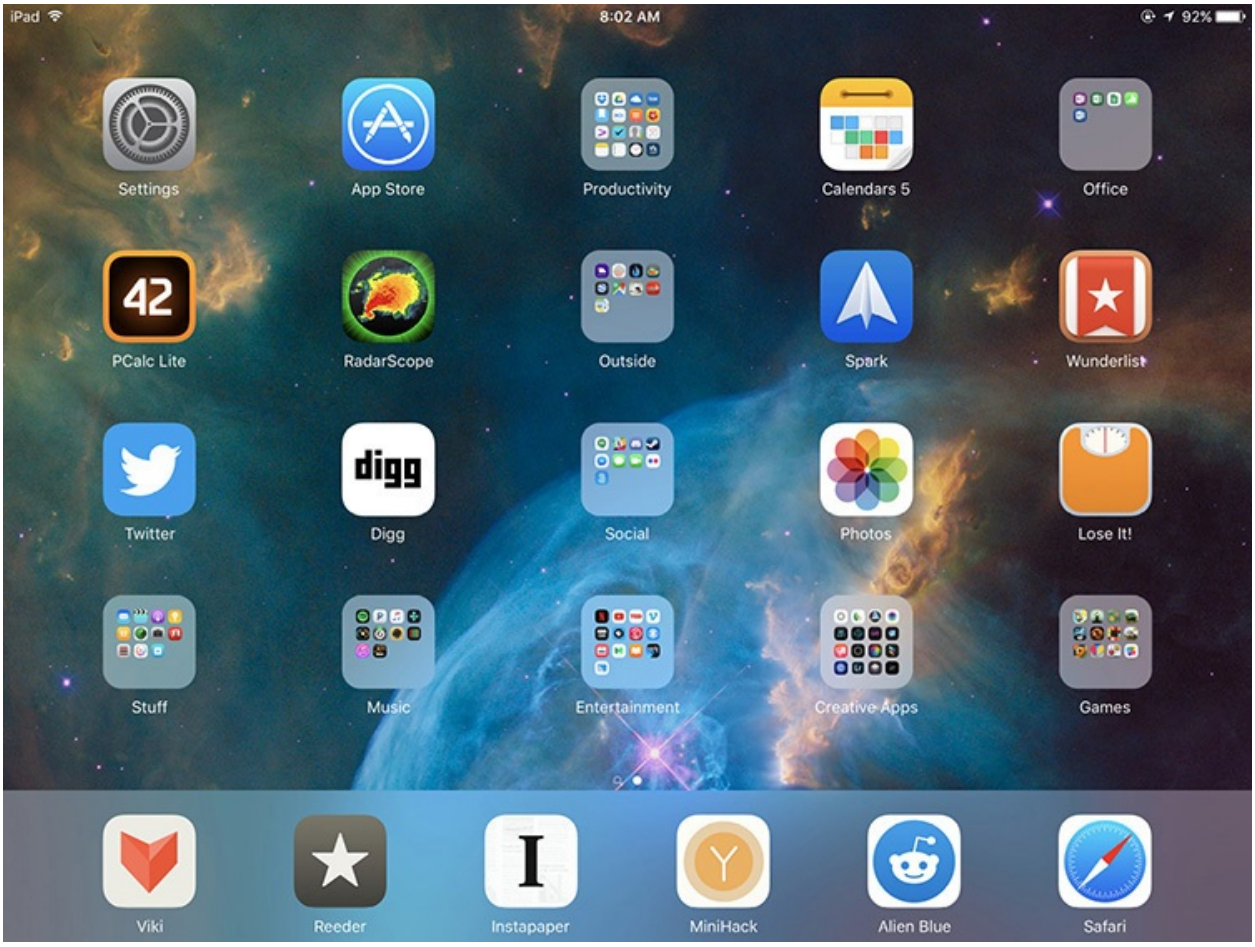


Figure 1-20 The Apple iOS operating system on an iPad

Android Google designed the Android OS—a variant of Linux—for mobile devices. Many lower-cost phones and tablets employ the free and open source Android OS. Android works on the same basic interface design as iOS, with icons arranged on a home screen. Most apps available for iOS are also available in Android versions. Figure 1-21 shows the Android OS on a smartphone.

https://t.me/learningnets

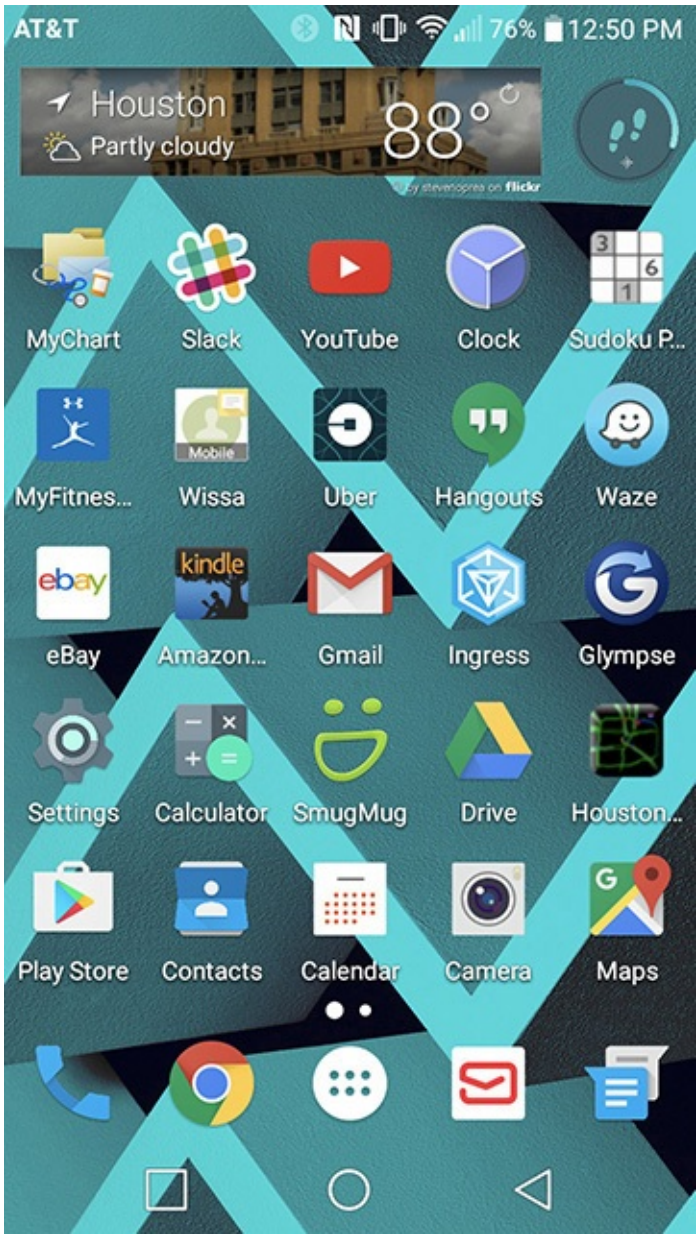


Figure 1-21 The Android operating system

Windows Phone Microsoft produces Windows Phone (see Figure 1-22) as a mobile-device version of Microsoft Windows. The Windows Phone main screen features resizable rectangular tiles, and you can make the tiles larger for applications you use most. Windows Phone has not been as widely adopted as iOS or Android; thus, fewer developers create versions of their apps for it. Microsoft licenses the Windows Phone OS to several different hardware manufacturers, so you'll find it on a variety of smartphones. A tablet version called Windows RT was available for a time, but it has been discontinued;

https://t.me/learningnets

current Windows-based tablets use Windows 10 Mobile, a mobile-friendly version of Windows 10 (note the name change from *Phone* to *Mobile*).



Figure 1-22 The Windows Phone operating system

BlackBerry The BlackBerry OS is a proprietary OS used only on BlackBerry smartphone hardware. Its parent company has recently announced that it will release only limited updates to the BlackBerry OS; BlackBerry has lost its market share in recent years and is not expected to be further developed. You'll likely encounter BlackBerry today only on exams.

https://t.me/learningnets

Networks: Hooking It All Together

Whenever two or more computers communicate, a *network* occurs. This section covers some basic concepts about networks; we'll get to more details in Chapter 10.

Networks come in a couple of flavors, named to describe their location and scope:

- A *local area network* (LAN) connects computers in a single physical location, such as a school, office, or home.
- Two or more LANs connect to form a *wide area network* (WAN).

Computers in a wired LAN connect through network cabling and connection boxes called *switches* (see Figure 1-23). Wireless LANs use radio waves instead of physical *network cables* to connect PCs. Computers on wireless networks connect through a special wireless connection box called a *wireless access point* (WAP). Some types of switch enable the computers to also communicate with other networks beyond the local one; these are called *routers*. A typical *small office/home office* (SOHO) network uses a SOHO router to enable the local computers to communicate with one another and to share a single Internet connection among them.

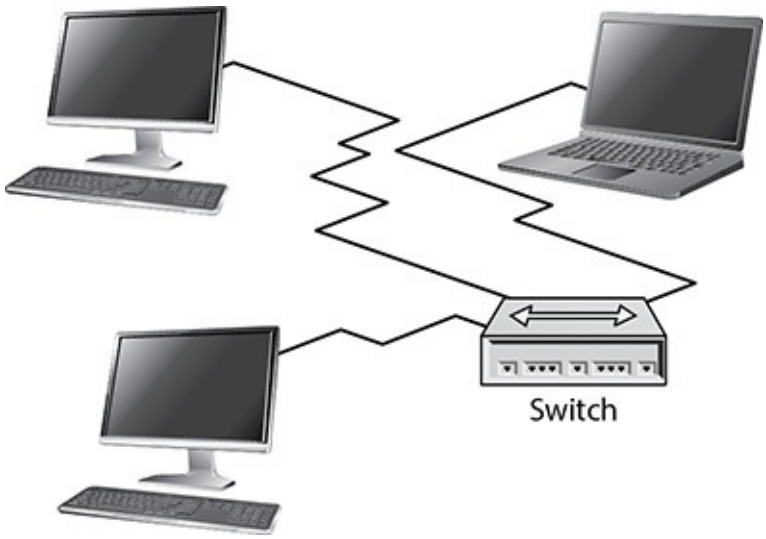


Figure 1-23 Typical LAN

WANs are generally a collection of LANs in multiple buildings or multiple

https://t.me/learningnets

cities, which is why you'll occasionally hear them described as *remote networks*. The best example of a remote network is the *Internet*—a worldwide network of remote networks connected by a series of high-speed communication lines (see Figure 1-24). Other examples of remote networks are school or office networks that enable you to connect to them from home or on the road.

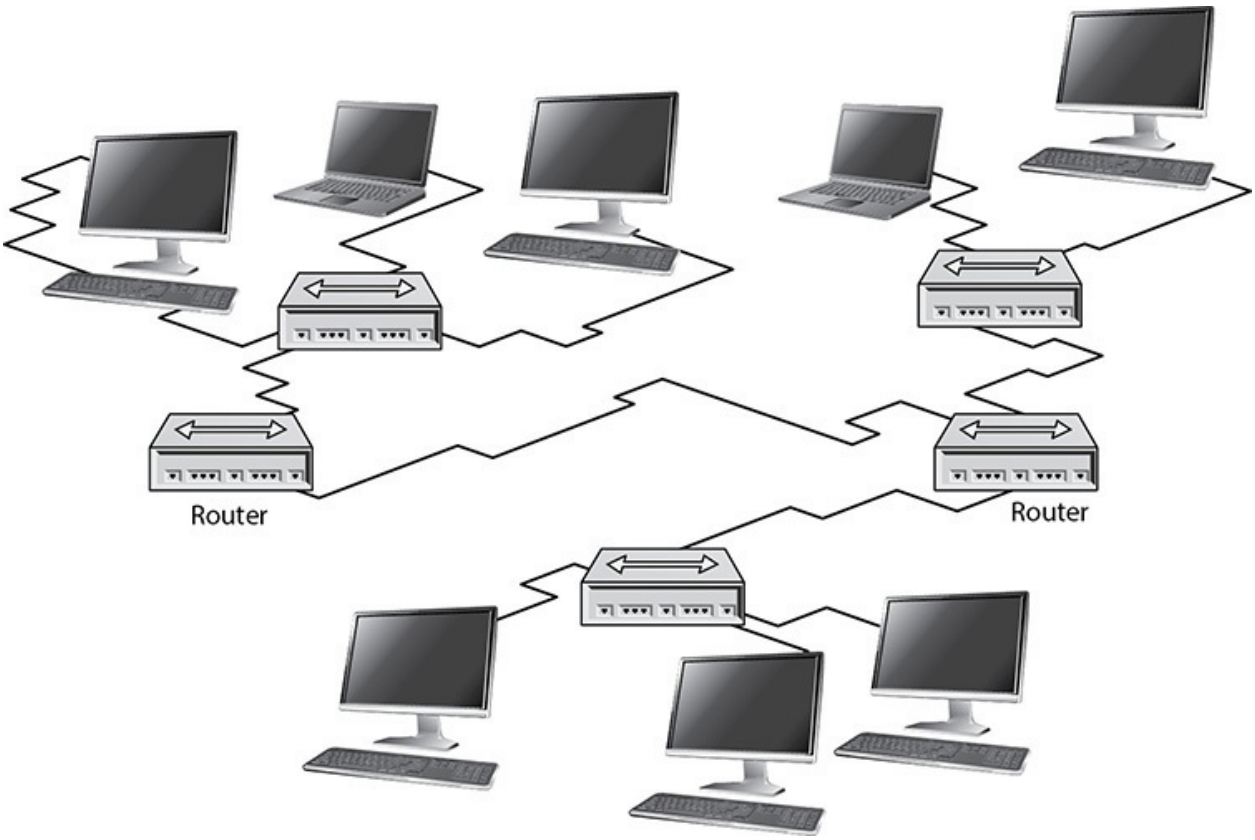


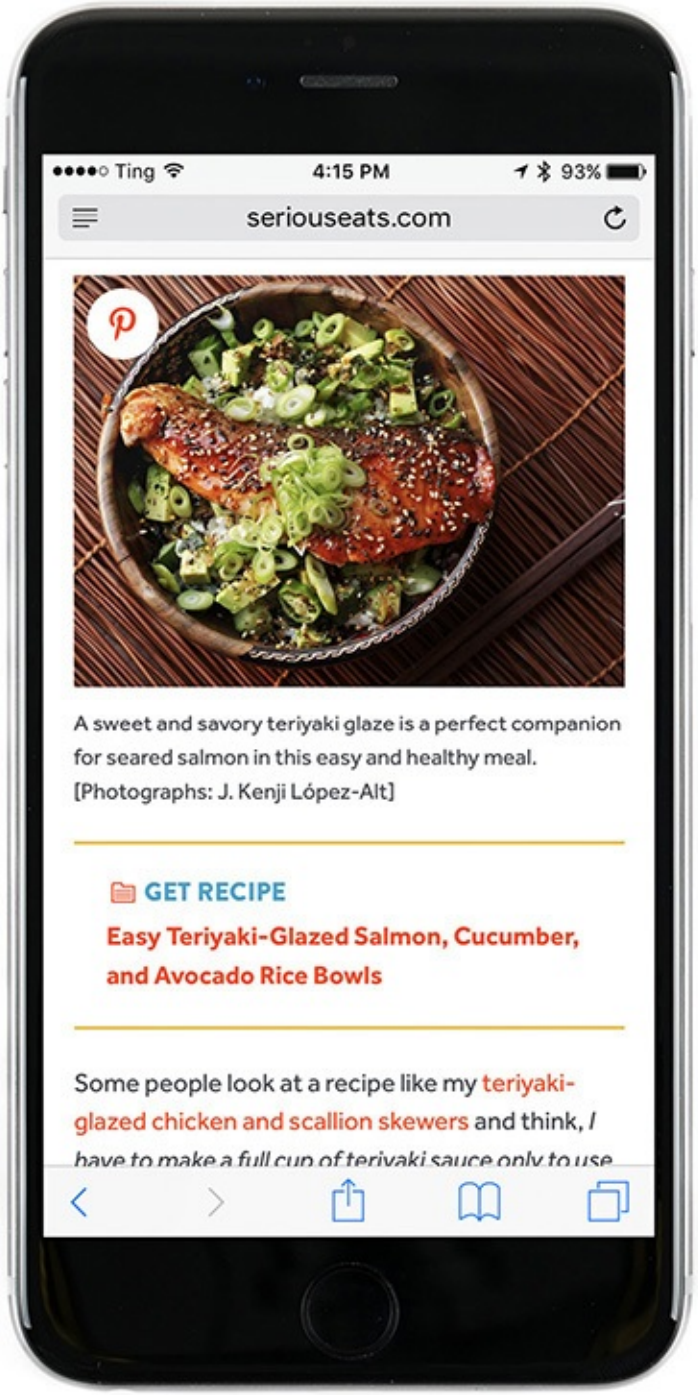
Figure 1-24 Typical WAN

Single computers and LANs connect to WANs such as the Internet through wired or wireless hardware devices called *routers*. Routers send network communications out through the following:

- Regular telephone lines
- Digital subscriber line (DSL) connections
- Cable television lines
- Special dedicated network cabling with exotic-sounding names like ISDN, T1, and T3

https://t.me/learningnets

Handheld devices such as tablets and smartphones can connect to the Internet wirelessly (see Figure 1-25). Even advanced gaming consoles, such as Xbox One and PlayStation 4, offer Internet connectivity for the special purpose of smacking your friends and neighbors in computer games online.



https://t.me/learningnets

Figure 1-25 Apple iPhone surfing the Net

Servers

Manufacturers produce microcomputers to fulfill specific roles on computer networks, such as storing and sharing data or application programs from a central location or providing network services such as e-mail and printing. We usually label these specialized systems—called *servers*—based on what they serve: files, applications, mail, print services, and so on. PCs that receive services from server systems are called *clients*. A well-equipped desktop PC can act as a server, provided you install server software on it; servers can also be much more powerful than a desktop PC, and groups of servers can work together to handle the computing tasks of businesses or web sites.

Resource Sharing

Decentralized networks enable computers to share storage space, printers, scanners, application programs, and, in special cases, even processing power. Sharing one printer is much cheaper than installing ten separate printers on ten separate computers. All modern operating systems enable you to share resources with a few clicks (see Figure 1-26). You'll learn how to share files and printers on a network in Chapter 10.

https://t.me/learningnets

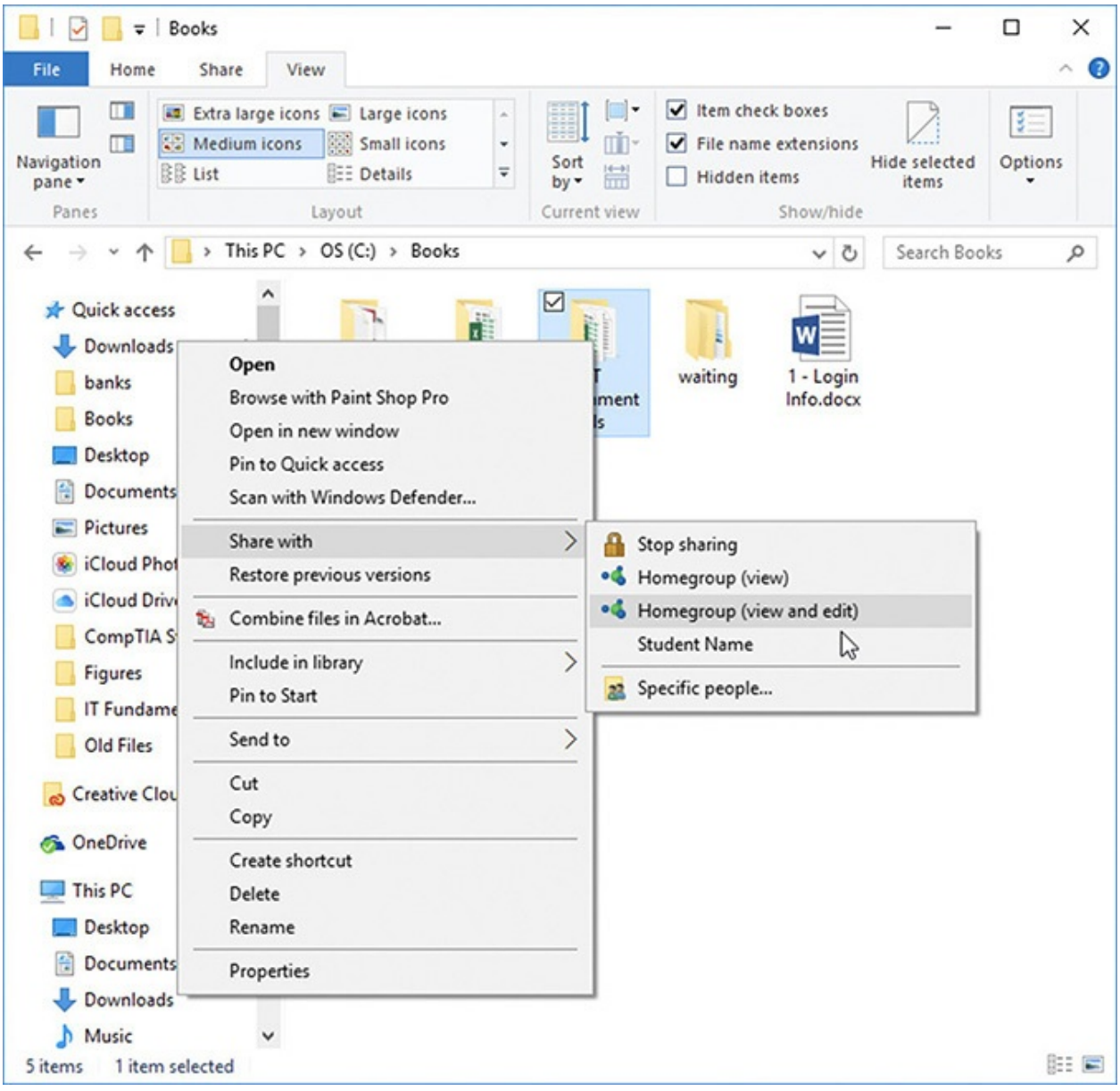


Figure 1-26 Sharing a folder in Windows

Remotely Accessed Computer Systems

Earlier in the chapter you learned about mainframes, which users accessed via *dumb terminals*—a keyboard and monitor connected to a device that had no processing power, just connection points. The mainframe did the processing, in other words, and the terminal simply provided the input and output devices for the user and the communication medium to access the mainframe. This same principle is at work in modern remotely accessed systems. A big, high-capability computer exists somewhere (the *server*), and other computers (the *clients*)

https://t.me/learningnets

located elsewhere access it through the Internet or a private network.

Clients access servers for a variety of reasons. At the simplest level, a client accesses a file server to share files; the server functions like an external *hard drive* (a device for storing data). Remote access can be much more than that, however, as you will learn in the following sections.

Mobile Apps

Mobile apps are simple applications that run on smartphones and tablets. Mobile apps come from online stores maintained by the same company that makes the operating system (Apple Store for Apple devices, Windows Store for Windows devices, and so on). Having all apps come from a single store helps ensure they are virus-free and compatible with the OS.

Some mobile apps run alone on the device, but most connect to servers on the Internet. The app itself provides a basic user interface through which the user can interact with data from the server. For example, a smartphone weather app, like the one in Figure 1-27, retrieves current local weather data from a server and drops it into placeholders on the app screen. Although the app itself resides on the phone, it is useless without a connection to the server.

https://t.me/learningnets

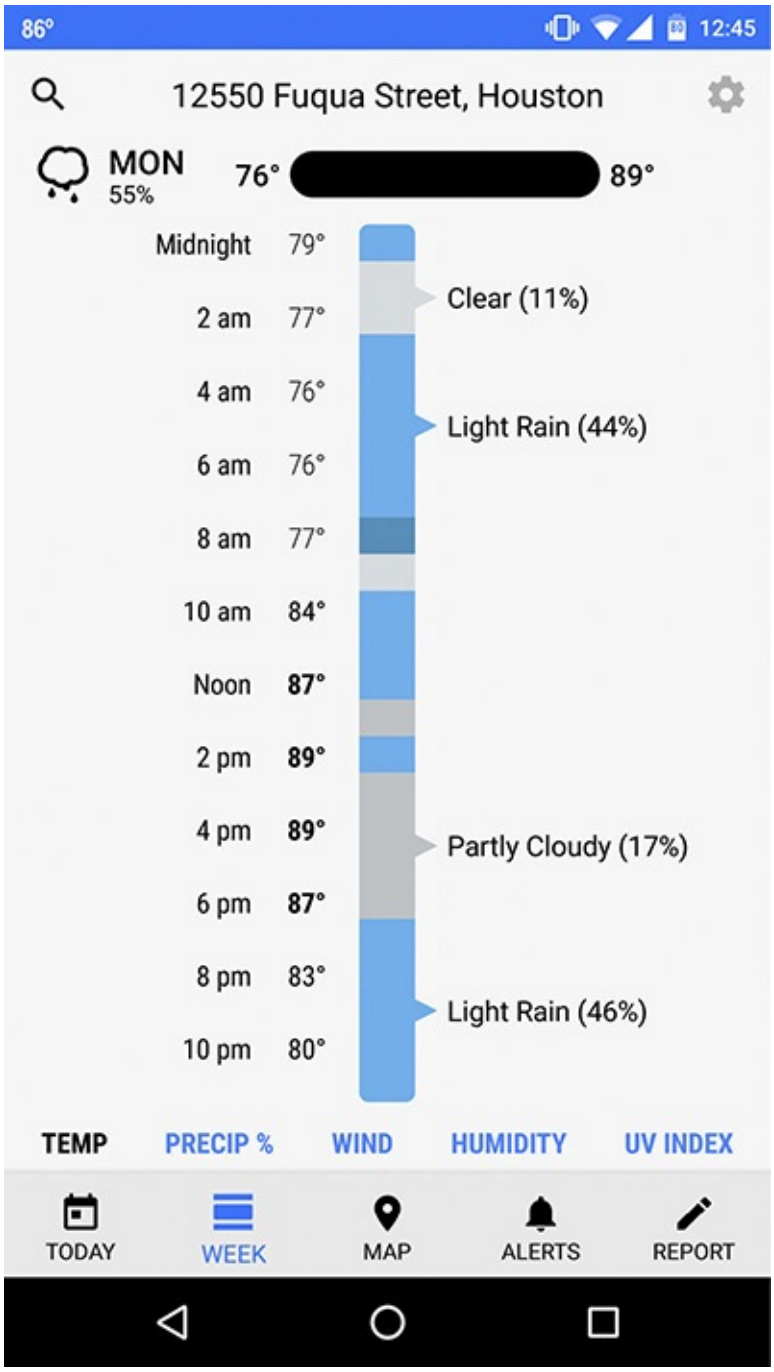


Figure 1-27 This weather app formats and displays weather data from an online server.

Streaming Media

When you *download* a music or video clip, the file transfers permanently to your local computing device, and you can play it back even when your device isn't

https://t.me/learningnets

connected to the Internet. *Streaming*, on the other hand, is when your system plays the clip back immediately as the data transfers without bothering to save it for later. Streaming is popular with subscription-based music services (such as Pandora or Spotify) where users pay a monthly fee to stream as much music as they like (using a specific app) but lose access if they cancel their subscription.

Web Apps

Whereas mobile apps and music-streaming services simply access online databases of content, web apps take remote access a step further. With a web app, you run an application directly from the Internet via a web browser. You don't have to download or install an app; the app remains on the remote server, and you access it from there, as you would a web page.

Microsoft produces Microsoft Office Online (www.office.com), a popular set of web apps that enable anyone with a web browser to use free, simplified versions of their Microsoft Office applications online. Figure 1-28 shows the Word Online web app in action. The applications work only when the computer is connected to the Internet. Documents are stored in Microsoft's free online file storage service, OneDrive, and can be downloaded to the user's local hard drive as needed.

https://t.me/learningnets

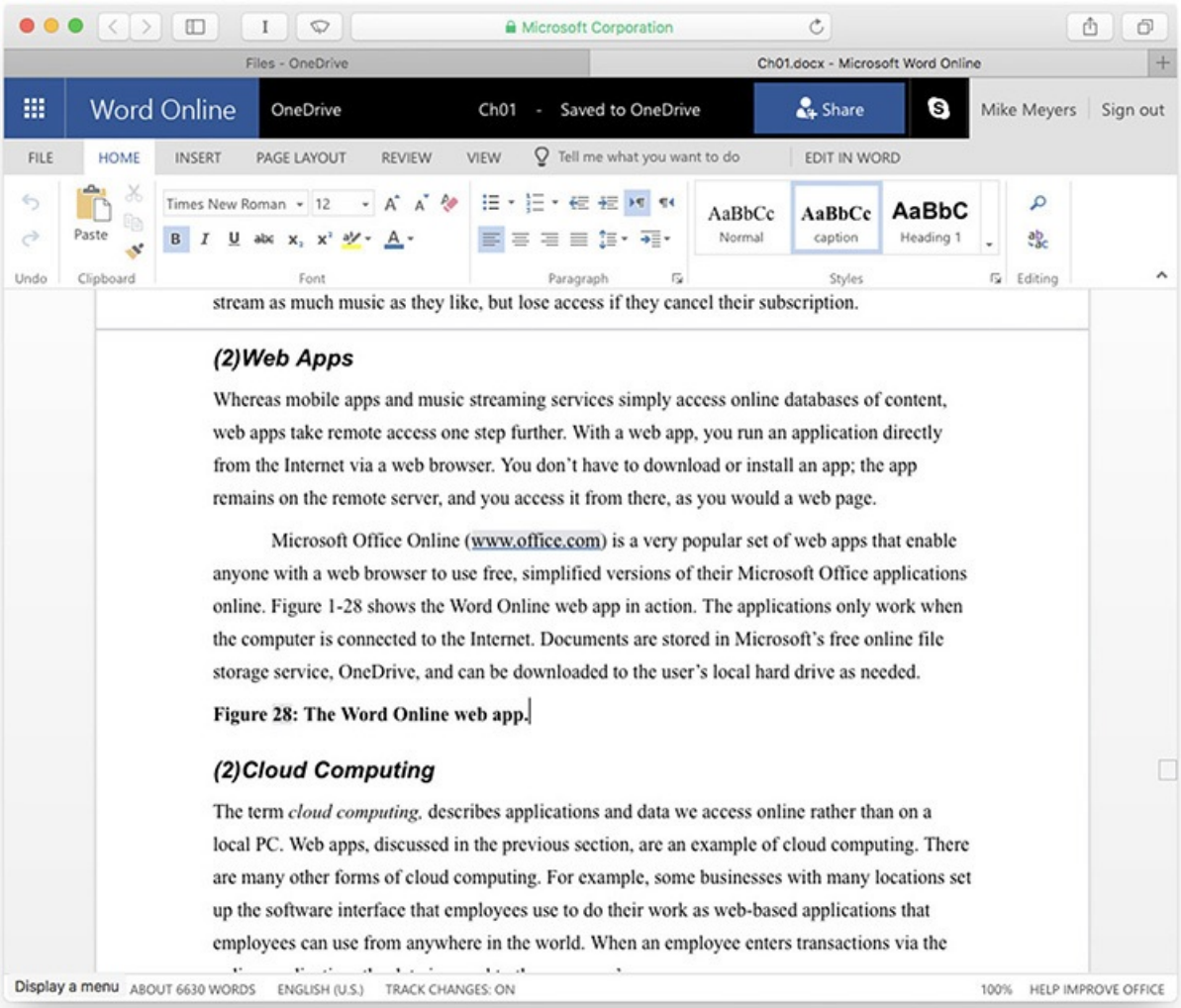


Figure 1-28 The Word Online web app

Cloud Computing

Cloud computing describes applications and data you access online rather than on a local PC. Web apps are an example of cloud computing. Cloud computing comes in many other varieties. Businesses with several different office locations, for example, can set up a software interface that employees use to do their work via web-based applications from anywhere in the world. When an employee enters transactions via the online application, the data is saved to the company's server.

Cloud computing has become a popular means of software distribution in some industries. Rather than an individual purchasing an application once and owning it forever, the user will buy a subscription to the application and access it

https://t.me/learningnets

online as needed. Whereas a retail version of an application might cost hundreds of dollars, a subscription might cost less than $10 a month.

Furthermore, if an individual buys an application outright and then the company releases a new version, the individual would have to shell out *more* money for the new version. With a subscription to an online application, the developer makes the latest version available online. Using online applications also saves local disk space because nothing must be downloaded or installed.



EXAM TIP Many cloud-based services and applications are *collaborative*—they enable multiple people to work on the same data simultaneously and instantly see each other's changes.

Virtualization

Most computers have only one OS (a Windows PC has Windows 10; a Mac has macOS). You can also set up a *multiboot* system that has more than one installed OS to choose from at startup, but you still run only one OS at a time.

Virtualization enables one physical computer to run an operating system or application (called a *hypervisor*) that allows multiple virtual machines (VMs) to share the underlying physical hardware. These virtual machines have their own OS and can all run concurrently if the underlying PC has enough hardware resources such as CPU power, memory, and storage. The VM OS can be different from the OS running on the physical computer system (Figure 1-29). The computer's "real" OS is known as the *host OS*, and the computer itself is the *host PC*. The secondary operating system installed inside the host OS is known as the *guest OS*.

https://t.me/learningnets

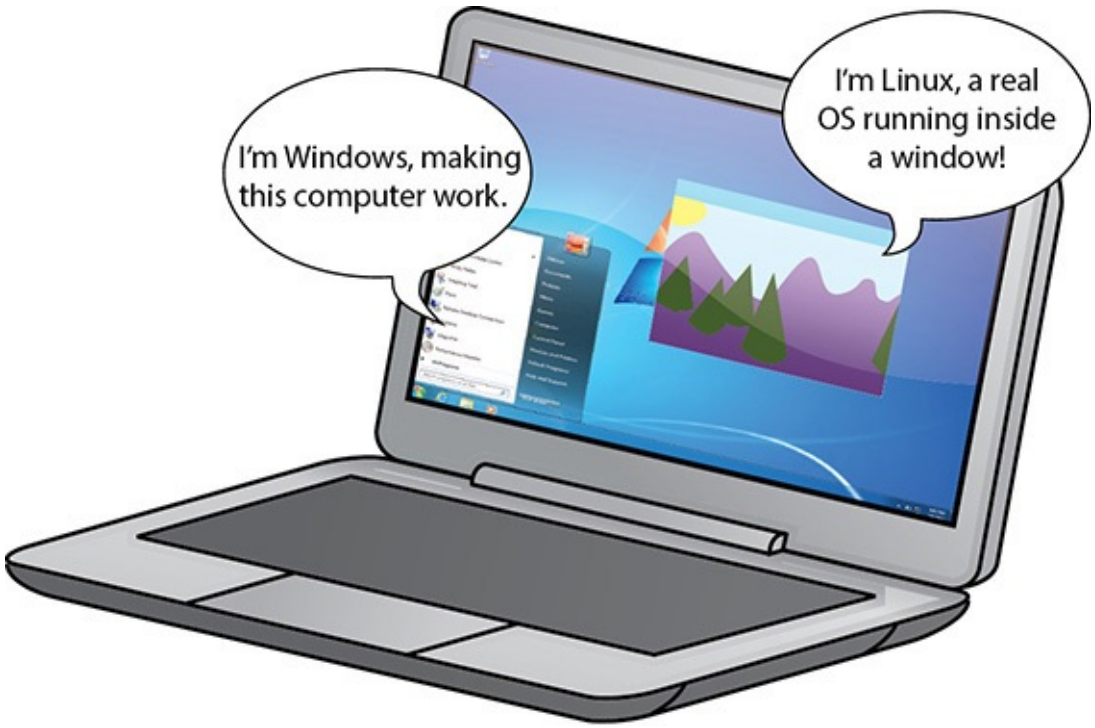


Figure 1-29 Virtualization in action

Hypervisors come in two flavors: Type 1 and Type 2. Type 1 hypervisors don't require an existing operating system; instead, they are the operating system that is designed to share hardware resources among virtual machines. Type 2 hypervisors require an existing operating system since they run as application software. Naturally, you can expect more efficiency and stability using a Type 1 hypervisor because there isn't a bunch of other unrelated stuff running on the machine.

Popular Type 2 hypervisors include VMware Workstation, VMware Fusion, VMware Player, Oracle VM VirtualBox, and the Linux-based QEMU. Microsoft Hyper-V and VMware ESXi are Type 1 hypervisors. As you configure a virtual machine, you tell the hypervisor how much memory it should appear to have, the number and type of input and output ports, and so on. The hypervisor even allocates unused space on the host computer's hard drive as a *virtual hard drive* to hold the secondary operating system and its associated files.

After the VM is configured, you start it up in the hypervisor and install an OS into it. When that task is complete, you can run that secondary operating system on the host computer any time. You can also run it full-screen locally or remotely over the network so that it appears to be the primary OS on the computer, if you like. We used virtualization when writing this book to check the

https://t.me/learningnets

steps for performing various tasks in different operating systems, including several versions of Microsoft Windows, Linux, and macOS. Figure 1-30 shows Linux running in a window on a Windows 10 PC.

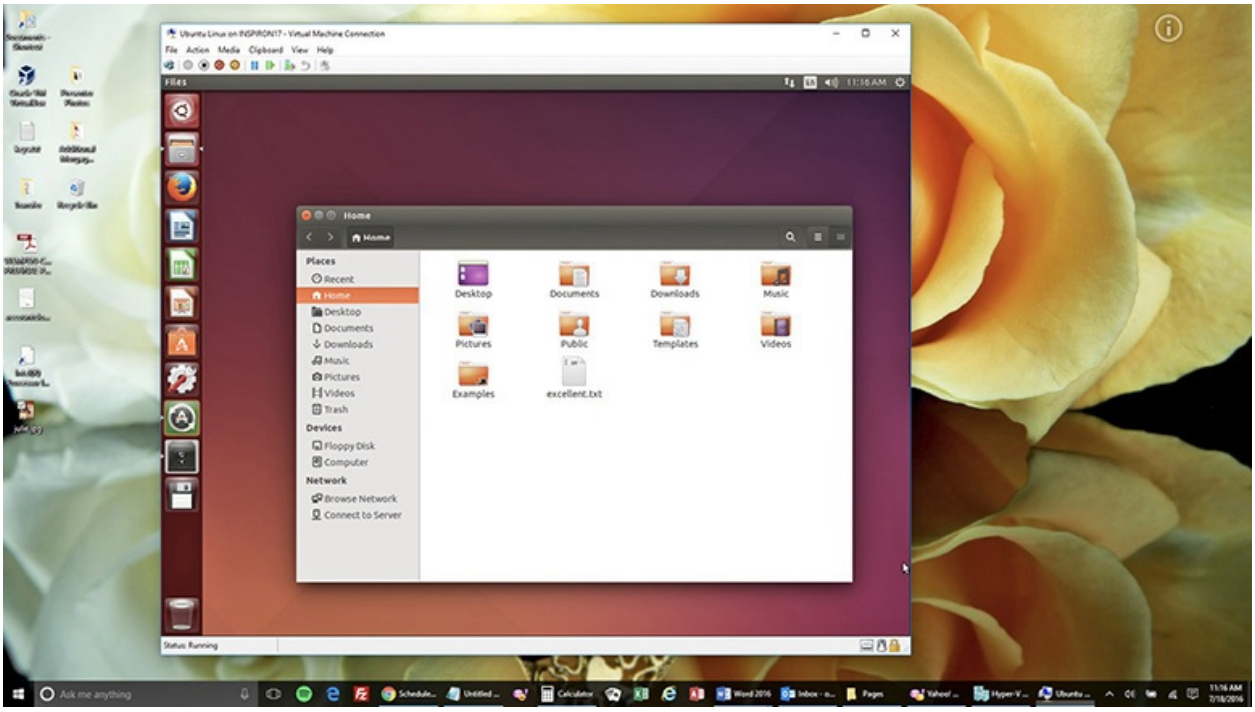


Figure 1-30 Linux running in a VM on Windows 10

Virtualization is handy for individual users on client PCs, such as software developers and IT administrators, but its primary use is on large networked servers. Virtualization enables one of these powerful server systems to run many virtual machines at the same time, saving companies a lot of money on not only initial hardware purchases but also hardware repair and maintenance. Cloud computing (running IT services on somebody else's hardware over a network) relies on virtualization.

Specialized Computer Systems

As we said at the beginning of the chapter, computers are everywhere. In addition to the desktops, laptops, and smartphones we all recognize as computers, there are hundreds of special-purpose computer systems permeating every aspect of modern life. You need to know the following for the CompTIA IT Fundamentals exam:

https://t.me/learningnets

- Point-of-sale terminals
- ATMs
- GPS
- Voice over IP/telepresence

Point-of-Sale Terminals

Point-of-sale (PoS) terminals process purchase transactions. When you pump your own gas and pay with a credit card at a gas pump, for example, you interact with a PoS terminal like the one in Figure 1-31. These computing devices contain a display screen, user input controls, and enough memory and processing power to collect user data and transmit it to a central computer (perhaps located inside the gas station or in the business's office).



Figure 1-31 A point-of-sale computer in a gasoline pump

ATMs

An *automated teller machine* (ATM) is a variation of a PoS terminal, designed for banking transactions. Banking customers have access to their money 24/7 by visiting an ATM terminal and inserting their ATM card.

Because theft is such an issue when money is involved, users authenticate

https://t.me/learningnets

their identities using *multifactor authentication*—in other words, by using more than one method of verifying ID. ID verification can be based on either what you have or what you know. An ATM requires you to have something (a valid ATM card) and also know something (your personal identification number, or PIN) to prove your identity.

GPS

The Global Positioning System (GPS) is a series of satellites that orbit Earth at an altitude of about 12,400 miles (20,000 kilometers). GPS satellites constantly transmit signals to Earth. Every location on Earth has access to at least four of these satellites at any given time. A GPS receiver unit requires data from at least three satellites to function. It calculates how far away it is from each satellite by determining how long it took for the signal (traveling at the speed of light) to arrive. Based on that data, it calculates a 2D position of longitude and latitude, accurate to within a few feet.

The original GPS units were stand-alone devices, but today's smartphones and cars integrate GPS receivers with navigation applications that have become wildly popular with everyday consumers, changing the way people give directions and making standard paper maps nearly obsolete.

VoIP/Telepresence

Voice over IP (VoIP) is a means of using the Internet as a conduit for telephone calls, rather than using the standard telephone lines owned by a phone company. VoIP translates audio data into digital packets that can be sent on computer networks, just like any other kind of network traffic. VoIP phone services such as Vonage and Skype beat the offerings of many more traditional telephone providers in quality, price, and additional features such as teleconferencing and telepresence.

Teleconferencing means having a conference (meeting) via telephone, but the term has come to mean having a video-enabled remote business meeting. Teleconferencing uses a video camera and microphone at each end of the conversation, with VoIP service software to facilitate the connection.

Telepresence is a step up from teleconferencing; it uses sophisticated, high-quality video-conferencing equipment to create an immersive environment where the remote user feels almost *present* at the meeting. The remote user might use local controls, such as a virtual reality headset that enables the operator to look around the robot's environment from hundreds of miles away.

https://t.me/learningnets

Chapter Review

Whew! What a first chapter, right? Let's do a quick review.

In this chapter, you started with features common to all computing devices, such as processors, programming, and data storage. You learned about many different kinds of computers in the modern world. A multi-user computer serves more than one person at the same time, as opposed to a dedicated computer. Dedicated computers include desktops, laptops, and mobile computers such as smartphones and tablets.

You learned that each country has its own laws and regulations regarding the collection and use of private data. Processed data assets result in "information" that can be used to support informed decision-making. Intellectual property is a digital creative work that can be protected from copycats through patents.

The type of operating system a computer runs depends on the computer's hardware. PCs and many portables use Windows or macOS, for the most part, although you'll see Linux and Chrome OS out in the wild. Mobile devices run iOS, Android, or Windows Phone. (BlackBerry OS is an afterthought today.)

Virtualization allows multiple guest operating systems to run concurrently on a single set of computing hardware; this is made possible through a hypervisor. Type 1 hypervisors run directly on the physical hardware where Type 2 hypervisors require an existing operating system.

You also learned how LAN and WAN networks tie computers together. We went through some of the basic hardware devices that make connectivity happen, such as routers, servers, and clients. Specialized hardware devices such as medical monitoring devices that transmit data over the Internet are called Internet of Things devices.

Various programs enable remote connectivity, such as mobile apps, streaming media, and web apps. You learned about cloud computing concepts and touched on virtualization, running an operating system within another operating system.

Finally, the chapter discussed how specialty devices such as point-of-sale terminals and ATMs help consumers accomplish their daily tasks.

Questions

1. What type of computer, also called a notebook, has a monitor that folds down to cover the keyboard for transport?

   A. Server

https://t.me/learningnets

B. Laptop

C. GPS

D. Mainframe

2. What would be an appropriate use for a supercomputer?

A. Playing online games

B. Running a high-volume web site

C. Tallying census results

D. Managing a large business's accounting department

3. Which of these is a workstation operating system?

A. iOS

B. Windows Phone

C. Windows

D. Android

4. Which of these operating systems *cannot* run on a desktop PC with an Intel processor?

A. Linux

B. iOS

C. Google Chrome OS

D. Windows

5. What kind of OS enables users to interact with it using a pointer and graphics?

A. Command line

B. GUI

C. Decentralized

D. Centralized

6. A version of Linux packaged with add-ons and utilities for a particular purpose is known as a:

A. Distro

B. GUI

C. Version

D. Service Pack

https://t.me/learningnets

7. A BlackBerry is a type of smartphone known for what distinctive feature that most other modern smartphones lack?
   - **A.** Graphical screen
   - **B.** Internet connectivity
   - **C.** Touchscreen
   - **D.** Hardware keyboard
8. What operating system is used on an iPad?
   - **A.** macOS
   - **B.** Windows
   - **C.** Android
   - **D.** iOS
9. What kind of network is used to connect individual computers in a single physical location?
   - **A.** WAN
   - **B.** LAN
   - **C.** Internet
   - **D.** Remote
10. Listening to music using an online service like Spotify is an example of what?
    - **A.** Cloud computing
    - **B.** Virtualization
    - **C.** Streaming media
    - **D.** Telepresence
11. You are running virtual machines on a single physical server. The server operating system does not run any other applications and is dedicated to virtualization. What type of hypervisor is this?
    - **A.** Type 1
    - **B.** Type 2
    - **C.** Type 3
    - **D.** Type 4
12. Which factor distinguishes IoT devices from standard computing devices such as laptops and smartphones?

https://t.me/learningnets

A. They must run as virtual machines on a Type 1 hypervisor.

B. They are specialized devices.

C. They must run as virtual machines on a Type 2 hypervisor.

D. They are kept isolated from the Internet.

13. How are information and data different?

A. Data is processed information.

B. Information is processed data.

C. Data does not need to be backed up.

D. Information does not need to be backed up.

Answers

1. **B**. A laptop is a portable computer that folds up for transport, with the monitor covering the keyboard. A server is a specialized computer accessed by multiple other computers. A GPS is a single-user computing device that provides the current geographical location. A mainframe is a large single computer that multiple users access.
2. **C**. Supercomputers are for the most intensive computing applications. They are so expensive that it would be a waste to do any of the other listed activities with one.
3. **C**. Windows is a workstation OS (that is, one designed for desktops and laptops). iOS, Windows Phone, and Android are all mobile operating systems.
4. **B**. iOS is an operating system for portable Apple devices such as the iPad and iPhone. All the other operating systems listed here will run on a desktop PC with an Intel processor.
5. **B**. A graphical user interface (GUI) uses a pointer and graphics. A command-line interface uses text. Decentralized and centralized processing have no relationship to whether there are graphics and a pointer.
6. **A**. Distro is correct, short for distribution. A GUI is a graphical user interface. A version is a release of an OS at a particular point in time, usually numbered, like Windows 10. A Service Pack is an update to a certain version.

https://t.me/learningnets

7. **D**. A traditional BlackBerry has a hardware keyboard, unlike most other smartphones. All other choices are features that all smartphones have.
8. **D**. iOS is used on an iPad. macOS is by Apple but used on Mac desktops and laptops. Windows and Android are not Apple operating systems.
9. **B**. A local area network (LAN) connects computers in the same location. A wide area network (WAN) connects computers far away from one another. The Internet and a remote network are both examples of WANs.
10. **C**. Streaming media allows you to watch and listen to video and audio clips from online sources without downloading them. Cloud computing involves running applications and accessing storage online. Virtualization runs different operating systems on a host OS. Telepresence creates an immersive remote environment.
11. **A**. Type 1 hypervisors run directly on the physical hardware and are dedicated to running virtual machines. Type 2 hypervisors are not dedicated to virtualization; they run within an existing operating system that can do more than run virtual machines. Type 3 and Type 4 are not valid hypervisor types.
12. **B**. IoT devices are specialized computing devices used for medical patient monitoring, home thermostat control, or baby monitoring, to name just a few uses. IoT devices can be controlled or monitored over the Internet; they are designed for this connectivity. Other than for software developer testing, IoT devices do not run as virtual machines.
13. **B**. Data is raw; information is processed data. Both data and information should be backed up, and in some cases this is dictated by laws or regulations.

https://t.me/learningnets

CHAPTER 2

System Hardware

In this chapter, you will learn how to

- Differentiate among CPUs in terms of speed and features
- Explain the types and technologies of memory in a PC
- Describe motherboard form factors and features
- Identify the purpose and functions of a power supply

Knowing how all computing devices work enables you to accomplish several goals. First, you can understand the importance of various components and know when a computer has the right stuff for the job. Second, you can gauge the efficiency of the computing process. Third, you can troubleshoot when something goes wrong.

As you know from Chapter 1, computers consist of two elements, hardware and software, with software further divided into operating systems and programs/apps. Both elements work together to make the computing process happen. This chapter starts the discussion, focusing on hardware. Later chapters cover the software in more detail. Let's look briefly at the process and then get to the meat of the chapter.

Data flows through a computer in this three-step process:

- **Input** The computer accepts incoming data. This could be the user clicking the mouse, typing something, or starting a program that loads instructions.
- **Processing** The computer performs operations (math) on data to transform it. For example, data of 2 + 2 would be processed as 4.
- **Output** The result of the calculation is delivered to the appropriate recipient. This result might go back to an application that requested it, for example, and the application might then display the result on a screen or print it on a printer.

https://t.me/learningnets



NOTE An important part of the computing process is *data storage*, where you save stuff to work on later. We address storage in Chapter 4.

With the computing process firmly in mind, let's turn now to the core hardware involved. We'll start with a discussion of the processors and then turn to memory. The chapter examines motherboards and wraps up with a discussion about power supplies.

CPUs

The *central processing unit* (CPU), sometimes called the *microprocessor* or the *processor,* handles most of the math processing in any computing device. Physically, processors are thin, fragile wafers of silicon and tiny transistors packaged in a robust shell (see Figure 2-1).



Figure 2-1 An Intel Core i7 CPU

https://t.me/learningnets

Intel and Advanced Micro Devices (AMD) make most of the CPUs in today's laptops and desktops. Intel has a much larger market share; AMD is the scrappy underdog.



EXAM TIP ARM Holdings designs the vast majority of CPUs used in mobile devices, such as smartphones and tablets. ARM licenses its CPU designs to many manufacturers that produce the physical chips.

CPUs (and just about every other component in a computer) plug into a circuit board called a *motherboard* (Figure 2-2), also called a *system board*. The motherboard enables all the components to communicate. We'll tackle the specifics about motherboards a little later in the chapter.

https://t.me/learningnets



Figure 2-2 CPU plugged into a motherboard

All processor manufacturers work hard to make each generation of CPUs better than the one before. To make CPUs better, processor makers have focused on optimizing for speed, features, and efficiency.

Speed

The basic measurement of a CPU is its speed, or how many things it can do in one second under perfect conditions. Each thing is a *cycle,* and one cycle per

https://t.me/learningnets

second is expressed as 1 *hertz* (Hz). In the 1980s and 1990s, we measured CPU speed in millions of cycles per second, or *megahertz* (MHz), but we measure today's CPUs in billions of cycles per second, or *gigahertz* (GHz).



EXAM TIP Megahertz and gigahertz are measures of the speeds at which things happen. In contrast, megabytes (MB) and gigabytes (GB) are measures of storage capacity.

To get a sense of what these numbers mean, add 2 to 3. How long did it take you? What about 323 + 718? A typical CPU in a modern PC can add or subtract more than three *billion* such equations every second. That amazing speed translates into what seems like magic, as we discussed in Chapter 1—a glorified calculator that can generate full-motion pictures or play fabulous games.

A CPU works directly with the motherboard to achieve the proper speed. Similar to CPUs, motherboards run at a specific clock speed (called the *bus speed*), again measured in hertz. CPUs run at some multiple (such as 10× or 25×) of that bus speed. If the motherboard runs at 100 MHz and the CPU has a 25× multiplier, the CPU runs at 2500 MHz (or 2.5 GHz).

Features

CPU clock speeds hit a wall around 4 GHz, so CPU makers needed to find new ways to continue increasing processing power. Many of these improvements go beyond a CompTIA IT Fundamentals discussion, but let's look at these four relevant methods:

- 64-bit computing
- Multicore CPUs
- Program handling
- Cache

64-Bit Computing

For more than a decade, CPUs in personal computers had a *32-bit architecture*, meaning the CPU could handle data that was 32 bits in complexity. If you know

https://t.me/learningnets

your binary math (and who doesn't?), a 32-bit CPU could work with numbers up to about 4 billion and could handle an operating system or application with an equal number of lines of code. We all use decimal (base 10) math, such as when working with the worldwide monetary system. Hexadecimal (base 16) notation is often used by computer programmers because it is a shorthand way of representing large values. Characters 0–9 and A–F are used for hexadecimal representation where A is equivalent to 10, B is 11, C is 12, and so on.

Today, most desktop and full-size laptop CPUs are 64-bit, and they require a motherboard with a 64-bit CPU slot. In binary math, doubling the potential size of a value requires just one more bit. Each bit added, therefore, doubles the complexity. A 33-bit value can be twice as large as a 32-bit one. Double that again, and it's 34 bits. You get the idea. A 64-bit CPU can easily handle numbers up to 8,446,744,073,709,551,615. Moving to 64-bit computing has enabled programmers to increase the complexity and awesomeness of their applications.

It's definitely worth noting that both 32-bit and 64-bit applications will work on a 64-bit computer, although 64-bit applications may not run as quickly or be able to address as much RAM as they are designed to. Note, too, that 64-bit applications will *not* run on a 32-bit machine.

Multicore CPUs

Both Intel and AMD decided at virtually the same time to combine two CPUs into a single chip, creating a *dual-core architecture.* This architecture increases both processing capability and efficiency because each core can pick up the slack when the other core gets too busy. Prior to dual-core CPUs, all CPUs were *single-core.*

Today, CPU makers offer CPUs with two (dual-core), four (quad-core), six (hexa-core), and even eight cores (octa-core) on a single chip. These are known collectively as *multicore* processors.



NOTE Assigning the number of virtual CPUs (vCPUs) is common when deploying a cloud-based virtual machine. Some software licensing is based on the number of physical or virtual CPUs present in the system. Of course, more vCPUs means more computing power, which always results in more cost.

Handling Programs

https://t.me/learningnets

CPUs have a preset list of commands they understand called the *codebook* or *instruction set.* Programmers write applications in different computer languages that are translated into code understood by the CPU's instruction set. The processor then works through the code and outputs commands to various parts of the computer.

Every CPU works with incoming commands and data differently. Two different CPUs with the same clock speed won't necessarily process the same image in a complex application like Adobe Photoshop in the same amount of time. The CPU that processes the image faster might even come in last at copying a huge file from one drive to another. These improvements typically mean a previous-generation processor with a fast clock speed may be outperformed by a current-generation CPU with a slower clock speed. It's all about the efficiency of processing (along with other features).

Cache

When you launch an application, it's loaded into the PC's memory, and it operates from there while the application is open. The application sends data to the CPU for processing and receives the processed data back.

Every time the CPU needs data it doesn't already have, it must fetch it from random access memory (RAM). The pathway between memory and the CPU (the *system bus*) is fast, but it's still subject to the physical limitations of the motherboard's *traces* (electrically conductive metal pathways embedded into the circuit board).

Another way to speed up CPU performance is by embedding small amounts of super-fast RAM, called a *cache*, in the CPU chip itself. When the CPU grabs data from RAM, it also copies it into the cache. When the CPU needs the same data again, it first checks the cache. If the data is there, the CPU uses that copy to save time.

Today's CPUs have several levels of cache. Level 1 (L1), the smallest and fastest, is checked first; each subsequent level (L2 and L3) is larger and slower. Different multicore CPU designs will have shared or separate caches for each core, which can influence cost and performance.

Power and Heat Management

When trying to produce better processors, CPU makers need to overcome the fact that faster CPUs require more electricity and thus generate more heat that can damage components.

https://t.me/learningnets

CPU makers discovered while working on processors for portable computers that if you make the components of the CPU very tiny, you can get the same performance with less electricity. Further, if you refine the way the CPU processes its instruction set, the CPU can perform better with even less electricity. Taking design cues from those portable processors, CPU makers have transformed current CPUs into leaner, greener processors.

Even today's lower-powered CPUs still run hot enough to burn you. Other components in the PC (such as chips on the motherboard and hard drives) also generate heat. When a chip overheats, it may malfunction or even stop working until it cools down, and repeated overheating can shorten a chip's life span. Therefore, it's important to have effective cooling systems in many computing devices.

Passive Cooling

Passive cooling does not use power or mechanical parts, meaning it can't keep hotter components cool. The most common type uses a *heat sink* (shown in Figure 2-3), which is a block of heat-conductive metal such as aluminum affixed to a chip with some heat-conductive *thermal paste*. The heat sink has spikes or baffles that increase its surface area. Heat wicks away from the chip into the heat sink and dissipates into the air. Case fans then circulate the hot air out of the case (more on those in a moment).

https://t.me/learningnets

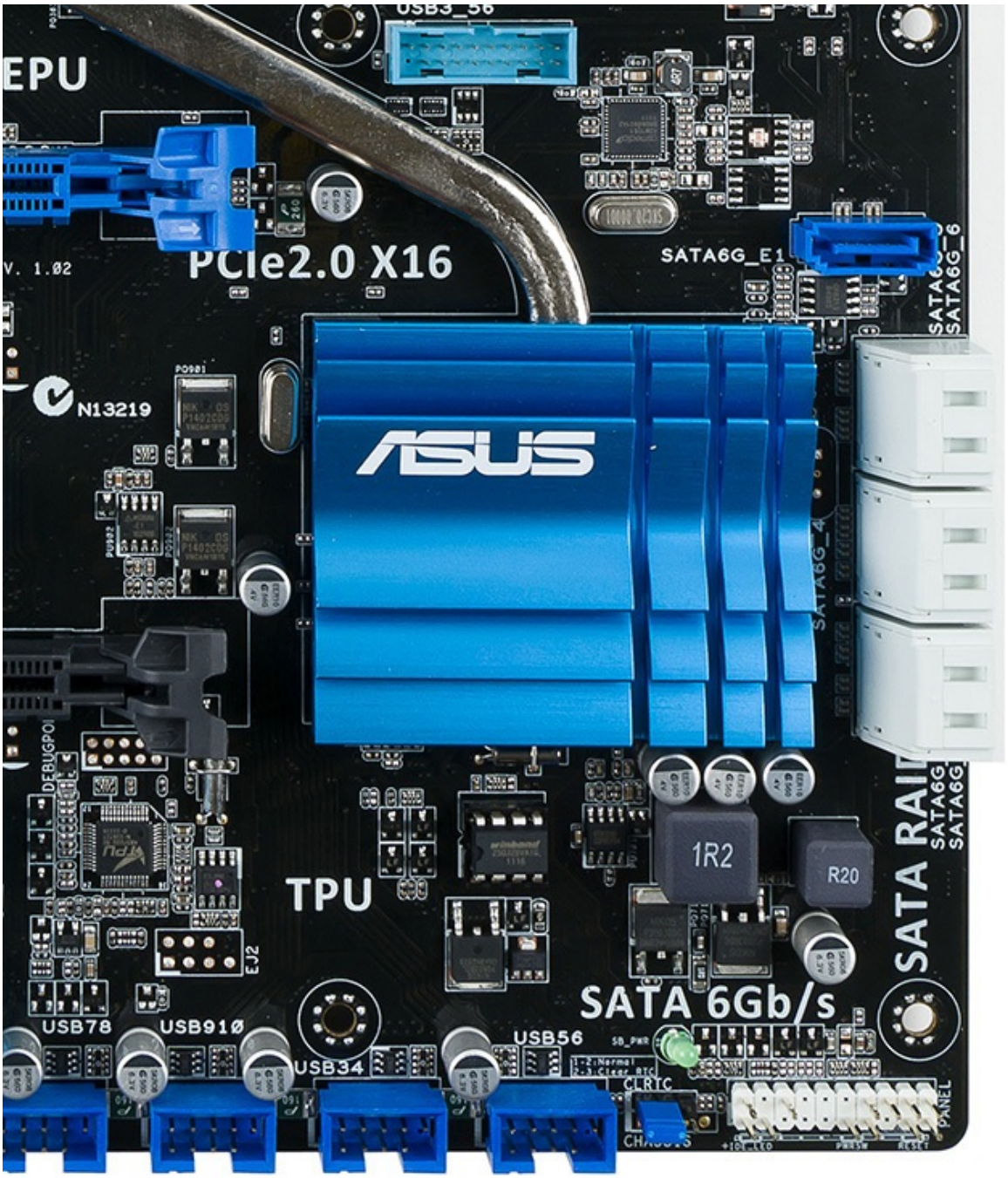


Figure 2-3 A passive heat sink is made of metal that conducts heat away from the CPU.

Active Cooling

Active cooling uses electrically powered mechanical parts. In most PCs, a fan is strapped to the CPU's heat sink in an attempt to circulate air through the heat

https://t.me/learningnets

sink and away from the CPU to keep it cool. The fan typically has its own two-wire cable to draw the small amount of power it needs from the motherboard. Figure 2-4 shows a simple CPU fan and heat sink.



Figure 2-4 A CPU fan is an active cooling device that keeps the CPU from overheating.

In addition to the CPU fan, a desktop or laptop typically also has one or more *case fans* that cool off the entire interior of the computer, not just the CPU. Figure 2-5 shows a case fan. On a desktop PC, the power supply (discussed later in the chapter) has its own fan that pulls in air from the outside of the case, and there may be extra fans and air vents in the sides of the case, or fans that blow directly onto other hot components.

https://t.me/learningnets

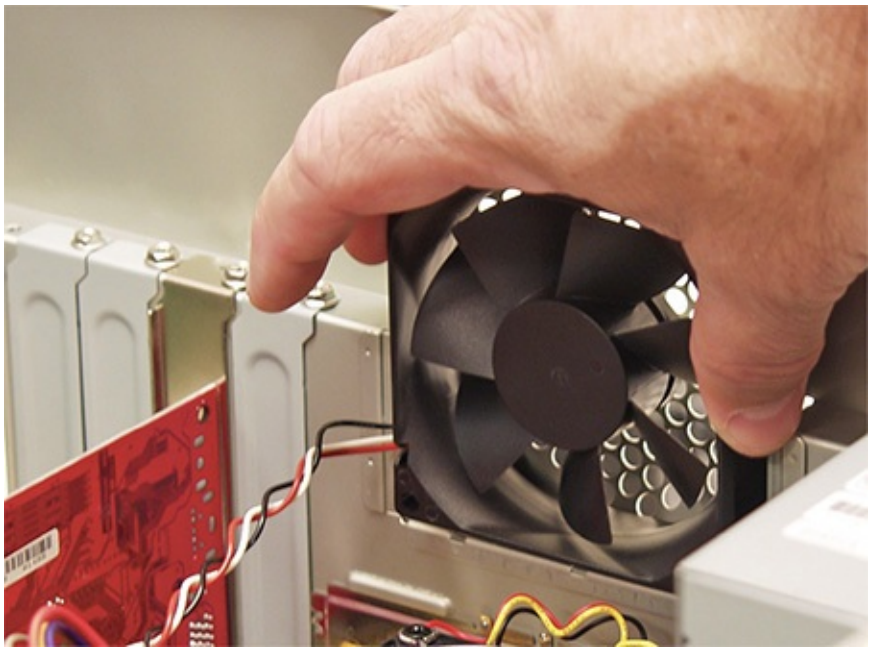


Figure 2-5 A case fan circulates air in the case in general.

Liquid Cooling

Combining liquids with electronics is normally a recipe for disaster because liquids conduct electricity efficiently and can cause short-circuiting. Some high-end gamers and enthusiasts run that risk and use *liquid cooling* systems for effective active cooling. (Liquid is a more efficient conductor of heat than air.)

Liquid cooling systems attach heat sinks (sometimes called *water blocks*) to each of the chips that get hot in the PC, including the CPU and key chips on the motherboard and video card (Figure 2-6). (The video card has a processor called a Graphics Processing Unit (GPU) that helps the CPU produce images on the screen.) The liquid flows through sealed tubing and channels inside the heat sinks, so it doesn't directly touch any of the electronics.

https://t.me/learningnets

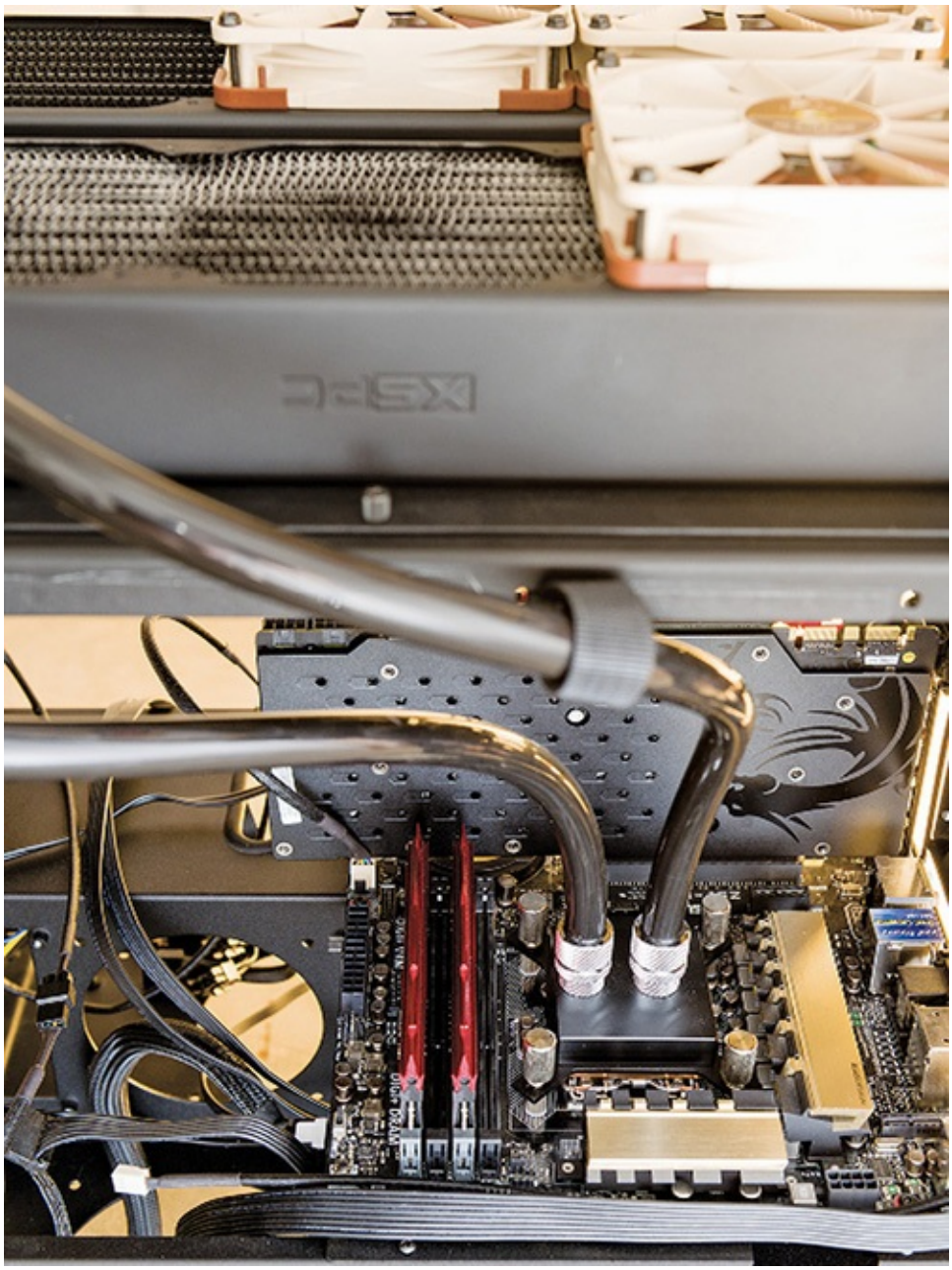


Figure 2-6 Liquid cooling systems circulate liquid among multiple heat sinks placed in key locations in a PC case, wicking away heat from each chip.

A pump circulates liquid from a reservoir through the tubing, from hot chip to hot chip. As the liquid reaches a chip, it picks up some of the heat from the chip and carries it back to the liquid reservoir (which may itself be a fan-cooled radiator to dissipate the heat).

https://t.me/learningnets



EXAM TIP Be sure you are familiar with system cooling methods, including case fans, CPU fans, and liquid cooling.

RAM

Generically, *memory* is solid-state storage that stores the binary translation (ones and zeroes) of some data. (*Solid state* in this case implies no moving parts.) There are many kinds of memory, but if someone mentions PC memory, they probably mean *system RAM*. The word *system* means the memory generally serves the computer as a whole, not one particular component. It's called *random access memory* (RAM) because data can be read from any section of memory. It does not need to be accessed sequentially. A table keeps track of what's stored where.

There are different kinds of RAM, but the kind used for system RAM is *dynamic RAM* (DRAM), which must be constantly refreshed because it can retain data only while powered. When the computer is powered down, whatever was in system RAM vanishes.



EXAM TIP Computers come with other types of memory, including *read-only memory* (ROM). The ROM stores important pieces of information for how the computer works. ROM is nonvolatile, so it retains information when the power goes off.

Different Types of RAM in a Computer

If you look at a desktop PC's motherboard, you'll see some long, thin circuit boards (these may be encased in a heat spreader in high-performance systems) slotted perpendicular to the mainboard. This is RAM. Those circuit boards are called *dual inline memory modules* (DIMMs). Figure 2-7 shows performance DIMMs (with heat spreaders) on a desktop motherboard.

https://t.me/learningnets

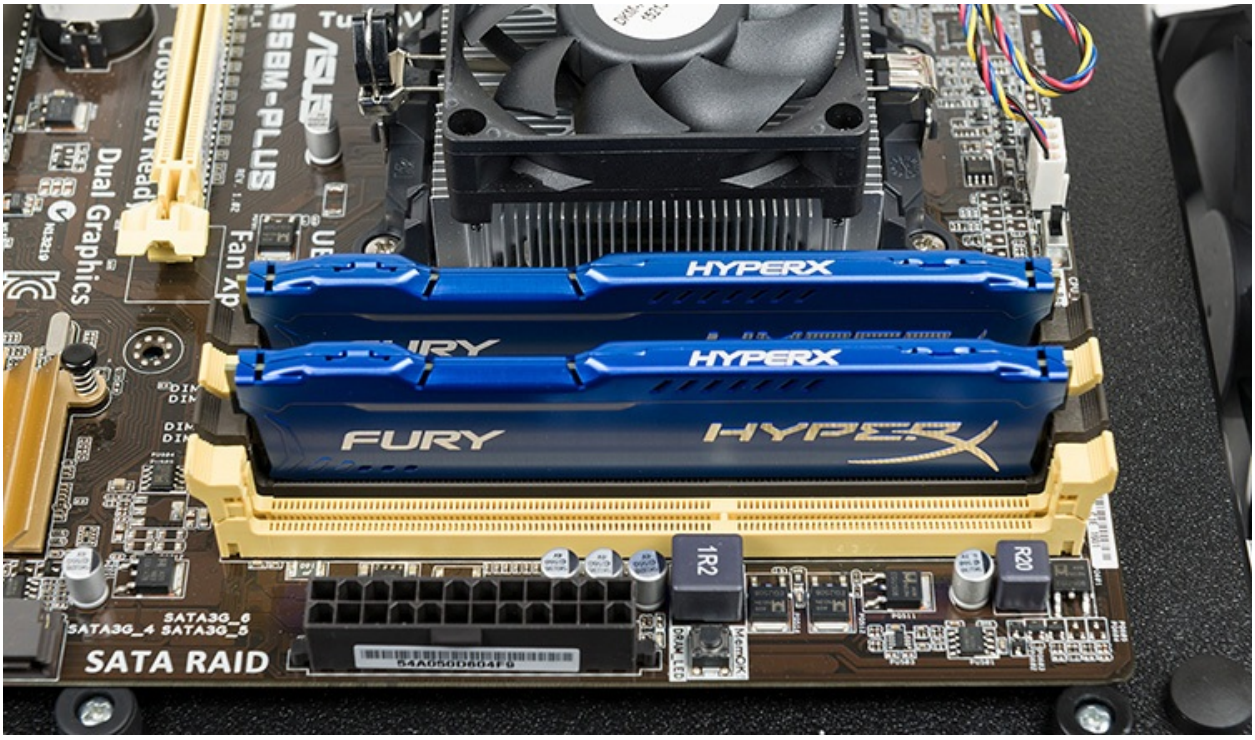
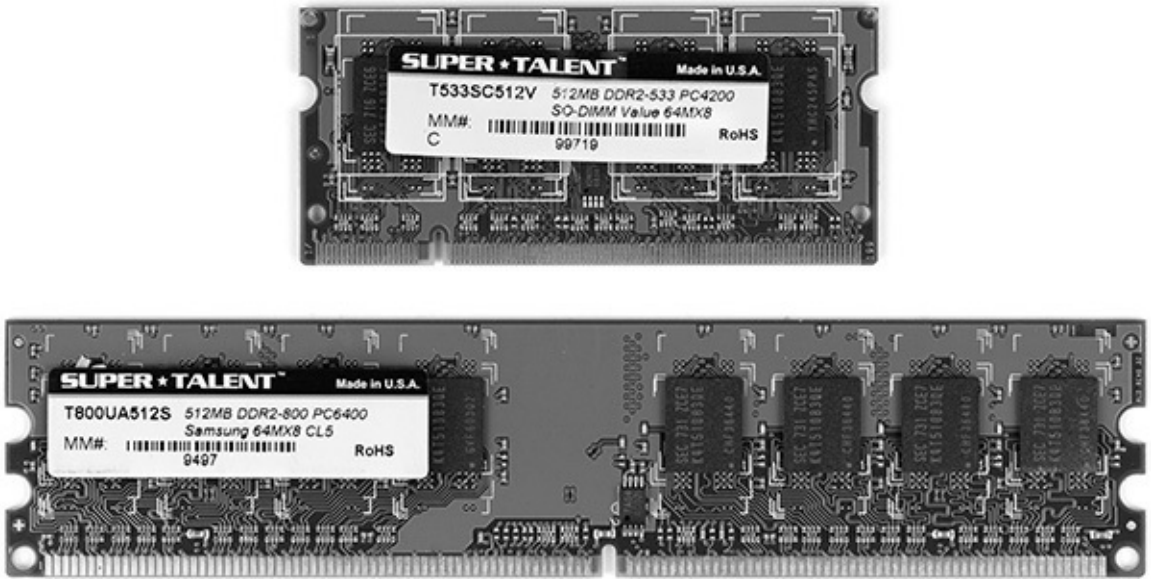


Figure 2-7 RAM installed inside a desktop PC

Laptop PCs use space-saving *small outline DIMMs* (SODIMMs) instead. They typically install almost parallel to the motherboard, at a slight angle. Figure 2-8 compares SODIMMs to regular DIMMs. RAM circuit boards are commonly called *sticks.*



https://t.me/learningnets

Figure 2-8 SODIMM (top) and DIMM (bottom)

The metal tabs across the bottom of a DIMM or SODIMM are called *pins.* Different types of RAM have different numbers of pins so that they fit into certain types of slots. These types are not just physically different but differ in terms of how they operate. See “RAM Technologies and Speeds” later in this chapter.



NOTE The RAM in this section is for desktop and laptop computers. In mobile devices like smartphones and tablets, the RAM is built in, and you can’t see it without disassembling (and probably ruining) the device, so just take my word for it; it’s there.

RAM Capacity

RAM sticks vary in capacity, with higher-capacity sticks naturally costing more than lower-capacity sticks. A DIMM might have a capacity ranging from 1 GB to 16 GB in a typical desktop system, for example. A particular computer’s motherboard will support only a limited range of RAM capacities, so you must be careful when replacing and upgrading RAM in a computer to buy the right capacity, as well as the right type.

RAM Technologies and Speeds

Single data rate (SDR) RAM, now mostly obsolete, is synchronized with the motherboard’s system timer so that it performs one operation per tick of that timer. (That timer isn’t a literal time clock but more like a fast metronome, ticking millions of times per second.) SDR RAM had 168 pins on a DIMM.



NOTE You can’t mix RAM stick types or technologies. RAM sticks are keyed so that they only fit in the motherboard designed for that technology.

Double data rate (DDR) RAM can send or receive data twice for each clock tick on the motherboard. DDR RAM has 184 pins on a DIMM and fits into a

https://t.me/learningnets

different kind of slot than SDR RAM, so there's no way to accidentally mix them up.

In addition to capacity, RAM also has a speed rating that describes how fast it can transfer data. There are four different speed technologies: DDR, DDR2, DDR3, and DDR4. Each is faster and more efficient than the technology that preceded it. Figure 2-9 shows DDR2 and DDR3 with their pins lined up so you can see the difference.

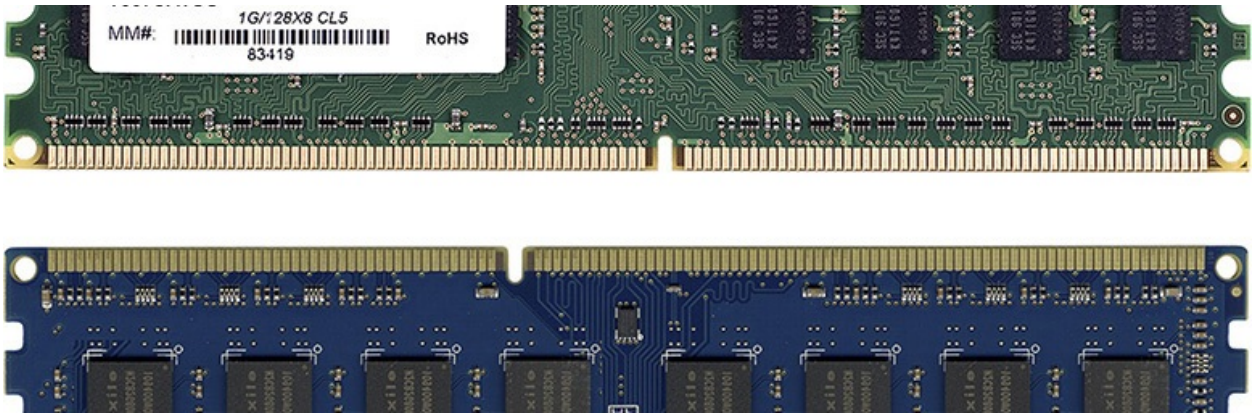


Figure 2-9 DDR2 and DDR3—you can't mix and match because of the position of the spacer.

There are a few other changes between generations aside from the improvements in speed and efficiency:

- DDR2 uses a 240-pin DIMM that, like with the other types, fits into only its own type of slot.
- DDR3 uses a 240-pin DIMM (same number of pins as DDR2), but there is a notch in a different position on DDR3 RAM so it won't fit in a DDR2 slot, or vice versa.



EXAM TIP The CompTIA IT Fundamentals acronym list includes both terms, but DDR RAM and DDR SDRAM are synonymous. The *S* in SDRAM means synchronous, and there is no such thing as nonsynchronous DDR RAM.

https://t.me/learningnets

- DDR4 uses a 288-pin DIMM. DDR4 is relatively new as of this writing, so you can expect to see the earlier generations for some time. The CompTIA IT Fundamentals exam objectives don't cover DDR4.



NOTE Just like with vCPUs mentioned earlier, when assigning virtual hardware to a virtual machine, the amount of RAM can be specified. The combination of CPU and RAM is collectively referred to as *compute power*. Increasing or decreasing the amount of virtual machine computer power is called *vertical scaling*, *scaling up*, or *scaling down*.

Motherboards

Everything in a computer plugs directly or indirectly into the motherboard (Figure 2-10). The motherboard, therefore, is an essential component in the computing process.

https://t.me/learningnets



Figure 2-10 The motherboard provides connectivity among all the pieces.

The motherboard provides pathways (buses) between the memory slots, CPU socket, input and output ports, and built-in devices like network adapters and sound adapters. It's not just a dumb highway system; the motherboard has its own intelligent controller (the *chipset*) that manages the traffic and tells the various buses how fast they can run.

Motherboard Form Factors

Motherboards come in different sizes and shapes (*form factors*), each one fitting into a different kind of case, whether for a mobile device (such as a laptop), a desktop, or a server. Figure 2-11 shows three different form factors: an ATX (a full-size motherboard for large desktops), a microATX (a motherboard for

https://t.me/learningnets

smaller systems), and a Mini-ITX (a tiny motherboard for even smaller or specialty systems).



Figure 2-11 Three motherboards: ATX, microATX, and Mini-ITX (left to right)



EXAM TIP The purpose of the motherboard/mainboard is to connect computer components. Know that they come in different sizes called *form factors*.

Motherboard Features

Motherboards vary widely in price, mostly based on the following features:

- **CPUs supported** Each motherboard supports only a narrow range of CPUs, based on specific physical chip attributes, such as the number of pins. Motherboards only support chips from Intel or AMD; they're never interchangeable.
- **RAM supported** Each motherboard supports only a certain kind of RAM, such as DDR3 or DDR4, with a certain minimum and maximum capacity.
- **Built-in components** Some motherboards have built-in capabilities (on-board) such as audio, video, and network support. You will probably want

https://t.me/learningnets

these in any computer, so having them built in saves you from having to buy and install separate add-on expansion cards. High-end users who are choosy about these components often find the built-in ones lacking.

- **Expansion slots** A motherboard will have several slots into which you can place expansion cards (circuit boards that add capabilities beyond the basics). There are different technologies for these slots, but the most common kind today is PCI Express (PCIe). Chapter 3 explains these slots in more detail.
- **Firmware** Each motherboard has a setup program stored, or embedded, on a chip on the motherboard; this chip is its *firmware*. Contemporary systems should come with Unified Extensible Firmware Interface (UEFI) firmware, but you'll probably still encounter older systems with Basic Input Output System (BIOS) firmware.
- **Special features** Higher-quality motherboards include controllers for special types of storage, extra security measures, hardware assistance for virtualization, and more. Know your needs and shop accordingly.

Power Supplies

The *power supply unit* (PSU) in a desktop PC is a big metal box (Figure 2-12) mounted in one corner of the case. It has a bouquet of multicolored wire bundles coming out of it; these wires and connectors provide power to multiple individual components inside the case, including the motherboard and the disk drives. It's often referred to as just the *power supply*, and that's how we refer to it here as well, but keep in mind that you may see the acronym PSU on the exam.

https://t.me/learningnets



Figure 2-12 A typical computer power supply

A power supply converts the alternating current (AC) power from the wall outlet to the direct current (DC) power that computer components require, and it steps down the voltage of the incoming power to the exact amounts that each component requires. The step-down is dramatic: wall-outlet power comes in at 110 volts (V), and components require somewhere between +2 and +12 V.



EXAM TIP When we talk about DC current, there is a positive or negative symbol associated with it because direct current stays at a certain polarity, either positive or negative. In contrast, AC switches continuously between positive and

https://t.me/learningnets

negative.

The largest connector on the power supply (20- or 24-wire) connects to the motherboard, which in turn parcels out small amounts of power to each of the built-in components and to the CPU and RAM slots. This connector is commonly known as the *P1* or *ATX* connector. Some systems have an extra 12-volt connector with four pins that attaches elsewhere on the motherboard; this is the *P4* connector. Figure 2-13 shows these attached to a motherboard.

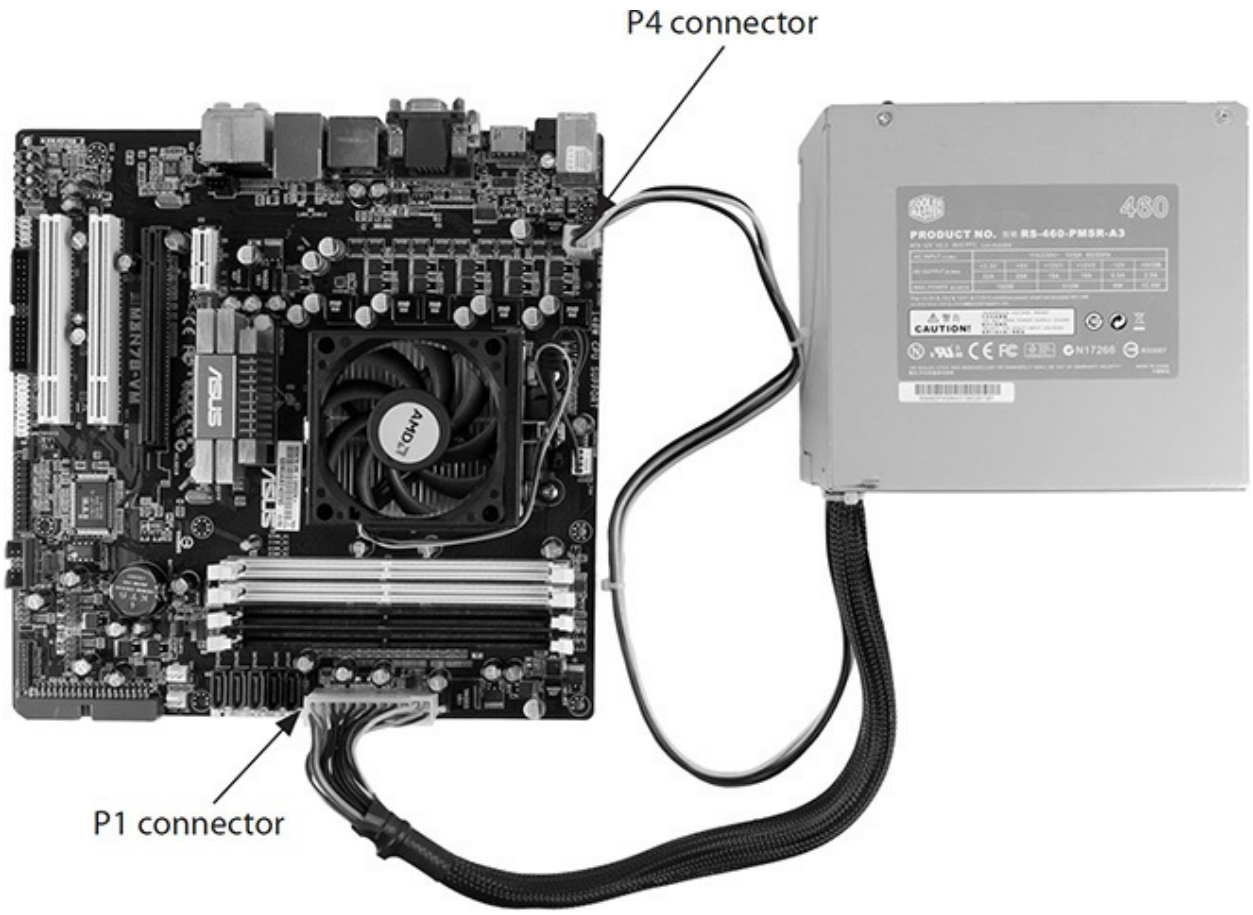


Figure 2-13 A power supply connected to a motherboard



NOTE Higher-end motherboards require an eight-wire additional power connector, rather than the four-wire P4.

Each wire color is significant; red wires provide +5 V power, white wires

https://t.me/learningnets

provide –5 V, yellow wires provide +12 V, orange wires provide +3.3 V, and black wires are for grounding. (We're just telling you the voltages for each color because it's interesting; you don't have to memorize them for the exam.) The small connectors from the power supply each have different purposes. Some are for drives, while others connect directly to different spots on the motherboard or on certain kinds of expansion cards.

A laptop doesn't have a power supply inside the case that converts power. Instead, it has a power cord with a transformer block on it (sometimes called a *brick*) like the one in Figure 2-14. This block converts the power to DC and steps down the voltage for the system, but then the motherboard passes power on to each component as needed.



Figure 2-14 A laptop's power cord includes a transformer block that converts power.



NOTE One compelling benefit of cloud computing is that because you are

https://t.me/learningnets

using IT services running on provider hardware, the hardware purchase, configuration, and maintenance are not your responsibility; they are the provider's.

Chapter Review

In this chapter, you learned about the essential system components (CPU, RAM, cooling system, motherboard, and power supply) inside a personal computer and how they work together to process inputs and outputs.

Because the speed of modern processors has run into a wall around 4 GHz, manufacturers work hard to add and refine new features with each generation to achieve greater performance at the same speed. Some of these improvements include the move to 64-bit CPUs, the inclusion of multiple CPU cores, and refinements to how the CPU executes commands and caches data. To cope with the heat produced by these components, most desktops use active air or liquid cooling systems that push air or liquid, respectively, through a metal heat sink attached to the CPU.

Recent systems have DDR2, DDR3, or DDR4 RAM, which is where the system stores programs and data while they are in use. Each generation of RAM improves speed and power efficiency, but you need a motherboard designed to take advantage of a specific generation of RAM.

Motherboards, power supplies, and cases come in a few form factors (a standard for their size and mounting locations), so these components need to be compatible with the same form factor. The motherboard provides a foundation for the system and the buses (pathways) between components, so it affects what CPUs, RAM, expansion slots, and other features the system can use. The power supply converts AC current from a wall outlet to appropriate DC current for the system; some components receive this power through direct connections to the power supply, and others receive it through the motherboard.

Questions

1. Which of these is *not* part of the data processing sequence?
   - **A.** Networking
   - **B.** Processing
   - **C.** Output
   - **D.** Input

https://t.me/learningnets

2. What is another name for a CPU?
   - **A.** Microprocessor
   - **B.** Intel
   - **C.** System memory
   - **D.** Chipset
3. Which of these is *not* a feature of a CPU?
   - **A.** Multicore
   - **B.** 64-bit processing
   - **C.** L1 cache
   - **D.** DDR
4. Why is passive cooling not usually used for a CPU?
   - **A.** Draws too much power
   - **B.** Not effective enough
   - **C.** Moving parts break down
   - **D.** Uses too much RAM
5. What is the main advantage of liquid cooling over air cooling?
   - **A.** Less expensive
   - **B.** Safer
   - **C.** More effective
   - **D.** Uses less power
6. In what type of computer is SODIMM memory used?
   - **A.** Laptop
   - **B.** Desktop
   - **C.** Server
   - **D.** Smartphone
7. In what two ways are DDR3 DIMMs better than DDR2 DIMMs? (Choose two.)
   - **A.** Less expensive
   - **B.** More reliable
   - **C.** Uses less power
   - **D.** Faster

https://t.me/learningnets

8. What manages and controls the speed of a motherboard's buses?
   - **A.** RAM
   - **B.** CPU
   - **C.** Chipset
   - **D.** L1 cache
9. What are the two functions of a desktop PC's power supply? (Choose two.)
   - **A.** Steps down the voltage
   - **B.** Increases the voltage
   - **C.** Converts AC to DC
   - **D.** Converts DC to AC
10. What is the reason for different color wires on a power supply?
   - **A.** The wire color determines the appropriate component for the connector.
   - **B.** Each wire color represents a different voltage.
   - **C.** Certain color wires deliver AC power, and certain ones deliver DC power.
   - **D.** Certain color wires deliver higher-quality power than others.
11. You are reconfiguring a cloud virtual machine with additional vCPUs and additional RAM. Which term best describes your actions?
   - **A.** Scaling down
   - **B.** Scaling in
   - **C.** Scaling up
   - **D.** Scaling out

Answers

1. **A**. Input, processing, and output are the three steps in the data processing sequence.
2. **A**. Microprocessor is another name for the central processing unit (CPU). Intel is a company that makes CPUs. System memory is RAM. The chipset is a controller for the motherboard.
3. **D**. DDR is a type of memory. All the others are CPU features.

https://t.me/learningnets

4. **B**. Passive cooling is not effective enough to cool most CPUs. Passive cooling draws no power, has no moving parts, and uses no RAM.
5. **C**. Liquid cooling is more effective than air cooling. It is more expensive and less safe (because of the risk of leaks) and uses more power.
6. **A**. SODIMM is a small-outline DIMM used in a laptop PC. Desktops and servers use regular DIMMs. A smartphone has built-in memory.
7. **C**, **D**. DDR3 uses less power and is faster than DDR2. It is not more reliable or less expensive.
8. **C**. The chipset manages the motherboard. RAM and CPU are items installed on the motherboard. The L1 cache is a memory cache inside the CPU.
9. **A**, **C**. A desktop power supply converts 110 V AC current from the wall to DC current in the range of +3.3 V to +12 V.
10. **B**. Each wire color is a different voltage. All wires deliver DC power of the same quality level.
11. **C**. Vertical scaling means increasing or decreasing underlying virtual machine compute power. Increasing vCPUs and RAM is called scaling up, whereas decreasing is called scaling down. Scaling out means adding additional virtual machines to handle an IT workload, whereas scaling in means removing virtual machine when the workload lightens.

https://t.me/learningnets

CHAPTER 3

Device Ports and Peripherals

In this chapter, you will learn how to

- Differentiate among expansion card and slot types
- Identify the common ports and connectors on a PC
- Describe the types, technologies, and connectors for monitors
- Explain standard input devices
- Describe other common I/O devices

In Chapter 2 you learned about the essential processing components of a computer: the central processing unit (CPU), memory, motherboard, and power supply. Without any one of those, a computer doesn't function.

This chapter explores ways to expand the capabilities of a computing device through expansion slots and common ports. We'll look at monitors, the primary output device for most computers, and examine standard input devices such as the keyboard and mouse. The chapter wraps up with a survey of other input/output (I/O) devices you'll see in the wild.

Expansion Cards and Slots

As you learned in the "Motherboards" section of Chapter 2, motherboards have expansion slots, into which you can install *expansion cards* that add capabilities to the computer. You could add a video adapter (to replace a built-in adapter or to use in addition to it), for example, or you could add a type of port the motherboard doesn't natively support, such as FireWire or eSATA (which you'll see later in this chapter).

Expansion Cards

Expansion cards have a row of metal tabs (pins) along one edge (shown in

https://t.me/learningnets

Figure 3-1) that fit into expansion slots on the motherboard. The position and number of pins depend on what kind of slot the card is designed to fit into. An adjacent edge has a metal *backplate* that fits into an opening in the back of a desktop PC so you can access the expansion card's port (or ports).

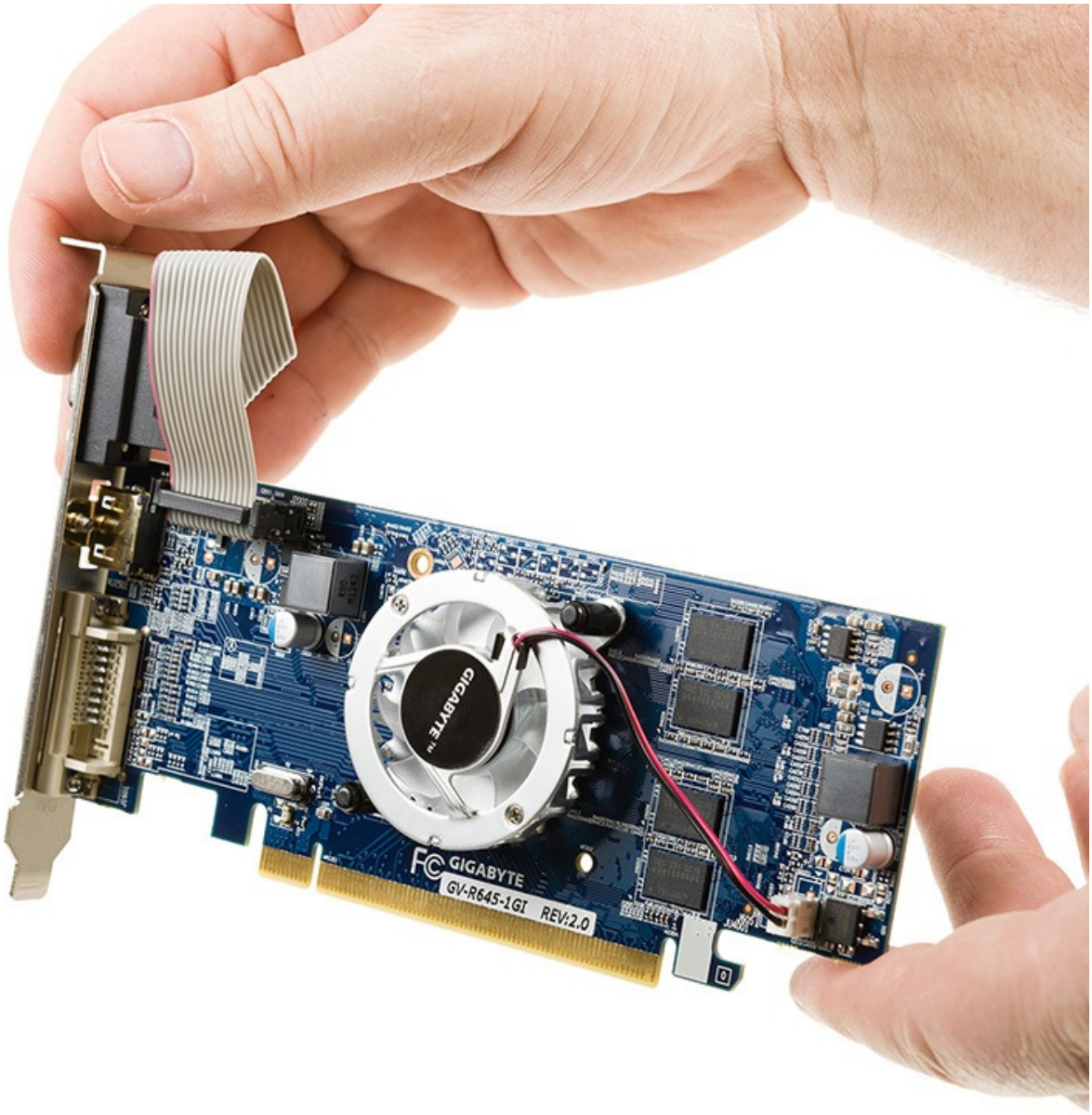


Figure 3-1 An expansion card for a desktop PC

There are many types of expansion cards providing different capabilities, and you can also find motherboards with the most common types built in. You need to know these four for the CompTIA IT Fundamentals exam:

https://t.me/learningnets

- **Video card** Also called a *display adapter,* a *video card* provides ports to connect to an external display and acts as a graphics processor interface between the operating system and the monitor. Monitor types and connections are covered later in this chapter. Video cards work hard, so it's best to use the fastest interface available.
- **Audio (sound) card** A *sound card* provides ports to connect speakers, headphones, microphones, and other digital audio input and output devices. Most of sound ports are round 3.5-mm connectors.
- **Network card** Also called a *network interface card* (NIC), a *network card* enables you to connect to a local area network. A network card can be wired or wireless. If wired, it has an *RJ-45* port (covered later in this chapter). If wireless, it may have a small external antenna. NICs have a 48-bit hexadecimal Media Access Control (MAC) address that uniquely identifies the NIC on the LAN.



EXAM TIP Network adapters are often referred to as NICs even when built into the motherboard. The acronym NIC has come to refer to the adapter's functionality, rather than the physical card.

- **Modem** A traditional *modem* enables you to connect to the Internet or some other network using a regular telephone land line for dial-up access. A modem expansion card will have two *RJ-11* (telephone) ports on it, side by side. The term *modem* is also now used to refer to high-speed cable and DSL Internet connectivity through existing copper wire-based cable television and telephone lines respectively. Figure 3-2 shows the similar RJ-45 and RJ-11 ports.

https://t.me/learningnets

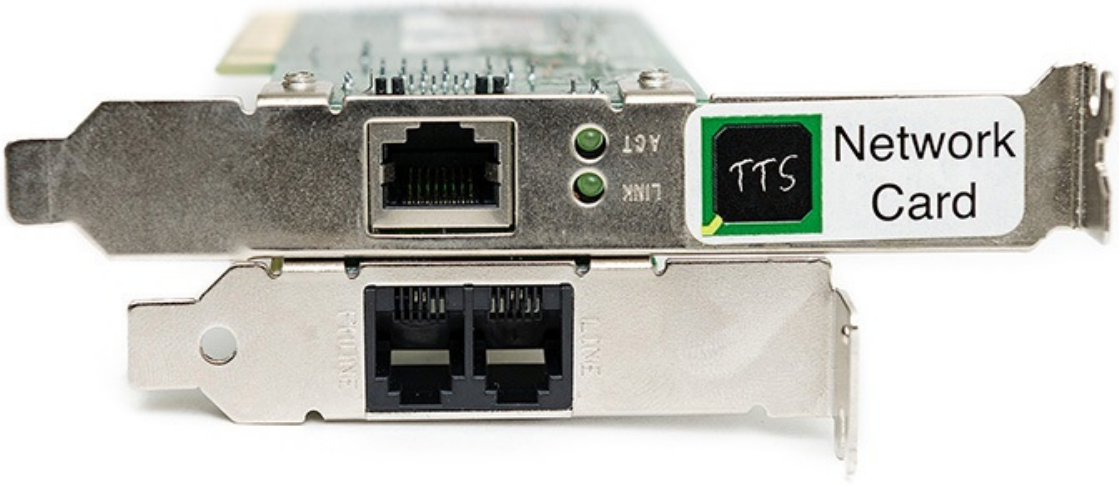


Figure 3-2 Expansion cards with one RJ-45 port (top) and two RJ-11 ports (bottom)

Expansion Slot Types

Computer manufacturers have used many different expansion slot types over the years; currently *PCI Express 3.0* (PCIe) dominates the market. The term applies to both the slot and the bus that carries data from the slot to the system bus. Each slot has between 1 and 32 independent lanes that carry data, and a slot has a numeric designation (such as ×1, ×4, ×8, or ×16) to describe how many lanes it has.

Lower-capacity slots can be used for expansion cards that do not carry a lot of data at once, like network cards. A motherboard typically has several ×1 slots. Higher-capacity slots, like ×16, are reserved for expansion cards that carry a lot of data, such as video adapters. A motherboard typically has only one or two ×16 slots.

Many motherboards sport an older general-purpose slot type, *Peripheral Component Interconnect* (PCI). Figure 3-3 compares a standard PCI slot with several PCIe slots (if you look closely, you can see labels near the slots).

https://t.me/learningnets

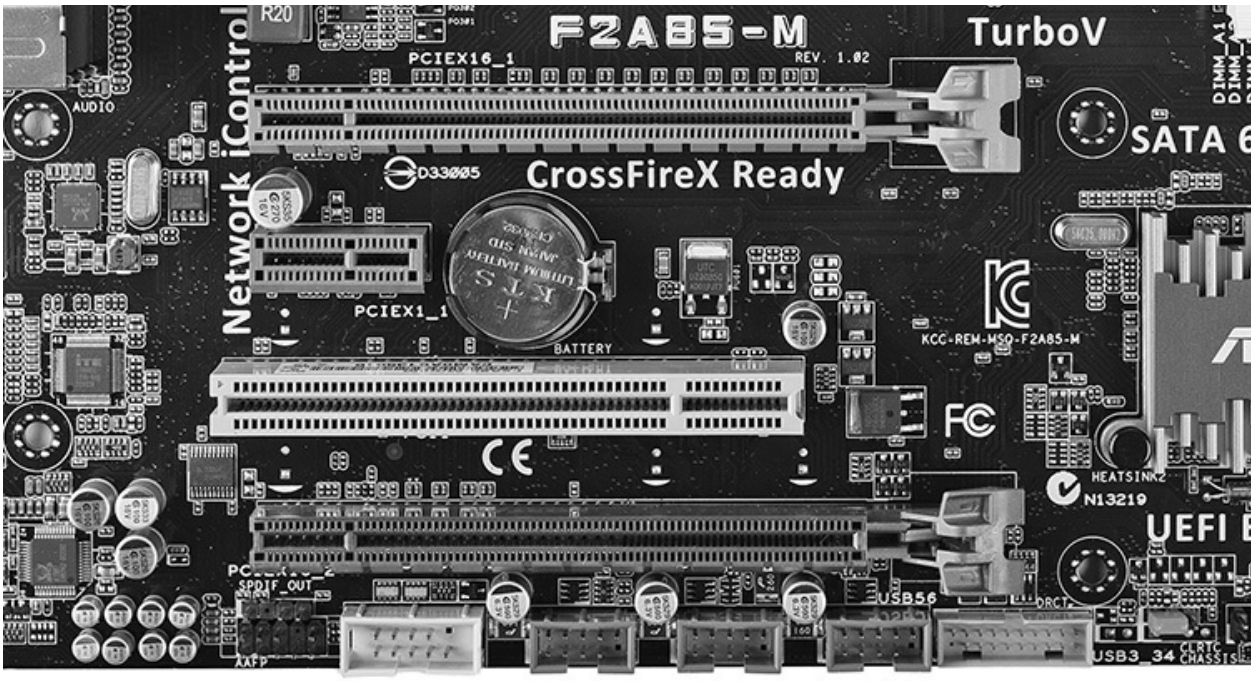


Figure 3-3 From top to bottom: PCIe ×16, PCIe ×1, PCI, and a black PCIe ×16 that operates at ×8 speed

Some laptop PCs have *mini-PCIe* slots that accept smaller versions of the same kinds of expansion cards that desktop PCs use. Older laptops, as you might expect, had *mini-PCI* slots. Figure 3-4 shows a mini-PCIe slot and card.



Figure 3-4 A mini-PCIe slot and card in a laptop PC

https://t.me/learningnets

Common Ports and Connectors

Different types of peripherals connect to computers in different ways, so a computer will typically have multiple port types, each with its own connector size, shape, and specifications. You should be able to identify many of these connectors on sight and tell what kinds of devices they may work with. We'll cover ports for monitors and other video devices later in the chapter, so for now we'll turn to ports and connectors for other peripherals.

USB

The *universal serial bus* (USB) enables you to add a remarkable variety of peripherals to computers. USB is an industry-standard connector; you'll find them on many brands and models of many computing devices. USB can carry both data and power, so a USB cable is sometimes used to connect small electronics to computers (or to alternating current [AC] power outlets, with the appropriate adapter) to charge them.

USB Generations and Speeds

USB comes in several flavors, such as USB 2.0, USB 3.0, USB 3.1, and USB 3.2. USB 2.0 has two standards, USB and Hi-Speed USB. For the most part, their ports are all physically interchangeable and backward compatible.

USB 2.0 Regular *USB*—often mistakenly called USB 1.1—transfers data at up to 1.5 megabits per second (Mbps) at low speed or 12 Mbps at full speed. On a system that color-codes different speeds of USB port, these are typically white.

Hi-Speed USB transfers data at up to 480 Mbps. Hi-Speed USB ports are sometimes color-coded black to differentiate them from the slower regular USB ports, and the little tabs inside the cable connectors may also be black rather than white.

USB 3.*x* USB 3.0 (also called *SuperSpeed USB*) transfers data at up to 5 gigabits per second (Gbps). On systems that use color-coding, USB 3.0 is usually bright blue. When USB 3.1 was released, USB 3.0 was confusingly renamed *USB 3.1 Gen 1*. USB 3.1 (or more correctly USB 3.1 Gen 2 and sometimes SuperSpeed USB 10 Gbps) increases the speed to 10 Gbps. The USB 3.2 standard maxes out at approximately 20 Gbps. If you're ever ordering a motherboard or a prebuilt computer, check the USB version supported as well as the number of USB ports; you'll always want enough ports to accommodate

https://t.me/learningnets

your USB devices with the fastest throughput possible.

USB Connector Types

There are a number of USB connector and port formats that you might see. Here's a little about each of the connectors shown in Figure 3-5:



Figure 3-5 Common USB connectors

- **Type-A** The "standard" rectangular USB ports on most desktop and laptop PCs and on one end of most USB cables.
- **Type-B** A near-square connector used most for full-size peripherals such as printers.
- **Mini-B** A smaller peripheral connector for smartphones, digital cameras, MP3 players, and so on. Mini-B is less durable than Micro-B, so it has become rare because few new devices use it.
- **Micro-B** Also for smaller peripherals and devices. The original Micro-B is more compact than Mini-B, though USB 3.*x* updates the Micro-B connector to add another part. The old Micro-B cables will fit into the new USB 3.*x* Micro-B ports (without using the new part), but the new part prevents the new 3.*x* Micro-B cables from using the older ports.
- **Type-C** A compact connector for both larger and smaller devices introduced alongside (but separate from) USB 3.1. To eliminate the problem of trying to insert a USB connector upside down, Type-C can be inserted in two orientations. Type-C connectors will eventually replace all previous USB connectors.

Other Peripheral Ports and Connectors

You should know how to spot a few more common ports that aren't USB, and the CompTIA IT Fundamentals objectives also expect you to be able to identify some legacy ports that are rarely used anymore.

https://t.me/learningnets

- **Thunderbolt** Like USB, Thunderbolt supports a variety of peripherals. Thunderbolt enables you to daisy-chain up to six devices, which means you can plug a Thunderbolt external storage drive into a Thunderbolt monitor, into another Thunderbolt monitor, and so on. Thunderbolt uses connectors adopted for earlier technologies and in turn supports those technologies. The version 1 and version 2 Thunderbolt ports (shown in Figure 3-6) used primarily on Macs for connecting monitors use a Mini DisplayPort connector. Thunderbolt 3 uses the same connector as USB 3.1 Type-C ports. That means you can plug a USB Type-C device into a Thunderbolt 3 port, for example, and the device will function. (The reverse is not true.)



Figure 3-6 Thunderbolt versions 1 and 2 connectors (right) on a MacBook Air

  - Thunderbolt 1 runs at 10 Gbps.
  - Thunderbolt 2 runs at 20 Gbps.
  - Thunderbolt 3 runs at 40 Gbps.
- **FireWire** Also known as IEEE 1394 (for the standard that defines it). This is used primarily with digital cameras, media devices, and external hard drives. It is generally a viable but less popular alternative to USB.
  - FireWire 400 runs at 400 Mbps.
  - FireWire 800 runs at 800 Mbps.
- **eSATA** Used exclusively for external SATA storage devices, such as external hard drives. These ports and connectors resemble USB and plain SATA, but they are *not* interchangeable with either.
  - The various eSATA standards run at 1.5, 3, or 6 Gbps.

https://t.me/learningnets



EXAM TIP I've listed the speeds of USB, Thunderbolt, FireWire, and eSATA so that you can rank them clearly. You don't need to memorize the numbers; just rank the standards from fastest to slowest—Thunderbolt, USB, FireWire, and then eSATA.

- **RJ-45** Ethernet networking connector. The port has visible metal pins inside; the rectangular plastic connector is transparent (with wires visible inside) and has a small release tab on top.
- **3.5-mm audio** The same connector as a small headphone jack, used for microphones, headphones, and speakers. These are color-coded on most systems.
- **PS/2** Round plugs for connecting older mice and keyboards (color-coded green and purple, respectively). This has been mostly replaced by USB.
- **RJ-11** Used for traditional modems and landline telephones. Both the port and connector look like smaller versions of the RJ-45 connector. This is becoming rare as dial-up Internet connections all but vanish.
- **Legacy parallel** Old printers. This uses a 25-pin D-shaped connector and has mostly been replaced by USB.
- **Legacy serial** Very old low-speed devices of many kinds. This uses a 9-pin D-shaped connector. It has been mostly replaced by USB.

Figure 3-7 shows each of these common connectors.



Figure 3-7 Common connectors

https://t.me/learningnets



EXAM TIP Take the time to study the appearance and purpose of each of these connectors and think through how to tell them apart from the other connectors in this chapter and how to spot the corresponding port on a device.

Monitors

The *monitor* is the primary output device for the computer. It displays the results of input and the computer's processing. This could be anything from moving through a level of an intense action game to moving your mouse across the desktop. When most people think about their interactions with a computer, they are probably thinking about what happens on the monitor.

Every monitor, while distinct, has the same basic components. The back of the monitor has connections for receiving a video signal from the computer and power from a wall outlet. The most important part is, of course, the display itself (see Figure 3-8).

https://t.me/learningnets

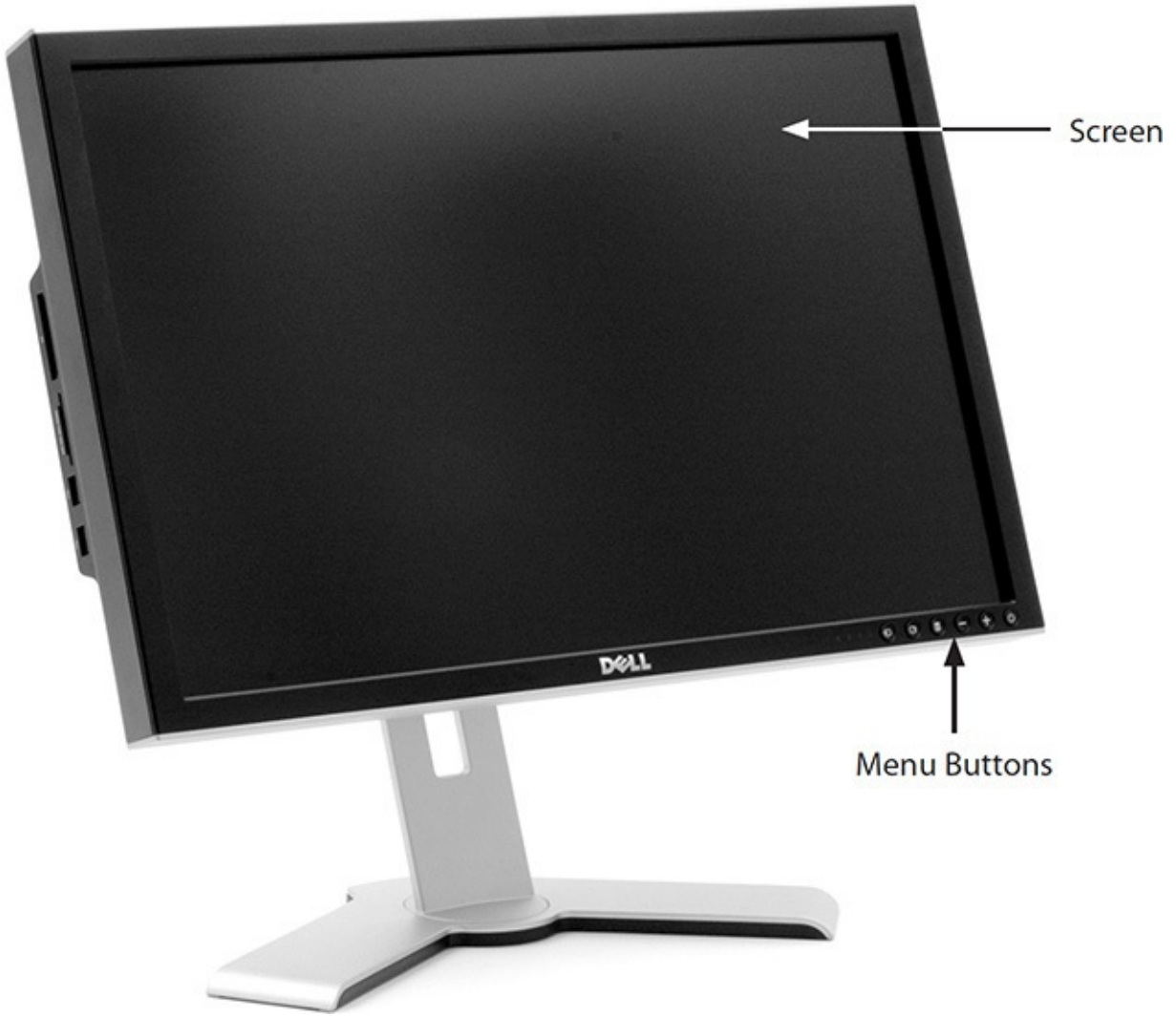


Figure 3-8 Front of monitor

You can power the display on and off and adjust other settings using a set of buttons usually found on an edge of the monitor. Pressing the Menu button opens an on-screen menu that enables you to adjust the brightness, contrast, color balance, size, and position of the display (see Figure 3-9). Most monitors also have a button that will automatically choose the best settings for you.

https://t.me/learningnets

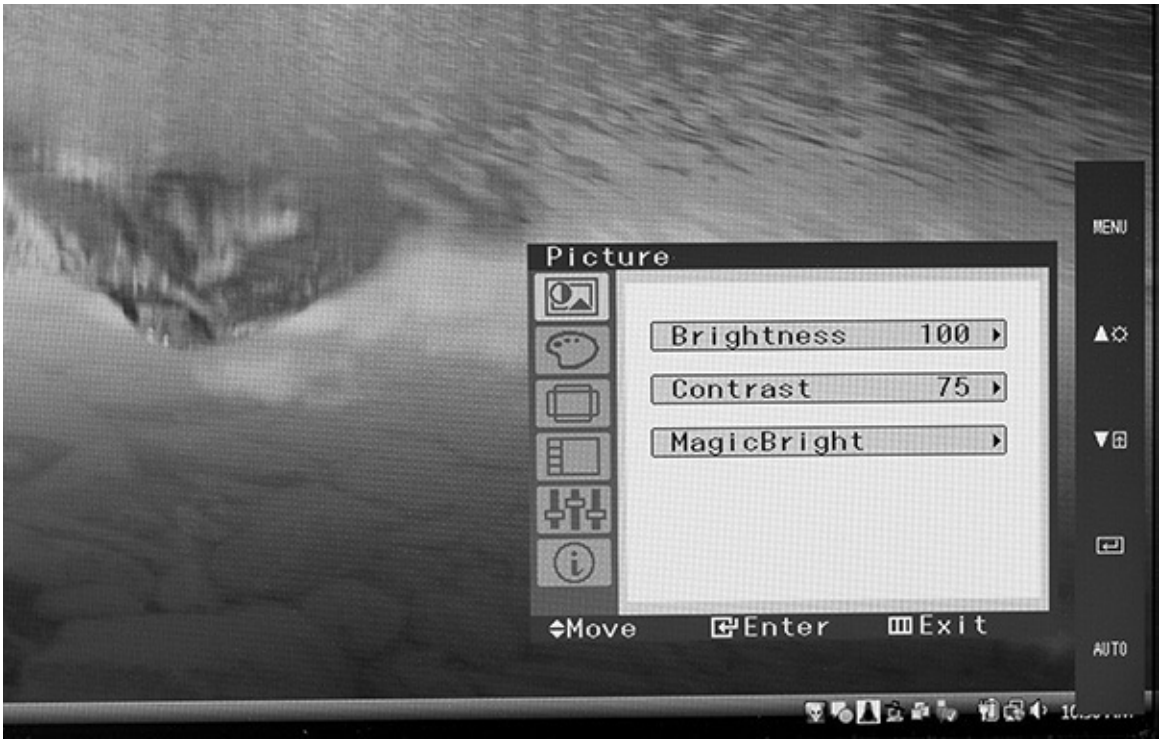


Figure 3-9 On-screen menu options

Monitor Types

There are two main computer monitor types: flat-panel displays (of various kinds) and the now-obsolete cathode ray tube (CRT). Computers can also hook up to external projectors. Let's look at the basics of how they work.

LCD and Other Flat-Panel Displays

A *flat-panel display* (FPD) is thin (many are thinner than a half-inch), is lightweight, and has very little power.

The most common FPD is the *liquid crystal display* (LCD), which has a backlit layer of liquid crystal molecules (called *subpixels*) sandwiched between polarizing filters. The older backlights are efficient, long-lasting *cold cathode fluorescent lamps* (CCFLs). Newer *light-emitting diode* (LED) backlights use a grid of many tiny lightbulbs. When power is applied to the diodes, the bulbs glow.

An efficient variant of LED called *organic light-emitting diode* (OLED) has grown popular on devices such as high-end smartphones and televisions, and by early 2016 it was finally beginning to show up on laptops and monitors. OLED uses organic compounds that naturally produce (colored) light rather than

https://t.me/learningnets

needing a backlight.

Plasma display technology is mostly for televisions, but you can of course connect a computer to it. Plasma TV sizes begin at around 32 inches because of the large pixel size. Plasma displays have their own method of lighting the screen with phosphorous cells instead of liquid crystals, and the phosphors do not require backlighting. Plasma displays are unfortunately thicker, require more power than LCDs, and suffer burn-in from screen elements that never move (such as elements on a computer desktop). One upside is a wide viewing angle.

Instead of being nearly square like old televisions (a 4:3 *aspect ratio* of width to height), most modern FPDs use a 16:9 or 16:10 *widescreen* aspect ratio. This ratio is great for looking at two documents side by side (or, of course, watching movies).

CRTs

A *CRT monitor* (see Figure 3-10) is bulky because it contains a large cathode ray tube. It uses electron guns to activate phosphors behind the screen, causing each pixel on the monitor to generate red, green, or blue. CRT monitors are obsolete, though you might see them in a CompTIA IT Fundamentals question. CRTs have high-voltage capacitors inside, so don’t open one for any reason. If a CRT is malfunctioning, dispose of it.

https://t.me/learningnets



Figure 3-10 A CRT monitor

CRT monitors are heavy and use a lot of electricity, though they do have the same sharp, crisp image at any display resolution. LCD monitors look crisp only at their native (highest) resolution.



NOTE CRTs contain an assortment of hazardous materials, including lead, phosphorus, and mercury, so don't throw them out with the trash! Instead, contact a computer recycling company near you. They will dispose of old computer components for you.

Projectors

Projectors shoot an image out the front and onto a screen. Front-view projectors (see Figure 3-11) connected to computers running Microsoft PowerPoint have

https://t.me/learningnets

been the cornerstone of almost every meeting since the Clinton administration. The qualities that matter most are brightness (in lumens—larger rooms need higher-lumen projectors) and throw (in image size at a given distance from the screen).



Figure 3-11 Front-view projector (photo courtesy of Dell Inc.)

All projectors have a recommended minimum and maximum *throw* distance. Manufacturers create short and long throw projectors. A high-end short-throw projector can create a 100-inch diagonal image from about 4 feet away. A long-throw projector would need 10-plus feet to accomplish the same thing. Pick a projector based on the space (and price).

Projector lamps work hard to generate a tremendous amount of light, and a lot of heat is a byproduct, so projectors come with a fan to keep the lamp from overheating. Replacement lamps are costly.

Most modern projectors don't require you to plug media sources in. You can use Bluetooth or Wi-Fi wireless connectivity to project items from a smartphone, laptop, or desktop computer to the projector.

Monitor Ports and Connectors

Monitors come with at least one port to connect to computers (which seems pretty obvious). Many offer several types of connectors to give you options.

https://t.me/learningnets

Let’s dig into what you might find.

Digital Visual Interface

A typical monitor sports one *Digital Visual Interface* (DVI) cable and connector (shown in Figure 3-12). Despite the name, this connector does not always carry a digital signal. There are actually three connector types: DVI-D (digital), DVI-A (analog), and DVI-I (integrates digital and analog).



Figure 3-12 A DVI cable and connector

High Definition Multimedia Interface

The *High Definition Multimedia Interface* (HDMI) is the current standard for television and home theater equipment connections and is increasingly common on computer monitors. HDMI handles both video and audio signals (in contrast to video-only DVI). Figure 3-13 shows the full-size Type-A connector. You will also see a smaller, mini connector (called a Type-C) on a lot of portable devices.

https://t.me/learningnets

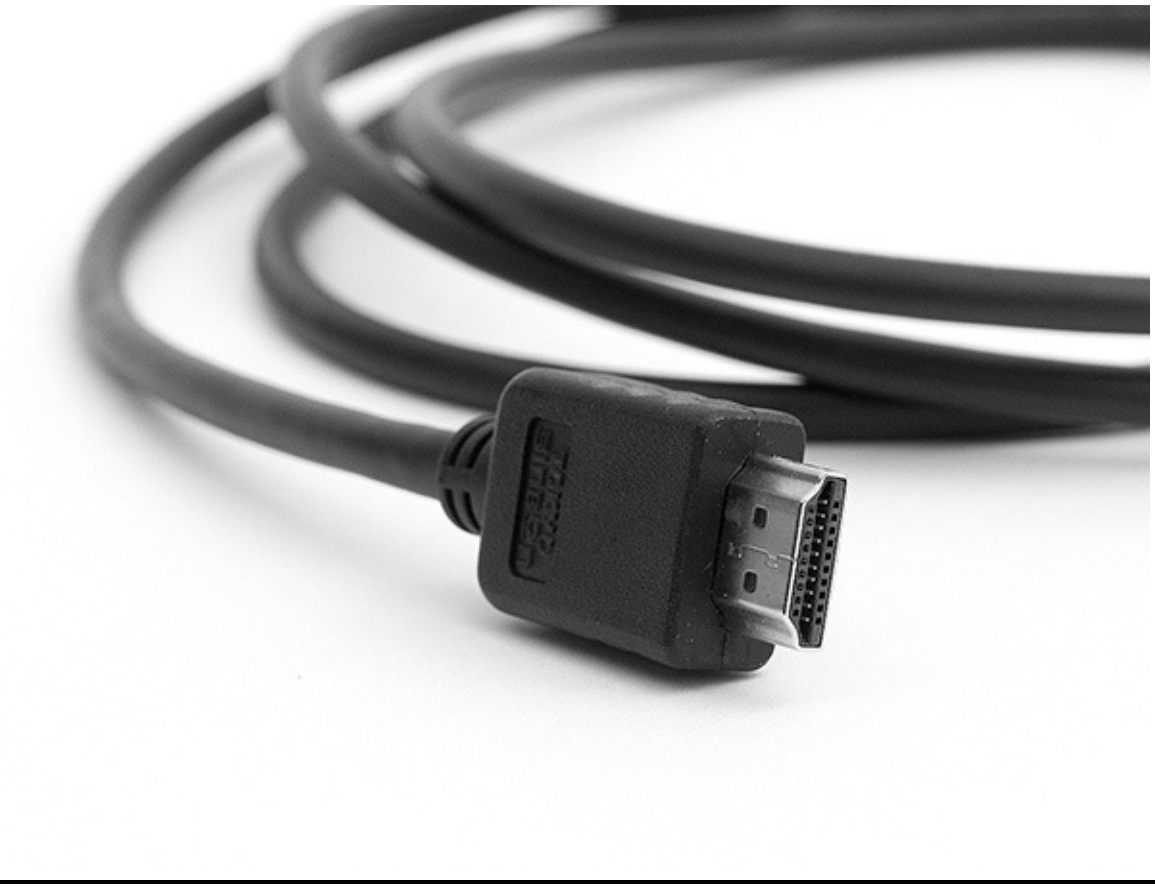


Figure 3-13 An HDMI connector

Video Graphics Array

The oldest type of video connector still in use today is *Video Graphics Array* (VGA), shown in Figure 3-14. It has 15 pins, laid out in three rows of five. This is an analog connector, meaning it sends an analog (not digital) signal to a monitor. Use VGA when DVI and HDMI are not available.

https://t.me/learningnets

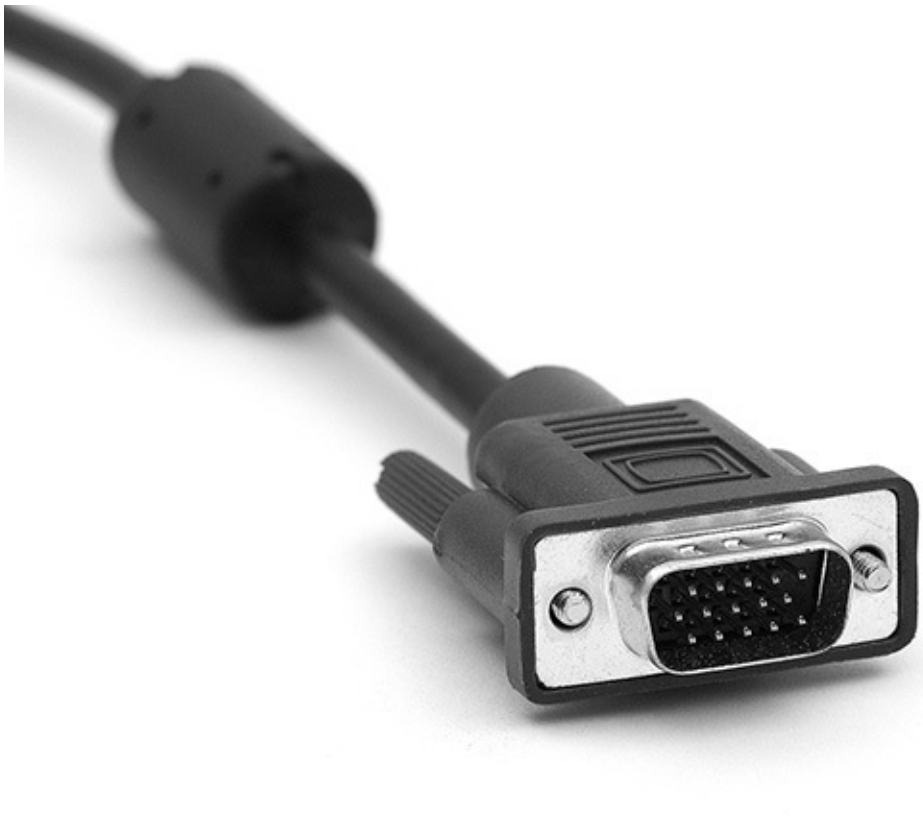


Figure 3-14 A VGA connector

Composite Video

A *composite* video connector (see Figure 3-15) is a round, yellow RCA connector. The figure also shows an RCA port (on an adapter), which is color-coded to match the connector. Many composite cables are joined to red and white RCA connectors (for stereo audio). Composite video is not a great interface for PC use and doesn't support high resolutions.

https://t.me/learningnets



Figure 3-15 The composite (RCA) video port and connector are yellow.

S-Video

S-Video (short for *separate video*) is an interface for standard-definition video. It is a round plug with four pins (as shown in Figure 3-16). It provides better image quality than composite video but is not as good as component video (discussed next). S-Video carries audio as well as video signals, like HDMI, but with lower-resolution video.

https://t.me/learningnets



Figure 3-16 S-Video cable and connector

Component (RGB) Video

Component video is an analog video signal where the three main video components (one for black and white and two for color information) are separated into their own channels. As shown in Figure 3-17, it uses three RCA cables (color-coded red, green, and blue). Although some monitors support it, few computer display adapters do, so it’s not a popular interface for PC monitors. It’s more common on TVs and home theater components.

https://t.me/learningnets



Figure 3-17 Component video



NOTE Some people assume the red, green, and blue (RGB) cables carry corresponding (red, green, and blue) signals as in the RGB color scheme, but in this case RGB just indicates the connector colors.

DisplayPort, Mini DisplayPort, and Thunderbolt

DisplayPort, Mini DisplayPort, and Thunderbolt are found primarily on Macintosh computers. DisplayPort was meant to be a replacement for VGA on all platforms, but it has failed to catch on, probably because of the growing popularity of the HDMI interface.

Thunderbolt and the older Mini DisplayPort are physically identical and can both be used to connect monitors. Thunderbolt ports can also accommodate other types of devices.

https://t.me/learningnets

Thunderbolt and DisplayPort support both high-definition video and audio, just like HDMI.

The full-size DisplayPort connector is roughly the size and shape of a USB connector, but it has a keyed corner to differentiate it. Figure 3-18 compares the Thunderbolt, DisplayPort, and USB ports.



Figure 3-18 From left to right: Thunderbolt port, DisplayPort, and USB



EXAM TIP Keep track of which video connections carry only video signals and which carry both video and audio. The latter group includes HDMI, S-Video, Thunderbolt, and DisplayPort.

USB

With the right adapter, you can use a USB port on a computer to connect to a monitor. You'll find these in use mainly for projectors and presentations. We have no idea what kind of projectors we'll meet when we travel to teach. If our presentation laptop has only HDMI and VGA ports, we also carry a USB-to-DVI adapter.

Touchscreens

A *touchscreen* is both an input device and an output device. It functions like a regular flat-panel display in every way, but it also has a touch-sensitive surface you can use to interact with the operating system. The touch-sensitive part of the screen, the *digitizer,* is a transparent overlaid grid of sensors that record your touch.

This works by recording how the flow of electricity through the sensor grid changes when you touch the screen. The most common variants used in

https://t.me/learningnets

consumer computing devices are resistive and capacitive.

A *resistive screen* consists of two thin, flexible sheets of plastic, with a gap between them. When you touch the surface of one sheet, that sheet presses down onto the sheet below it, creating an electrical signal. A resistive screen works no matter what is pressing on it—a finger, a gloved finger, or a stylus.

A *capacitive screen* uses the electrical properties of the human body to alter the capacitance of an electrostatic field on the screen. This type of screen is made of glass, so it is more durable than the plastic resistive touchscreen. The main drawback is that it doesn't usually work with gloved fingers or with styluses not designed for capacitive screens.

Standard Input Devices

Almost all desktop and portable computers feature two input devices, a keyboard for typing and a mouse or other pointing device for moving a cursor across the monitor screen. This section looks at both input device types in some detail.

Keyboards

The keyboard is the primary input device for many computing devices. Keyboards enable you to input text and to issue commands by pressing key combinations (called *keyboard shortcuts*).

Over the years, manufacturers have added extra keys to the standard keyboard, but most standard keyboards in English-speaking countries have the same QWERTY layout (see Figure 3-19). The *QWERTY* name comes from the first six letters on the top alphabetic row; there's typically a row of numbers above this row and a row of function keys above that. *Function keys* can change a lot depending on the program, but F1 is almost always Help.

https://t.me/learningnets



Figure 3-19 A QWERTY keyboard



NOTE Not every language uses the same alphabet. There are keyboard layouts available for most languages in the world. This is called *regionalization.* A keyboard for Spanish adds accented characters such as *é* and Spanish-only characters such as *ñ*.

Other keys you'll find on a Windows-based keyboard are ESC, TAB, CAPS LOCK, SHIFT, CTRL, ALT, and WINDOWS. On every keyboard you'll find keys such as HOME, END, BACKSPACE, DELETE, and so on. Keyboards for Macs have CONTROL, OPTION, and COMMAND keys instead of CTRL, WINDOWS, and ALT keys.

At the right side of all full-size keyboards is the *numeric keypad,* or *number pad*. The number pad lays out the numbers 0–9 along with various math symbols (plus, minus, and so on) like a calculator. Some keyboards, such as those on portable computers, leave off the number pad, but you can buy a stand-alone number pad peripheral if needed.

Most keyboards (even wireless ones) use a USB Type-A connector to connect to the computer. Very old keyboards used a PS/2 connector.

Modern wireless keyboards require two components. A wireless receiver

https://t.me/learningnets

plugs into a USB port and then communicates via radio frequency (RF) with a wireless keyboard. You may find much older wireless peripherals that communicate with short-range infrared (IR) light that requires an unbroken line of sight between the sending and receiving devices.



NOTE Wired keyboards and mice don’t need a separate power connection. Their power is provided by the PS/2 or USB port. With wireless keyboards and mice, a wireless RF receiver plugs into (and is powered by) the USB port on the computer, but the wireless keyboard or mouse needs battery power.

Pointing Devices

Mice and other pointing devices such as trackballs and touchpads are input devices that enable you to move a cursor around the screen and click things (Figure 3-20). Mice designed for Windows computers traditionally have two buttons, and this standard has evolved to include a scroll wheel in the center that enables you to move up and down in a window, as if you were clicking the scroll bar. They use the same Type-A USB or PS/2 connectors as keyboards.

https://t.me/learningnets



Figure 3-20 Various pointing devices



NOTE Mice for Apple Mac computers traditionally had only one button, but modern Mac mice have two buttons and a scroll area in the middle.

Mice originally came with a rubber ball on the bottom. When you move the mouse around, sensors inside track the ball's rotation and translate it to the screen. These *ball mice* collect dust and grime on the sensors and must be cleaned periodically. Modern *optical mice* use an LED or laser to track their movement.

Mice aren't the only game in town. A *trackball* is like a ball mouse but with the ball atop the device where you can manipulate it with a finger to move the cursor. Trackballs are great if you don't have a good surface or have wrist problems. You can also drag your fingers across a touch-sensitive *touchpad* to

https://t.me/learningnets

move the pointer (and tap it to click). Most laptops have a built-in touchpads, and you can find stand-alone versions for desktops.

A variant of a touchpad, called a *drawing tablet*, uses an inkless *stylus pen*. Where the pen touches the drawing tablet, it changes the electrical flow through a grid of underlying wires to send data to the computer. Drawing tablets are used by professional artists, drafters, and engineers to create computer graphics, blueprints, and designs.

A joystick is a fun input device that many gaming enthusiasts use to play certain kinds of games, like flight simulators. It's an upright vertical "stick" mounted in a base that allows it to tilt in any direction, and it typically has buttons or triggers on the stick to allow for selecting (or, as the case may be, firing missiles at alien invaders).

Other Common I/O Devices

Computing devices offer a phenomenal amount of adaptability to various tasks. Plug in the correct device, and you can turn a simple portable computer into DJ-jamming sonic experience. The only thing missing will be the disco ball. Plug in different devices and turn the same machine into a miniature office, complete with printing and faxing capabilities.

This section explores the typical devices used today to extend the capabilities of computing devices. We'll discuss audio devices, imaging peripherals, and printers and fax machines.

Audio Devices

Audio controllers enable the computer to play and record sound. All modern computers come with sound controllers built into the motherboard, but older systems needed add-on sound cards. The simplest sound controllers have three 3.5-mm audio ports (jacks), while more complex sound controllers have five or six jacks (see Figure 3-21). Each jack traditionally handles a specific audio input or output, although manufacturers use autosensing controllers on many portables. Most manufacturers use the color-coding scheme in Table 3-1.

https://t.me/learningnets

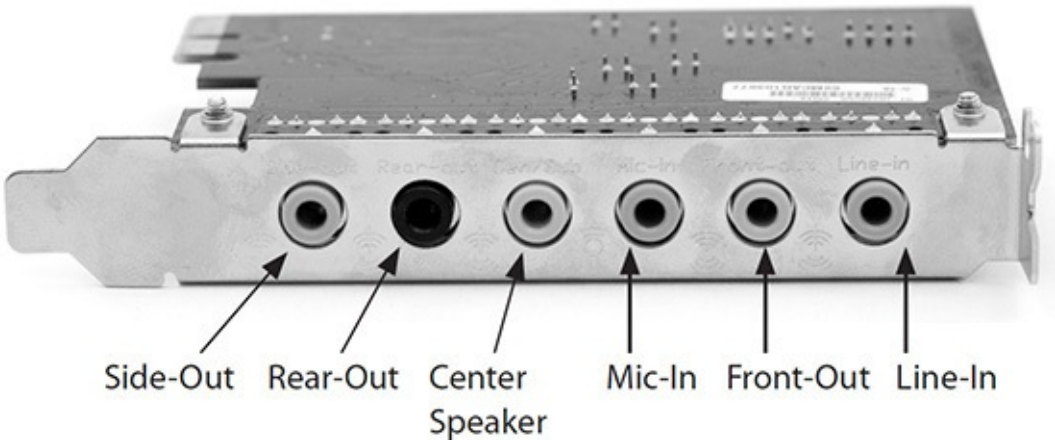


Figure 3-21 3.5-mm audio jacks on an add-on sound card

Connector	Color	Purpose
Line-out	Green	Main speakers or headphones
Microphone	Pink	Recording sounds
Line-in	Blue	Sound input from an audio device
Subwoofer	Orange	Thumping bass with a subwoofer attached
Rear surround sound	Black	Rear speakers
Middle surround sound	Gray	Extra speakers in a 7.1 sound setup

Table 3-1 Names and Color Codes for 3.5-mm Audio Jacks



EXAM TIP If you've connected a pair of headphones to a cell phone or portable media (cassette, CD, MP3, DVD) player in the past few decades, you've almost inevitably used one of these audio jacks. These are smaller than the full-size headphone jacks used in higher-quality home audio equipment (don't worry—the full-size version isn't on the exam). If you aren't familiar with the 3.5-mm connector, flip back to Figure 3-7.

Wireless Sound Connectivity

https://t.me/learningnets

Modern computing devices such as smartphones, tablets, and laptops can use Wi-Fi and/or Bluetooth wireless connectivity for connectivity to sound devices. The primary differences between the two wireless standards are that Bluetooth has a much shorter transmission range than Wi-Fi and Bluetooth doesn't use an IP address as Wi-Fi devices do.

You could, for example, use Bluetooth from your smartphone to connect to a Bluetooth speaker to play music available on or through your phone through the speaker. Just remember if you do this with a smartphone, you won't be able to go much more than approximately 10 meters (32 feet) away before the signal is choppy and then eventually lost.

In contrast, with a Wi-Fi speaker, a friend living in another country could play their music playlist through your local speaker!

Sound Output

A computer uses the sound processor and audio software to play music and sounds through speakers or headphones. Better motherboards offer high-definition audio processors.

Many users replace cheap bundled speakers with higher-quality systems, like the 2.1 system shown in Figure 3-22. In any *x*.1 speaker set, the *x* refers to the number of stereo speakers or satellites, and the 1 refers to the subwoofer (which provides the bass).



Figure 3-22 Klipsch ProMedia 2.1 speakers

https://t.me/learningnets



NOTE You can create a surround-sound experience in a media room with 5.1 or 7.1 speaker sets. These have a single subwoofer and multiple satellites for *surrounding* the listener.

Sound Input

A computer can also use the sound processor, the audio software, and a microphone or other audio device to record sound. All operating systems come with some (often limited) recording capability. Most desktops have at least a microphone (or mic) port, though portable computers may only have a built-in mic (don't despair—you can find excellent USB audio peripherals). Still, recording a great song or podcast may require more robust software, microphones, and other hardware.

Imaging Peripherals

Manufacturers create many computing devices dedicated to capturing and digitizing visual information, but the CompTIA IT Fundamentals exam focuses on two such peripherals: scanners and webcams. There's an argument for including fax machines here, but we'll look at those alongside printers and multifunction devices. Most modern imaging devices connect via USB, Bluetooth, or Wi-Fi.

Scanners

Scanners make digital copies of existing paper photos, documents, drawings, and other items. Some can copy directly from a photographic negative or slide, providing images of stunning visual quality (if the original was decent).

These days, traditional *flatbed* consumer-grade scanners are usually combined with a printer to make a multifunction device. You can also find scan-only devices for various purposes. A camera-based *document* or *book scanner* combines a digital camera with some hardware for positioning it squarely above a book or document, and sheet-fed document scanners can be found in desktop or travel-friendly formats for scanning full-size documents, receipts, business cards, and so on.

Digital Cameras

https://t.me/learningnets

Not that we have anything against your smartphone and selfie stick, but a dedicated digital camera or camcorder can offer higher quality, features tuned to the task at hand, and more room for creativity. While cameras and camcorders are converging and can each shoot still photos and video, consumer cameras are designed around shooting photos, and camcorders are designed for comfortable continuous recording.

The only digital cameras in the CompTIA IT Fundamentals objectives, *webcams*, tend to have modest, bandwidth-friendly resolutions that serve their primary mission: video calling and chatting over the Internet. You may already be familiar with this concept if you have a smartphone with rear- and front-facing cameras; the high-quality camera on the back of the phone functions as a traditional digital camera for taking pretty pictures, and the lower-quality front-facing camera functions as a webcam for video chat, messaging, and so on.

Webcams often come built into portable computers, all-in-one desktop computers (where the computer and monitor are integrated), and even some stand-alone monitors, but you can also buy stand-alone USB models. The webcam in Figure 3-23 includes a microphone, a typical feature. You can also use a separate stand-alone mic or headset.

https://t.me/learningnets



Figure 3-23 A stand-alone HD Pro Webcam C920 (courtesy of Logitech)

Printers and Fax Machines

Printers, as you probably know, output data (such as text and images) to paper. There are even printers capable of outputting three-dimensional objects made of plastic, metal, concrete, and chocolate—but the exam focuses on the more mundane two-dimensional kind. You don't see many stand-alone fax machines anymore, but fax technology is often included in all-in-one (multifunction) printers.

Let's look first at printer technologies and then examine costs associated with

https://t.me/learningnets

consumables and then at fax technologies and multifunction devices. After that, we'll discuss setting up printers and multifunction devices.

Printer Technologies

Manufacturers have created many types of printing devices over the years and have incorporated various technologies to get text and images from the monitor to the physical object. You need to know four printing technologies for the exam: impact, inkjet, laser, and thermal.

Impact Printers *Impact* printers create an image by physically striking an *ink ribbon* against the paper's surface, which makes them relatively slow and noisy. Impact printers are largely gone from our homes, but one kind—the *dot-matrix* printer—is still common in businesses because they can print to multipart forms. Point-of-sale machines, for example, use special *impact paper* that can print two or more copies of a receipt. Dot-matrix printers (see Figure 3-24) have a *printhead* that holds the pins or *printwires* that strike the inked ribbon, and many use tiny sprockets to advance *tractor-feed impact paper*.

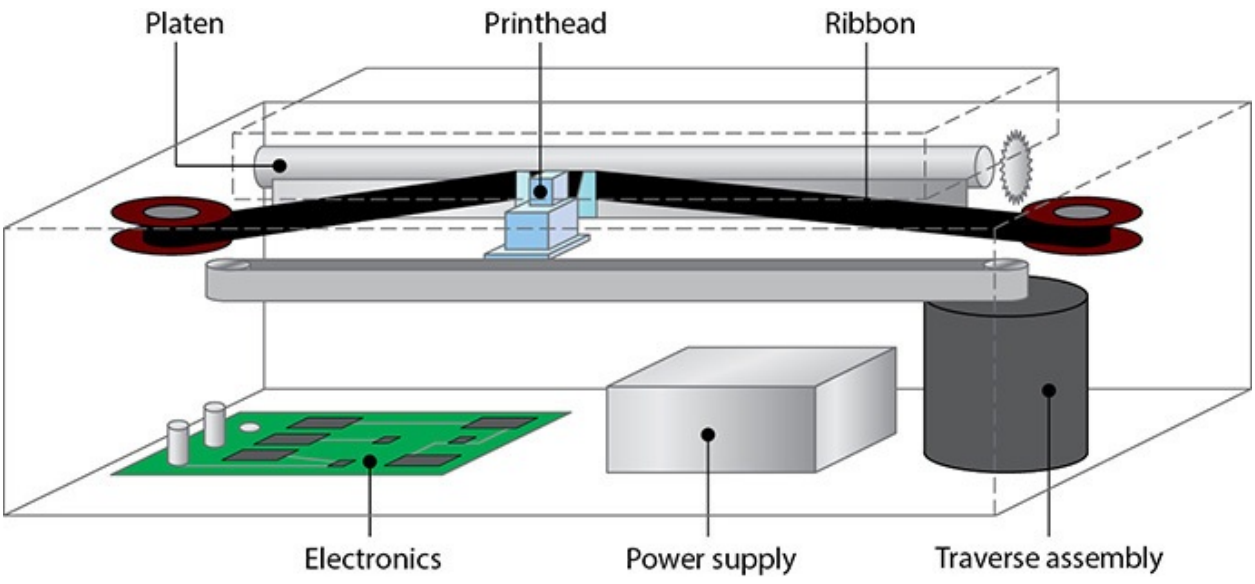


Figure 3-24 Inside a dot-matrix printer

Inkjet Printers *Inkjet* printers squirt ink out of special cartridges and combine ink colors to create a wide range of hues suitable for printing text and images. Inkjet printers use liquid ink cartridges. The process starts with a *friction feed* mechanism in which small rollers press down on paper stacked in the tray and

https://t.me/learningnets

pull a sheet through the printer. On its way through, most liquid inkjet printers use heat to eject ink through hundreds of tiny nozzles on the printhead (see Figure 3-25) and onto the paper. The other type uses pressure to move the ink through the printhead.

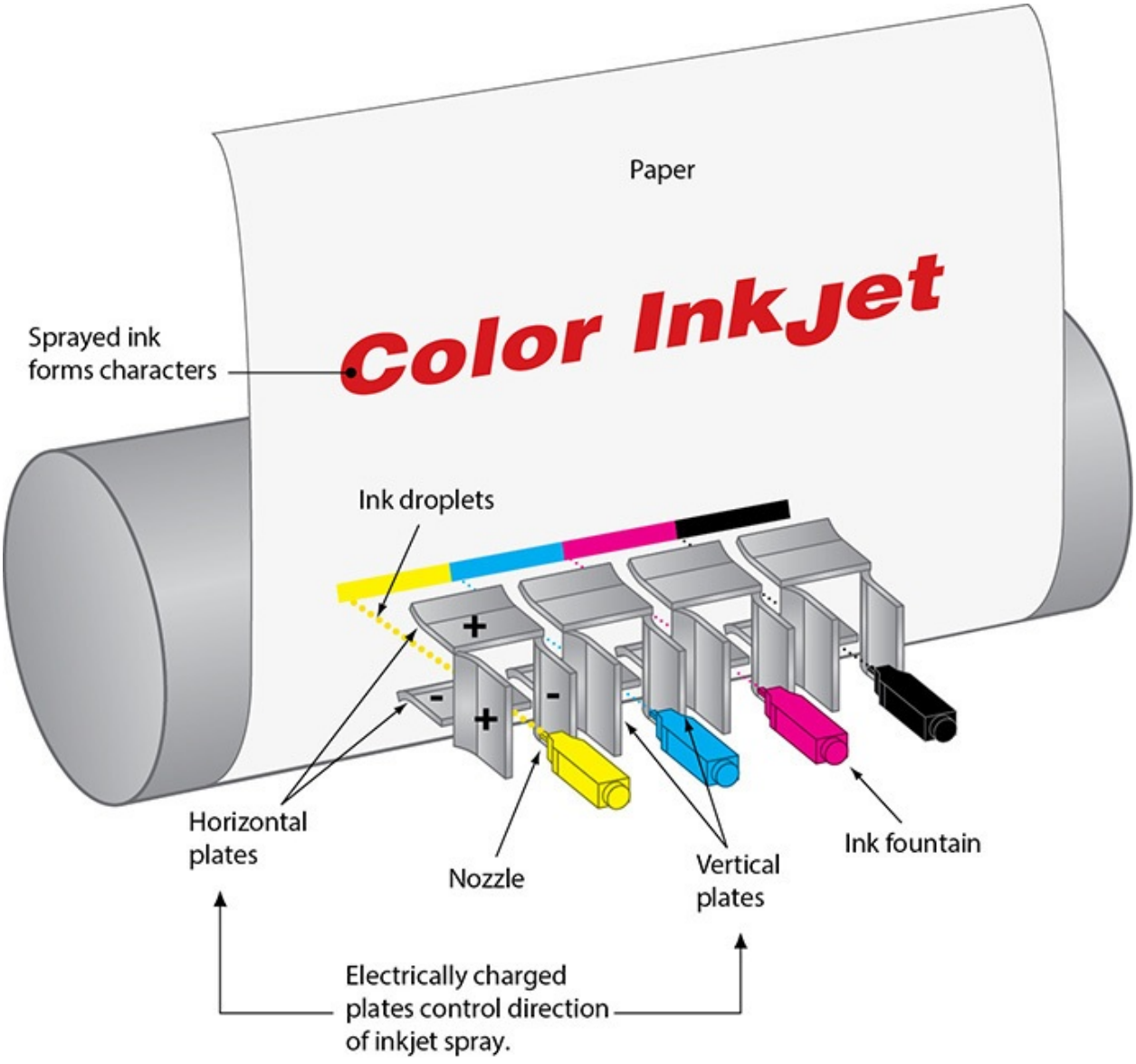


Figure 3-25 Detail of an inkjet printhead

Laser and LED Printers Laser printers (such as the one in Figure 3-26) rely on certain organic compounds that conduct electricity when exposed to light. Lasers can do this precisely, though some cheaper "laser" printers do a lower-quality job with LEDs.

https://t.me/learningnets



Figure 3-26 A typical laser printer



NOTE Printer resolution is measured in dots per inch (dpi) and speed in pages per minute (ppm). Higher is better.

Inside a laser printer, a spinning drum gets magnetized and demagnetized by the laser, and other components, which are tiny iron particles wrapped in plastic (called *toner*), jump to the drum. The printer transfers the toner to the paper and then melts it in place. That's why paper coming fresh from a laser printer feels a little warm to the touch. Toner is essentially the laser printer's ink.

Color laser printers, just like color inkjets, need multiple types of toner to match the primary colors. Color laser printers used to be expensive but have become much more affordable in the past couple of years. Snatch one up!

Thermal Printers *Direct thermal printers* selectively heat specially coated paper so that the heated areas turn black. Common uses are receipt printers and stand-alone fax machines. They don't print pretty pictures since they can't do gray, but they are simple, durable, and cheap to run.

Thermal transfer printing uses a heat-sensitive film ribbon instead of heat-

https://t.me/learningnets

sensitive paper and can even print in color with a wax-based film ink that melts onto the paper.

Printer Consumables

Printers, like all other good pets, cost more to feed and maintain than to buy; there's also a *cost per page* that accounts for ink/toner, paper, and parts that eventually wear out and must be replaced (such as the drums on laser printers). If you print often, don't let a low purchase price trick you into getting taken for a ride over the long term.

Inkjet printers are cheap, but ink cartridges are expensive per page. Laser printers cost more to buy, but toner is cheaper per page than ink. Over time, therefore, inkjet printers cost more to operate than laser printers. If you can live with their limitations, direct thermal printers are the cheapest to operate, requiring only thermal paper.



NOTE Printers tend to generate a lot of waste paper and cartridges, the latter containing chemicals we don't want in our food, water, or air. At a minimum, check with the local sanitation department or disposal service company before throwing away components. But really, recycle everything you can. Cartridges often come with a mailer to return them for reuse, and some companies will pay good money for used toner cartridges.

Fax Machines

Fax machines predate personal computers. A fax machine is both an input device and an output device; it scans a hard copy and then converts it to digital data and transmits it across telephone lines using a built-in modem to another fax machine. At the receiving end, a fax machine functions as a printer, re-creating the original hard copy.

The original fax machines included direct thermal printers. As a result, they required special thermal paper, and they printed only black and white (no gray shading). Today's fax machines, however, use laser or inkjet technology, so they can receive faxes in grayscale or in color.

While stand-alone fax machines are still sold, it is much more common to find faxing built into a multifunction printer.

https://t.me/learningnets

Multifunction Devices

A *multifunction device* (MFD) is also called a *multifunction printer* or *all-in-one printer*. This is a printer with one or more other devices rolled in. The typical MFD combines a printer, copy machine, scanner, and fax machine in one unit.

MFDs don't cost much more than regular printers, so you can make out like a bandit if you need the additional functions. Figure 3-27 shows a typical multifunction device with a feed tray for the scanner and copier portion and a variety of slots for memory cards on the lower right.



Figure 3-27 A multifunction device

Setting Up Printers and MFDs

After you unpack a new printer or MFD, you have a couple of steps to take before you can use the device. Essentially you plug it into the computer and install software to support the device. Printers and MFDs bring a couple of wrinkles to the process, though, so you need to read the documentation thoroughly. Some devices require you to start installing the software and plug the device in during that process.

Printers today connect in one of three ways: through USB directly to a

https://t.me/learningnets

computer, plugged into a switch, or connected wirelessly for availability to all network devices. FireWire printers were a thing for a short period of time. Much older printers connected to one of two now-extinct ports, the parallel and serial ports. Parallel ports were 25-pin ports; serial were 9-pin. Both used a D-shaped format appropriately called a *D-shell*.



EXAM TIP FireWire, parallel, and serial printer connections went away a long time ago. Questions involving them may show up on the CompTIA IT Fundamentals exam. Be prepared.

Installing software for a printer is pretty straightforward. Place the installation media—usually a CD that came with the printer—and follow the instructions on the screen.

Installing software for an MFD, on the other hand, can get tricky. You're essentially installing four or five different devices after all, so you need to follow the manufacturer's instructions carefully.

Note that you need to install software for every computer that will use the printer or MFD. This can trip up newer computer users, especially if they move a printer from one computer and plug it into another one. Even a known-good printer won't work without the software installed.

Chapter Review

In this chapter, you learned about many of the devices you can connect to a computer and the slots and connectors you use to do so. Most contemporary expansion cards use PCIe, with intensive cards such as video adapters typically using a 16-lane (×16) slot and less-demanding cards using ×1, ×4, or ×8 slots. USB is the predominant external expansion port, though it's important to recognize the many USB versions and connector types for compatibility and performance reasons. Other important connectors include Thunderbolt, FireWire, eSATA, RJ-45, and 3.5-mm audio, as well as older (rare) connectors such as PS/2, RJ-11, legacy parallel, and legacy serial.

Flat-screen displays (including LCD, LED, and OLED) are ubiquitous these days, but you may also encounter CRT and projector displays. There are tons of ports and connectors that can carry video signals, though only a few (DVI,

https://t.me/learningnets

HDMI, DisplayPort/Thunderbolt, and USB 3.*x*) can handle modern high-definition video; you should be able to recognize other connectors such as VGA, composite video, S-Video, component (RGB) video, and older generations of USB, but use them only as a last resort. Some recent displays are also integrated with touchscreen technology, which enables them to double as both input and output devices.

The ports introduced early in the chapter enable you to connect common input and output peripherals such as keyboards, pointing devices (mice, trackballs, touchpads, drawing tablets, joysticks), and devices for inputting and outputting sound, images, and video. Modern devices such as printers and speakers also allow wireless connectivity through Bluetooth and Wi-Fi. Finally, we examined a few key printer technologies such as inkjet, laser, and thermal printers, including how to manage the "consumables" such as paper and ink.

As you finish studying the material in this chapter, make sure that given a device, you can say whether it is for input, output, or both. Here's a list of the device types to know:

Input	Output	Both Input and Output
Keyboards	Printers (laser, inkjet, thermal)	Fax machines
Pointing devices (mouse, touchpad, joystick, stylus pen, trackball)	Displays (flat screen, CRT, projector)	External storage devices (covered in Chapter 4; these include flash drives, external hard drives, optical drives, network-attached storage, memory cards, mobile media players, and smartphones)
Scanners	Speakers	Touchscreen displays
Microphones		
Webcams		

Questions

1. A video card on a modern motherboard would run best in which type of slot?
   - **A.** PCI
   - **B.** PCIe
   - **C.** VGA
   - **D.** DVI
2. Which port is used exclusively for external hard drives?
   - **A.** FireWire
   - **B.** USB

https://t.me/learningnets

C. eSATA

D. PS/2

3. Which of these external ports is *not* obsolete?

A. FireWire

B. Legacy parallel

C. Legacy serial

D. PS/2

4. What type of connector does a modem use?

A. PS/2

B. RJ-45

C. 3.5 mm

D. RJ-11

5. The USB connector that plugs into a full-size printer is:

A. Type-A

B. Type-B

C. Mini-B

D. Micro-B

6. Which of these is *not* a flat-panel display?

A. OLED

B. LCD

C. Plasma

D. CRT

7. Which of these ports are physically identical?

A. USB Type-A and USB Type-B

B. Thunderbolt and Mini DisplayPort

C. DisplayPort and FireWire

D. DVI and VGA

8. What is the purpose of a wheel on a mouse?

A. Scrolling the display

B. Greater precision of pointer movement

C. Right-clicking alternative

https://t.me/learningnets

D. Locating the pointer

9. A video camera that works only when connected to a computer is a:
   - **A.** Scanner
   - **B.** Digital video camera
   - **C.** Megapixel camera
   - **D.** Webcam
10. A receipt printer on a cash register is likely to be what kind of printer?
   - **A.** Inkjet
   - **B.** Laser
   - **C.** LED
   - **D.** Thermal

Answers

1. **B**. PCIe is correct. PCI is an older type of slot that is slower and less desirable for video cards. VGA and DVI are not slot types.
2. **C**. eSATA is correct. FireWire and USB can be used for external hard drives, but they also have other uses. PS/2 is an old port used for keyboards and mice, not hard drives.
3. **A**. FireWire is correct. All the others are obsolete.
4. **D**. RJ-11 is correct. PS/2 is an old port used for keyboards and mice. RJ-45 is used for wired Ethernet networking. The 3.5-mm connector is used for audio ports.
5. **B**. Type-B is correct. Type-A is the standard full-size USB connector on a PC. Mini-B and Micro-B plug into smaller devices.
6. **D**. CRT is correct. All the other types are flat-panel displays.
7. **B**. Thunderbolt and Mini DisplayPort are correct. The other pairs are not identical.
8. **A**. Scrolling the display is correct. The other actions are not controlled by the mouse wheel.
9. **D**. Webcam is correct. A scanner is not a video camera. A digital video camera can be removed from a computer and used independently. A megapixel camera is a still camera that supports at least 1 million pixels in

https://t.me/learningnets

resolution.

10. **D**. Thermal printing is common on cash registers because of the low cost of consumables. The other answer choices are types of printers but not the most likely choice for a cash register.

https://t.me/learningnets

CHAPTER 4

Data Storage and Sharing

In this chapter, you will learn how to

- Differentiate among types of storage
- Choose appropriate storage locations

This chapter reviews the current storage and file-sharing landscape. We'll start with three common storage technologies: magnetic, optical, and solid state. Then we'll evaluate the available options for local, network, and online storage.

Storage Technologies

Modern computers can store enormous programs, documents, and media files on spacious storage devices. An understanding of how we measure the size of these devices is important for comparing them. Let's start there.

In computing, file sizes and disk storage capacity are measured in *bytes*. One byte is eight binary digits (*bits*). A binary digit is either a zero or a one and is the smallest unit of storage on a computer. Storage devices are available in different capacities measured in some multiple of bytes. Most files are measured in kilobytes or megabytes, but storage drives are currently measured in gigabytes and terabytes. ASCII is an industry standard used to represent 8-bit characters in the English language across different computing platforms; unicode represents characters from most spoken languages in addition to English. Refer to Table 4-1 for a summary of capacity measurements.

https://t.me/learningnets

Unit	Exact Amount	Notes
Kilobyte (KB)	1,024 bytes	Approximately one thousand bytes
Megabyte (MB)	1,024 kilobytes	Approximately one million bytes
Gigabyte (GB)	1,024 megabytes	Approximately one billion bytes
Terabyte (TB)	1,024 gigabytes	Approximately one trillion bytes
Petabyte (PB)	1,024 terabytes	Approximately one million gigabytes

Table 4-1 Storage Capacity Measurements



EXAM TIP The list of CompTIA IT Fundamentals acronyms includes kilobit (Kb), megabit (Mb), gigabit (Gb), and terabit (Tb). Note the lowercase *b*, which indicates bits, not bytes. (Recall that a byte is 8 bits.) Storage is described in bytes, such as 100 GB. Data transfer rates are usually described as a certain number of bits per second, as in 1 Gbps.

Don't confuse bits or bytes with *hertz*, as in megahertz (MHz) and gigahertz (GHz), describing a certain number of processing cycles per second for a central processing unit (CPU).

These days, most data is stored on magnetic, optical, and solid-state storage devices. Most storage devices are internal (they mount inside the computer case), but you'll also see some external storage devices that connect via an external port and may have an additional source of power. Let's take a look at the different mechanisms these devices use to read and write data.



NOTE The section "Storage Locations" examines the different interfaces that internal and external drives use.

Magnetic Storage

Magnetic storage encodes data in patterns of positive and negative magnetic polarity on some magnetic medium. In previous decades, there were different

https://t.me/learningnets

kinds of magnetic storage such as floppy disks or zip disks, but the only ones left standing are hard disks and magnetic tapes. You won't see magnetic tape on the exam, but it is cost effective in large archival systems where it may well soldier on for years or decades after most hard disks are retired.

A *hard disk drive* (HDD) is a sealed metal cartridge with a stack of metal platters inside (Figure 4-1). Modern consumer HDDs range from 500 GB to 10 TB, but you may see older systems with smaller disks.



Figure 4-1 Inside a hard disk drive

The platters are coated with iron dust, and each side of each platter has a separate read/write head. The platters spin under the read/write head, which uses an actuator arm to access data from the outside to the center. The drive's *integrated drive electronics* (IDE), a controller that translates requests from the PC into action, tells the heads where to read or write.

https://t.me/learningnets



NOTE The terms *hard disk drive*, *hard disk*, and *hard drive* are all synonymous because the disk and drive can't be separated without destroying the unit. In contrast, optical media (such as CDs, DVDs, and BDs) are separate from the drives that read them.

Once HDD platters spin up, they spin at a constant *rotation speed*; the most common speeds are 5,400; 7,200; and 10,000 revolutions per minute (rpm). Higher rotation speeds result in more noise, faster transfers, more power consumption, and greater cost. Modern drives have a small RAM cache to help get data to and from the drive faster. Standard cache sizes are 16, 32, 64, and 128 MB (see Figure 4-2).



Figure 4-2 Hard drive package advertising rotation speed and cache size (photo courtesy of Western Digital)

Optical Storage

Optical discs (note the spelling of *disc* versus *disk*) store data in reflectivity patterns on a shiny surface. Common optical discs include CDs, DVDs, and BDs. Unlike with HDDs, optical discs are removable from the drives that read them, so the *optical disc* and *optical drive* are two different things. The optical drive (which may be internal or external) measures how much laser light the disc reflects.

You should be familiar with these generations of optical media in use, all of which you can find in single or double-sided varieties:

https://t.me/learningnets

- The *compact disc* (CD) initially became popular for distributing music but later became the standard for distributing computer programs and data.
- The *digital versatile disc* (DVD) was developed to distribute standard-definition movies, but software distribution followed for programs too large to fit on a CD. DVDs can also be single-layer or double-layer (the drive uses a different laser angle to read each layer). Double-layer discs have a -DL suffix, as in DVD-DL.
- The *Blu-ray Disc* (BD) was designed for high-definition movies. The name comes from the blue laser these drives use (rather than the red laser used in CD and DVD drives). Blu-ray Discs are also available in triple-layer and quadruple-layer versions, called *Blu-ray Disc XL* (BDXL).

The combination of these various features means there are a number of potential capacities (summarized in Table 4-2) for each disc technology. The drives are backward compatible, so a Blu-ray Disc drive can read both DVDs and CDs, and a DVD drive can also read CDs.

Disc Type	Layers	Capacity (Per Side)
CD	1	700 MB
DVD	1	4.7 GB
DVD	2	8.5 GB
BD	1	25 GB
BD	2	50 GB
BDXL	3	100 GB
BDXL	4	128 GB

Table 4-2 Optical Disc Capacity

Optical drives have a maximum rate at which they can read or write to a disc expressed in multiples of the technologies' base rate (for example, 1×, 48×, or 150×), and more is better. Each generation has a faster base rate (but you don't need to know these for the exam). Early optical drives were read-only, but modern ones can also write (and rewrite) to a variety of optical discs. In this case, you'll typically see multiple speeds for reading, writing, and rewriting.

Discs that cannot be written to have a ROM suffix, as in CD-ROM, DVD-

https://t.me/learningnets

ROM, and BD-ROM.

Some writeable discs can be written only once; these typically end in R (as in CD-R, DVD-R, and BD-R). Once the disc surface has been changed, it can't be redone. Discs that end in RW or RE (as in CD-RW, DVD-RW, and BD-RE) have a different kind of metal surface; the drive can write at one temperature and erase at another.



NOTE Writeable DVDs have two different standards, referred to as *plus* and *minus*. For single-write DVDs, you'll find DVD+R and DVD-R discs; most drives support both, but make sure.

Solid-State Storage

Instead of disks (or discs), solid-state storage uses nonvolatile (*flash*) memory that can retain data when powered down. This technology has no moving parts. Solid-state storage is more expensive per gigabyte than disk-based storage, but it is also lighter, faster, quieter, and more efficient. Because there isn't a disk, flash media can take many creative forms. Here are the most common:

- A USB *flash drive* (Figure 4-3) is a stick of highly portable storage that plugs into a USB port.

https://t.me/learningnets



Figure 4-3 Inexpensive USB flash drives easily fit in a pocket or backpack.

- Flash *memory cards* are used in devices such as digital cameras, smartphones, and navigation devices. A prolific photographer will carry several, swapping out full cards for empty ones. You can transfer images off the camera with a cable or just pop the card out and insert it in a memory *card reader* (see Figure 4-4). Either way, the computer treats it like a drive. The most common formats are CompactFlash, Secure Digital (SD), MemoryStick, and MicroSD.

https://t.me/learningnets



Figure 4-4 Memory cards fit into built-in or separate card readers.

- Hard drives made with flash memory, called *solid-state drives* (SSDs), are more expensive per gigabyte but have quickly matured to the point where drives large enough to support the average user are affordable. Tablets and smartphones have an *embedded multimedia controller* (eMMC) containing flash memory permanently built into the device.

Local storage is physically connected to the individual computer accessing it. It is always available on that device, fast (because it doesn't have to travel far), and convenient. The catch is that it's available *only* on that device. *Network storage* is connected to a local area network (LAN) to share files with other devices on the same LAN. Businesses use network storage extensively to make sure all employees have access to important data and applications. A computer can access network storage only as long as it remains connected to the network.

But what if the devices aren't on the same network? That's when you turn to *online storage*, one form of which is *cloud storage*, where files are available anywhere in the world via the Internet. Let's look at these locations in more detail.

https://t.me/learningnets

Local Storage

Local storage, also called *direct attached storage* (DAS), has a direct internal or external connection to the device accessing it. Internal storage devices are physically located inside the main case of the computer, share its power supply, are harder to steal quickly, and don't take up desk space. On almost all systems, the primary hard drive is internal. Internal drive interfaces have historically been faster than external ones, but modern interfaces such as eSATA, USB 3.1, and Thunderbolt are just as fast (or faster).

Modern internal hard drives connect with *serial ATA* (SATA) connections, including a five-wire SATA connector from the power supply (see Figure 4-5) and a seven-wire SATA data cable from the motherboard (see Figure 4-6). Both connectors are keyed so you can't plug them in incorrectly.



Figure 4-5 A SATA power cable

https://t.me/learningnets



Figure 4-6 A SATA data cable

The older (now-obsolete) *parallel ATA (PATA)* drives used a wide 80-wire ribbon cable for data (Figure 4-7) and a 4-wire Molex connector for power (Figure 4-8). You might occasionally see these in an older desktop PC, particularly with an internal optical drive.

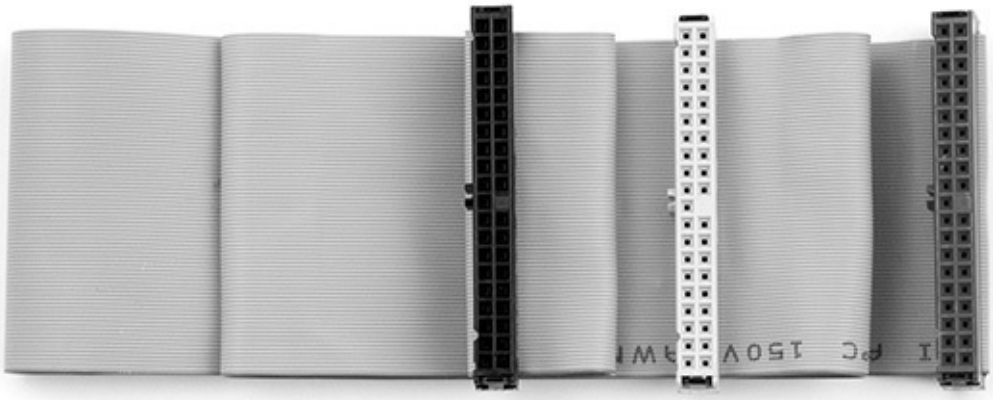


Figure 4-7 An 80-wire ribbon cable

https://t.me/learningnets

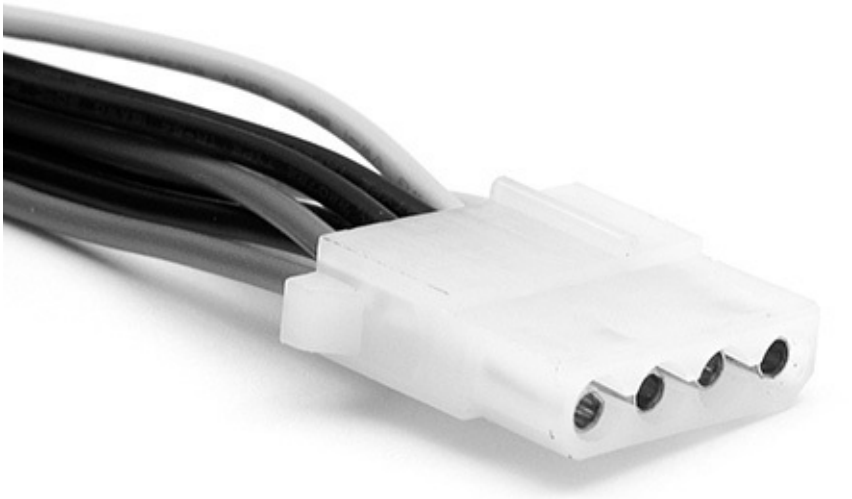


Figure 4-8 A Molex connector

External Storage

External storage connects to external ports. Some drives will draw all of their power from the port, but others may need an additional alternating current (AC) adapter.

The most common interfaces (shown in Figure 4-9) for external storage are as follows:



Figure 4-9 From left to right: USB, Thunderbolt, FireWire, and eSATA

- **USB** Hi Speed USB 2.0 and USB 3.0/3.1 are fast enough for nearly any external storage device.

https://t.me/learningnets

- **Thunderbolt** Thunderbolt connections are also a good candidate for external storage, but Thunderbolt comes with a higher price tag than USB.
- **FireWire (IEEE 1394)** FireWire offered a viable alternative to USB but has faded in use. Some drives support both USB and FireWire, which can be nice if your USB ports are full.
- **External SATA (eSATA)** eSATA is specifically for connecting external SATA drives to the internal SATA bus at full speed.

Network Storage

Network storage or *hosted storage* is accessed over a LAN in your own home or office, a wide area network (WAN) with computers in different countries, or anything in between. This section discusses four options for network storage: file servers, NAS, shared volumes, and ad hoc networks.



NOTE Technically all Internet-accessed storage is network storage, but we'll discuss Internet storage later in this chapter.

File Servers

Networked computers called *servers* are dedicated full-time to assisting (serving) other computers. There are many kinds of server, including e-mail servers that store and forward e-mail, authentication servers that manage user identities, web servers that respond to requests for web pages, and file servers that grant users access to the server's local storage.

A *file server* has fast, high-capacity HDDs or SSDs for storing files that multiple users need to access. When users connect to the file server, they can view and edit files that they have permission to use.



NOTE Many file servers use *Redundant Array of Inexpensive Disks (RAID)* technology, which combines more than one physical drive working together to improve performance or protect against data loss. You can even use RAID on high-end desktop systems with the correct hardware.

https://t.me/learningnets

Network-Attached Storage

Network-attached storage (NAS) typically describes a simple stand-alone device that contains one or more hard drive slots, a pared-down file server, and a network connection. It doesn't have a keyboard, mouse, monitor, or full-blown operating system (users can interact with its simple operating system via a web browser); it just shares access to the installed hard drives.

NAS appliances designed for home use (see Figure 4-10) are sometimes marketed as *home media servers* since a common use is to share music and video collections within a household.



Figure 4-10 A network-attached storage appliance

https://t.me/learningnets

Shared Network Volumes

You don't *need* a file server or NAS appliance to share files on a LAN. You can share a local folder on your own PC with network users and set permissions that control who can view and edit that folder's content.

The main drawback to this kind of *peer-to-peer file sharing* is that the files are available only when your computer is on the network to act as a file server. If your computer is offline for some reason, nobody will be able to access the shared folder (this also applies when you share connected printers). See Chapter 10 for more information about setting up and using a local area network.



NOTE As a noun, a *network share* is a shared folder or printer.

Ad Hoc Networks

An *ad hoc network* connects devices directly without any "infrastructure" hardware such as a switch, router, or server. Some examples of ad hoc networks include the following:

- **Direct link** Two computers can be physically connected directly to one another via cables. When this is done via the Ethernet ports (RJ-45), you must use a specially wired cable called a *crossover cable*.
- **Ad hoc wireless network** In some cases you can use the wireless LAN adapters in two or more computers to create an impromptu network. Because of the security risks involved in this kind of network, modern versions of Windows have made doing so more difficult, though.
- **Bluetooth** A Bluetooth device such as a keyboard, mouse, headset, or printer might connect directly to a computer, tablet, or smartphone. Chapter 7 explains Bluetooth in more detail.

Online Storage

Online storage is, as you might guess, accessed via the Internet. Online storage is not that different from network storage because the Internet is itself a network. Most users will see it as distinct, though, because the software used to access it creates a different experience. The following sections look at three types of online storage: cloud, FTP, and web-based.

https://t.me/learningnets

Cloud Storage

As you learned in Chapter 1, *cloud computing* is the use of applications or data storage accessible over the Internet. Many commercial businesses with employees all over the globe use cloud computing to provide their employees with standardized applications and file storage no matter where they are.



NOTE As a smartphone user, you would normally store contact lists and documents such as photos in the cloud. This way when you get a new smartphone, all of these items are available to the new phone as long as you sign in to your cloud account.

You can access thousands of cloud-based services and applications for free or as a paid subscription. When you use Microsoft Office Online (www.office.com) to access files stored in OneDrive (Microsoft's online storage service), for example, you are cloud-computing. Other free cloud storage services include iCloud (Apple), Dropbox, and Google Drive.



EXAM TIP Because someone else does the work of hosting these online services, you can think of them as *hosted storage*.

File Transfer Protocol

File Transfer Protocol (FTP), which predates the Web, is one of the oldest types of online file sharing still in use today. It is still popular because it's a simple way to move files from one place to another.

FTP is a protocol (a set of standards or rules for accomplishing something) that FTP applications use to transfer files. FileZilla (shown in Figure 4-11) is a popular free FTP application (www.filezilla-project.org). FTP is sometimes used as a verb, as in "I'll FTP those over to you this afternoon." An FTP server supports file upload and download via the protocol.

https://t.me/learningnets

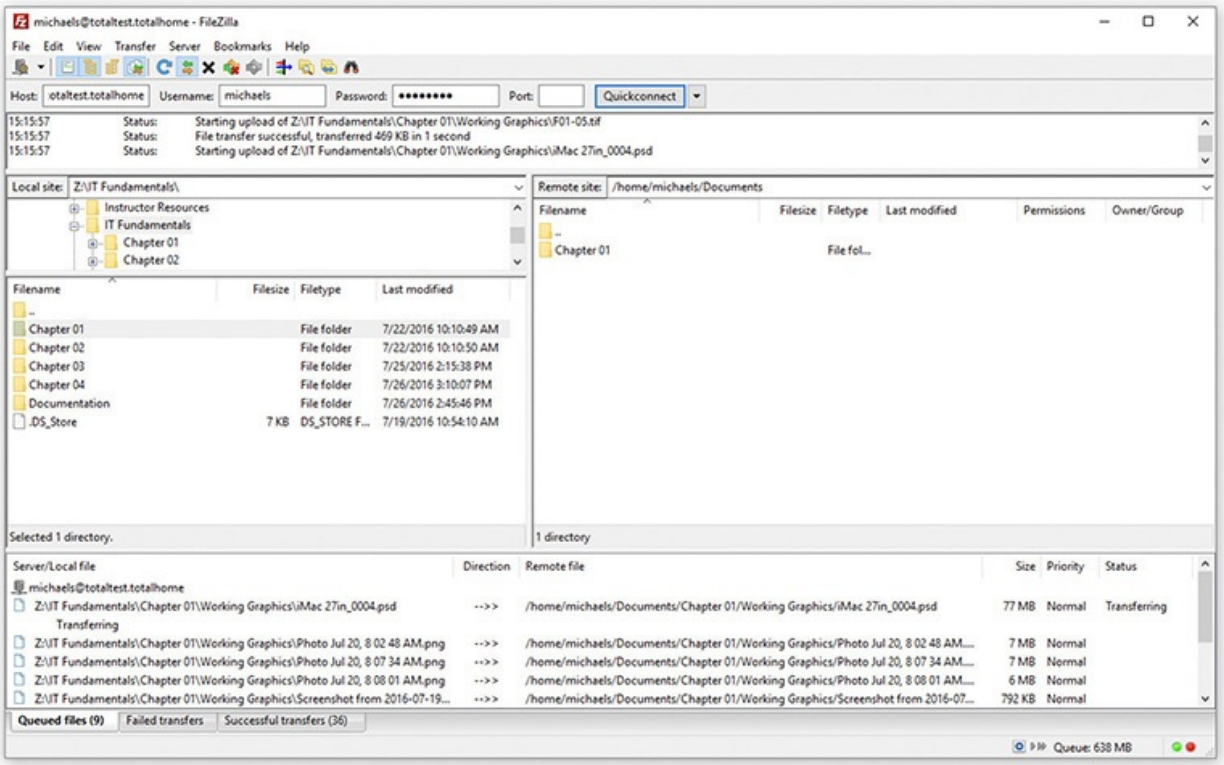


Figure 4-11 FileZilla transferring files via FTP

Like most protocols its age, FTP is not secure. It can require a login, but it sends the credentials (and any files you transfer) in the clear (without encryption) where anyone watching can see them. Developers have created multiple secure (encrypted) versions, including Secure FTP (SFTP) and FTP over SSL (FTPS), which you should use if possible. Despite the similar letters, SFTP and FTPS aren't synonyms.



EXAM TIP The CompTIA IT Fundamentals objectives expect you to compare FTP, FTPS, and SFTP as sharing and storage methods. While these acronyms are stable, people interpret them differently. CompTIA's list of IT Fundamentals acronyms uses *File Transfer Protocol over SSL* and *Secure File Transfer Protocol*, but you can find tons of variations in different resources, such as *File Transfer Protocol Secure* and *SSH File Transfer Protocol.*

FTPS secures the connection with either TLS or SSL, which you'll read

https://t.me/learningnets

more about in the next section. SFTP piggybacks on the Secure Shell (SSH) protocol.

Web-Based File Downloads and Storage

Many web sites have files you can download by clicking a hyperlink. Sometimes these are software or documents made by the site owner, but other file-sharing sites allow registered or even anonymous users to upload files. Beware these file-sharing sites. Outside of reputable app stores and developer web sites, there are few guarantees you aren't downloading a copy that is seeded with *malware*—programs that can damage your computer or steal from you.

For downloading and everything else you do online, it's important to understand that regular (insecure) web sites use the Hypertext Transfer Protocol (HTTP). Secure web sites, in contrast, use HTTP over SSL (HTTPS), a variant that establishes an encrypted link between the web server and the user's browser originally using a security protocol called Secure Sockets Layer (SSL). HTTPS-based web sites today use the more robust Transport Layer Security (TLS), but developers kept the original name of the protocol. You don't need to know how HTTPS and SSL work, but you should know how they indicate that they are keeping you safe.

- HTTPS (not HTTP) shows as the prefix for the address (shown in Figure 4-12) in the browser's address bar.



Figure 4-12 A secure address in Google Chrome (top), Internet Explorer, and Microsoft Edge (bottom)

- A lock symbol appears in the address bar.

Chapter Review

In this chapter, you learned the basics of how magnetic, optical, and solid-state storage works in a variety of modern devices. The magnetic storage you'll see

https://t.me/learningnets

most are the spacious hard disk drives that have dominated computing for years, though they are being slowly edged out by faster, lighter, and more-efficient solid-state drives as prices fall and capacities rise. Optical media and drives are still common, but they too have been shoved aside by two other solid-state memory formats: memory cards and USB flash drives.

You learned how to classify storage locations as local, network, or online; how systems connect to these types of storage; and the benefits and drawbacks of each location type. Local storage is directly connected from within your system or with an external expansion port such as USB, eSATA, or Thunderbolt, while network storage relies on wired (RJ-45) or wireless network connections to reach drives on other networked computers or in special file servers and NAS systems. Online, we have access to files through cloud storage, FTP servers, and direct downloads from web sites. Applications and data storage in the cloud play an important role in having access to the same data and software from multiple devices.

Questions

1. Which kind of device stores data in patterns of magnetic polarity?
   - **A.** DVD
   - **B.** CD
   - **C.** USB flash drive
   - **D.** HDD
2. Which unit of measurement describes approximately one trillion bytes of storage?
   - **A.** Terabyte
   - **B.** Gigabyte
   - **C.** Megabyte
   - **D.** Kilobyte
3. Which of these is *not* an optical disc?
   - **A.** DVD
   - **B.** SSD
   - **C.** BD-R
   - **D.** CD-RW

https://t.me/learningnets

4. How can a single DVD hold more than 4.7 GB of data? (Choose all that apply.)
   - **A.** Multiple actuator arms
   - **B.** Multiple sides
   - **C.** Multiple layers
   - **D.** High-density recording
5. Which type of optical disc is rewriteable multiple times?
   - **A.** DVD-ROM
   - **B.** BD
   - **C.** CD-RW
   - **D.** BD-R
6. What kind of drive reads CompactFlash storage?
   - **A.** USB flash drive
   - **B.** Card reader
   - **C.** HDD
   - **D.** SSD
7. Which of these is *not* a benefit of SSD over HDD?
   - **A.** Quieter
   - **B.** Uses less power
   - **C.** Faster
   - **D.** Less expensive
8. Which of these is an external storage connection?
   - **A.** ePATA
   - **B.** eSATA
   - **C.** PATA
   - **D.** SATA
9. Which of these is an ad hoc network?
   - **A.** PATA
   - **B.** NAS
   - **C.** RAID
   - **D.** Direct link with crossover cable

https://t.me/learningnets

10. Which of these is a secure protocol for transferring files?
    - **A.** SFTP
    - **B.** FTP
    - **C.** HTTP
    - **D.** USB
11. Which storage unit of measurement refers to millions of Gigabytes?
    - **A.** MB
    - **B.** GB
    - **C.** PB
    - **D.** TB

Answers

1. **D**. A hard disk drive (HDD) uses magnetic polarity to store data. DVD and CD are both optical, and a USB flash drive is solid state.
2. **A**. A terabyte is approximately one trillion bytes. A gigabyte is approximately one billion bytes, a megabyte is approximately one million bytes, and a kilobyte is approximately one thousand bytes.
3. **B**. SSD stands for solid-state drive. All the others listed are optical discs.
4. **B, C**. A DVD can have multiple sides and multiple layers. Optical drives do not have actuator arms. DVDs cannot have higher-density recordings than the standard for DVDs.
5. **C**. Rewriteable discs end in RW or RE. Discs that are not writeable end in ROM. Discs that are writeable only once end in R.
6. **B**. A card reader reads from a variety of flash memory cards, including CompactFlash. All other drive types listed contain their own storage and do not accept cards.
7. **D**. SSD has all the advantages listed except it is more expensive than HDD.
8. **B**. eSATA is external serial ATA. SATA and PATA are internal. There is no such thing as ePATA.
9. **D**. One kind of ad hoc network is a direct connection between two PCs using a crossover cable. PATA is a technology for an internal local hard drive connection. NAS is network-attached storage. RAID combines

https://t.me/learningnets

multiple hard disks into a single logical pool of storage.

10. **A**. SFTP is a secure form of File Transfer Protocol (FTP). HTTP is the protocol for web pages. USB is a type of external port on a PC.

11. **C**. A petabyte (PB) is approximately one million gigabytes. A megabyte (MB) is one million bytes, a gigabyte is one billion bytes, and a terabyte (TB) equates to one trillion bytes.

https://t.me/learningnets

PART II

Setting Up and Using Computers

- **Chapter 5** Understanding Operating Systems
- **Chapter 6** Setting Up and Configuring a PC
- **Chapter 7** Setting Up and Configuring a Mobile Device
- **Chapter 8** Managing Files
- **Chapter 9** Using and Managing Application Software

https://t.me/learningnets

CHAPTER 5

Understanding Operating Systems

In this chapter, you will learn how to

- Explain the functions of an operating system
- Discuss operating system characteristics
- Describe operating system interfaces
- Compare operating system features

Operating systems enable users of computing devices to interact with those devices in many ways. The various operating systems have features in common and stark differences. This chapter looks at the primary desktop operating systems you'll run into in the wild. While the CompTIA IT Fundamentals exam focuses a lot on Microsoft Windows, you'll get questions on three other desktop operating systems: Apple macOS, Linux, and Google Chrome OS. We'll start with an analysis of functions common to all operating systems and discuss characteristics of operating systems. Next, we'll survey the interfaces of the four most common desktop operating systems. The chapter finishes with a side-by-side comparison of features.



NOTE Chapter 7 dives into the three major operating systems for mobile devices—iOS, Android, and Windows Mobile.

The Functions of an Operating System

As you'll recall from earlier chapters, the *operating system* (OS) is a layer of software that enables the hardware and application software to work together. The OS also enables you to tell the computer what to do and enables the computer to show you the results. A typical OS performs five functions,

https://t.me/learningnets

summarized in Figure 5-1.

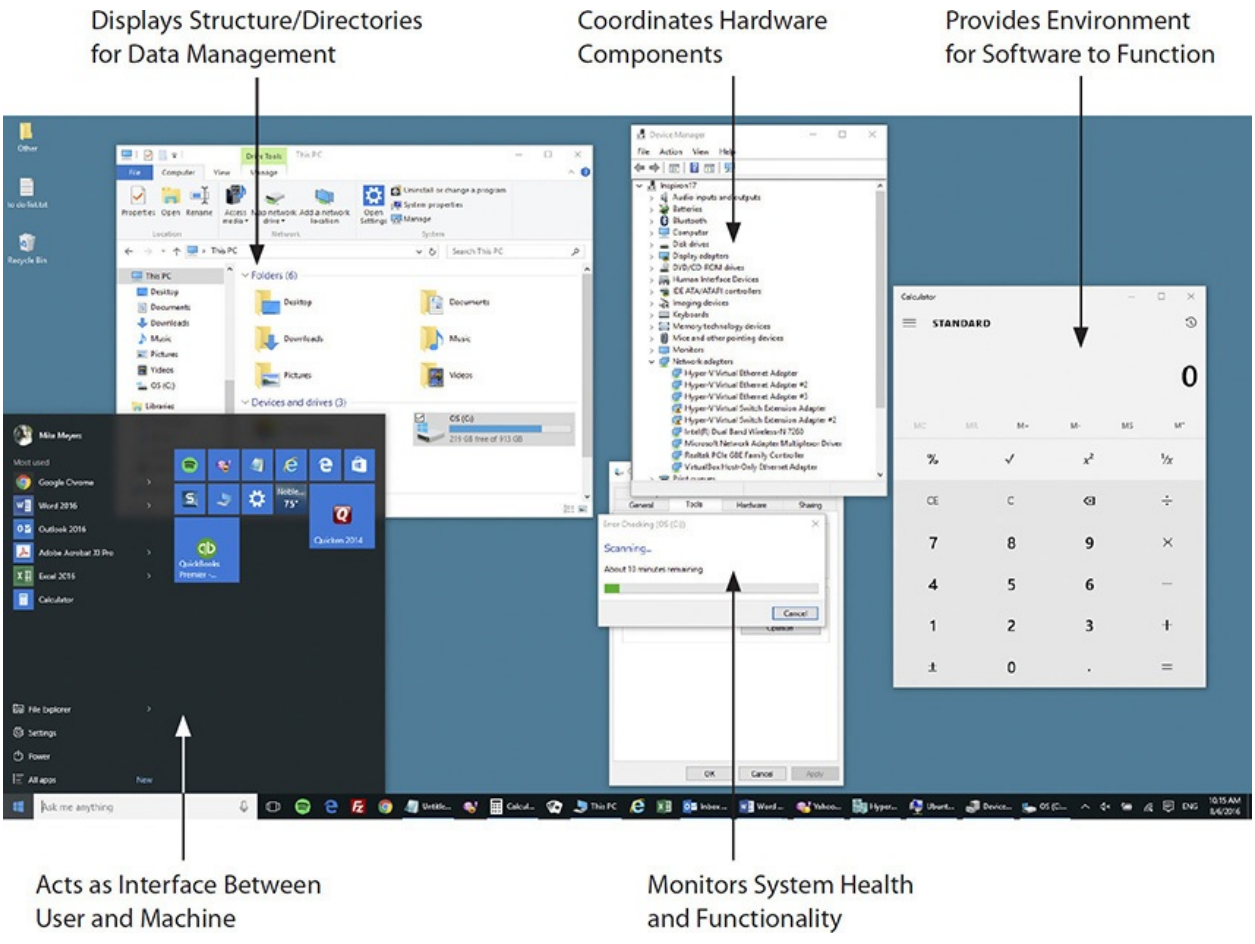


Figure 5-1 The five functions of an OS, illustrated in Windows 10

- *An OS provides an interface between user and machine.* This interface can be a graphical user interface (GUI) or a command line. A GUI enables you to click on-screen elements to interact with the OS. You type commands at the command-line interface (CLI) to tell the OS to do things.
- *An OS enables coordination of hardware components.* Each hardware device speaks a different language, but the operating system can talk to and manage them all through translation files called *device drivers*.
- *An OS provides an environment for software to function.* In GUI operating systems such as Windows and macOS, applications run within a consistent, graphical desktop environment.
- *An OS monitors system health and functionality.* Each OS comes with

https://t.me/learningnets

utility programs that help keep the system in good condition by checking storage drives for errors or monitoring system activity for malware.

- *An OS displays structure/directories for data management.* You can view file and folder listings and issue commands to act on those files and folders (move, copy, rename, delete, and so on).

Operating System Characteristics

Operating systems differ in three primary characteristics: licensing, software compatibility, and complexity. These different categories define strengths and limitations both among OS versions and among editions within those versions.

Operating systems vary depending on their intended use; there are OSs for user workstations such as desktops and laptops, OSs for servers, and OSs for mobile devices. Recall from Chapter 2 that many modern smaller special-use computing devices have an embedded OS that is just an OS stored within a hardware chip.

Licensing

Operating system developers want you to use their OS. They really do! They make their OS available to acquire in three basic ways: open source, free, or commercial.

As you learned in Chapter 1, Linux is an *open source* operating system, meaning that anyone can download and modify it. Open source operating systems can benefit from improvements contributed by thousands of programmers. Some people choose open source operating systems out of an anti-establishment spirit; others choose them as a practical matter because they are free.



NOTE *Public domain* software is a step beyond open source. Not only is it free to use and modify, but the owner has renounced ownership of it.

A *free OS* doesn't have to be open source. Some of them may be free to download and use but unavailable to modify. The OS remains owned by an individual or company that limits who can modify and distribute it. Google owns and manages Chrome OS, for example, and makes it free to use. Not just anyone

https://t.me/learningnets

can modify it.

Commercial operating systems are privately owned by companies that charge money for them. Examples include Microsoft Windows and Apple macOS. You need to pay for the right (or *license*) to use computers that run commercial operating systems. The end-user license agreement (EULA) must be acknowledged by the OS installer; it provides the licensee the legal right to use the software.



NOTE Public cloud providers generally allow you to reuse existing OS licenses to save money when you run virtual machines in the cloud; this is referred to as *bring your own license (BYOL).*

Software Compatibility

Programmers write applications to work with a specific OS. In other words, applications work only on the OS for which they were written. One reason to choose a certain OS over another is software compatibility. Generally speaking, Microsoft Office doesn't run on a Linux system, for example, and Linux software won't run in Windows. If you are choosing a computer to do a specific task, make sure any programs you *need* are available for your OS. Figure 5-2 shows a Mac failing to run an application not written for it.



Figure 5-2 An OS will report an error if you try to run software not designed for it.

Software compatibility can also be an issue with different versions of the

https://t.me/learningnets

same OS. For example, an application written for Windows 10 might not work under Windows 7. Check each application's advertised system requirements when assessing whether a particular application will work with your computer.



NOTE Many application developers make versions of their programs for multiple operating systems. Microsoft develops similar (but not identical) versions of Microsoft Office, for example, for both macOS and Windows. A retail DVD containing an application might contain application versions for multiple operating systems, but only the one for your OS will install or function.

Complexity

In Chapter 2 you learned that modern central processing unit (CPU) manufacturers produce both 32-bit and 64-bit versions of their processors. The bit support of a CPU refers in large part to the complexity of programming it can handle, including the programming or code that makes up the OS.

Operating systems also come in 32-bit and 64-bit editions. The 64-bit edition of an operating system has advantages over the 32-bit edition, such as the ability to use more random access memory (RAM). (The 32-bit editions of Windows are limited to 4 GB of RAM, for example.) A computer with a 64-bit CPU can run either a 32-bit or a 64-bit OS, but a computer with a 32-bit CPU can run only a 32-bit OS.



NOTE As we'll discuss in Chapter 9, applications also come in 32-bit and 64-bit versions. Most 32-bit applications will work on 64-bit operating systems, but not vice versa. Certain applications that work very closely with the operating system, however, such as anti-malware programs, must match the OS.

Comparing OS Interfaces

Each of the operating systems examined in this chapter has a graphical interface based on a desktop metaphor, where a colored background is the surface on which you open windows and click icons. The following sections show you the interfaces of the four operating systems you'll find in the wild: Windows,

https://t.me/learningnets

macOS, Linux, and Chrome OS.



EXAM TIP Every desktop OS has a command-line interface as well as a graphical user interface. The CompTIA IT Fundamentals exam pretty much ignores the CLI—with a few exceptions noted in this book—focusing instead on the GUI. Save your serious study of the CLI until you decide to go further in computers with CompTIA A+ certification.

The Windows Interface

Microsoft currently supports four versions of the Windows interface for desktop computers, but we can group the similar versions together for the purposes of discussion:

- Windows 7
- Windows 8 and Windows 8.1
- Windows 10

The CompTIA IT Fundamentals exam doesn't distinguish among the versions of Windows or even among the different editions within each version. Instead, you'll see questions that you can answer the same way regardless of version or edition. This section goes into a little more detail because you should be familiar with the most popular desktop OS on the planet.

Windows 7

Figure 5-3 shows the standard interface for Windows 7, a traditional multifunction computer. Windows uses a graphical user interface primarily, so you engage with the mouse or other pointing device and click elements. The background is called the *Desktop*. The open applications are Internet Explorer, Window's default web browser, and a Windows Explorer window showing the Windows 7 default Libraries.

https://t.me/learningnets

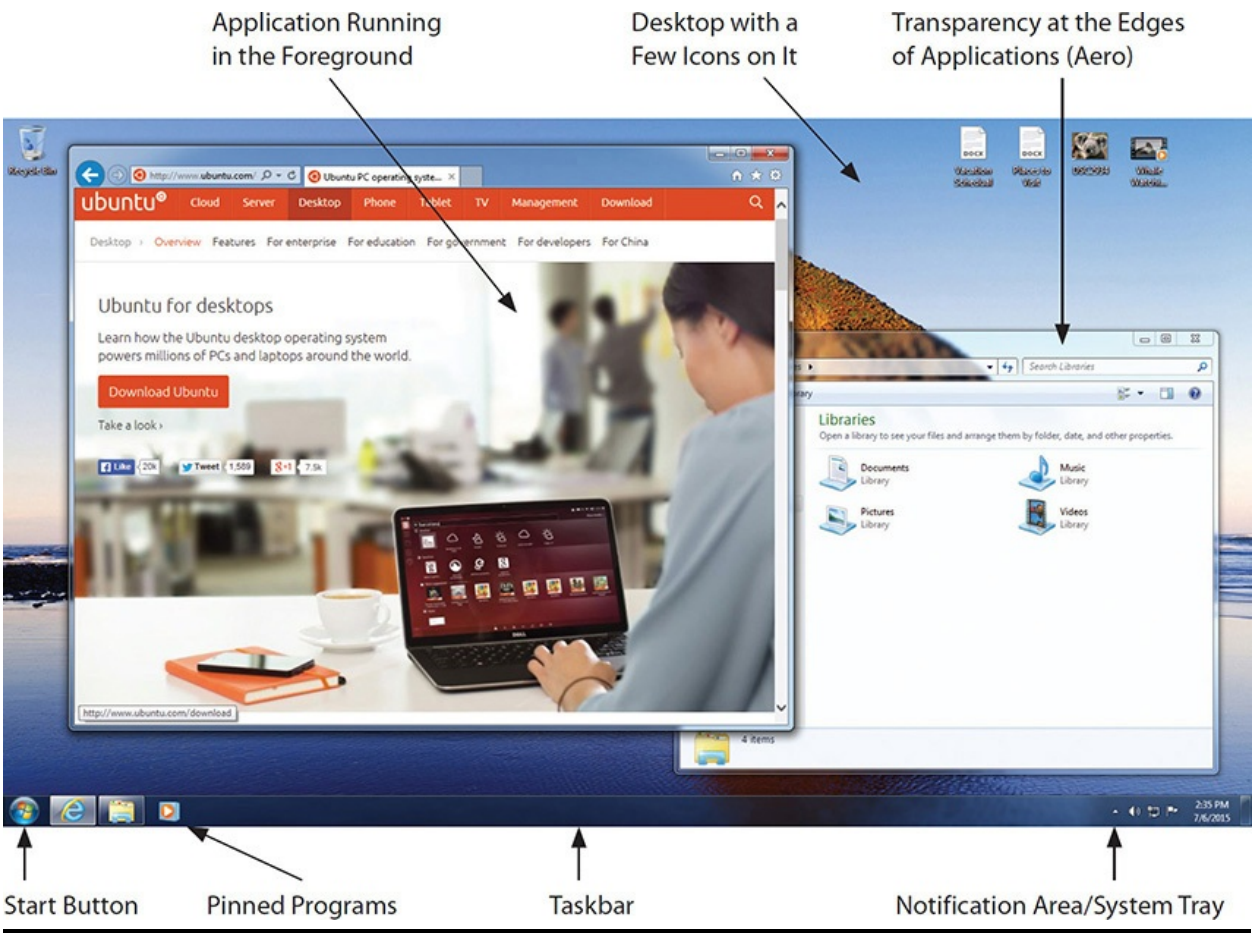


Figure 5-3 Windows 7 with applications open

Other visible items are as follows:

- The open applications demonstrate *transparency* , where the edges of the applications show blurred background images. This feature is called *Aero* or *Aero Glass.*
- Click the *Start button* to get access to applications, tools, files, and folders.
- The *pinned programs* enable you to launch a program with a single left-click.
- The *taskbar* shows running programs.
- The *notification area* shows programs running in the background. Many techs also call it the *system tray*.

Interacting with the classic Windows interface primarily involves using a mouse or touchpad to move the cursor and either left-clicking or right-clicking

https://t.me/learningnets

the icons. Left-clicking selects an item; double-left-clicking opens an item. Right-clicking opens a *context menu* from which you can select various options (see Figure 5-4).

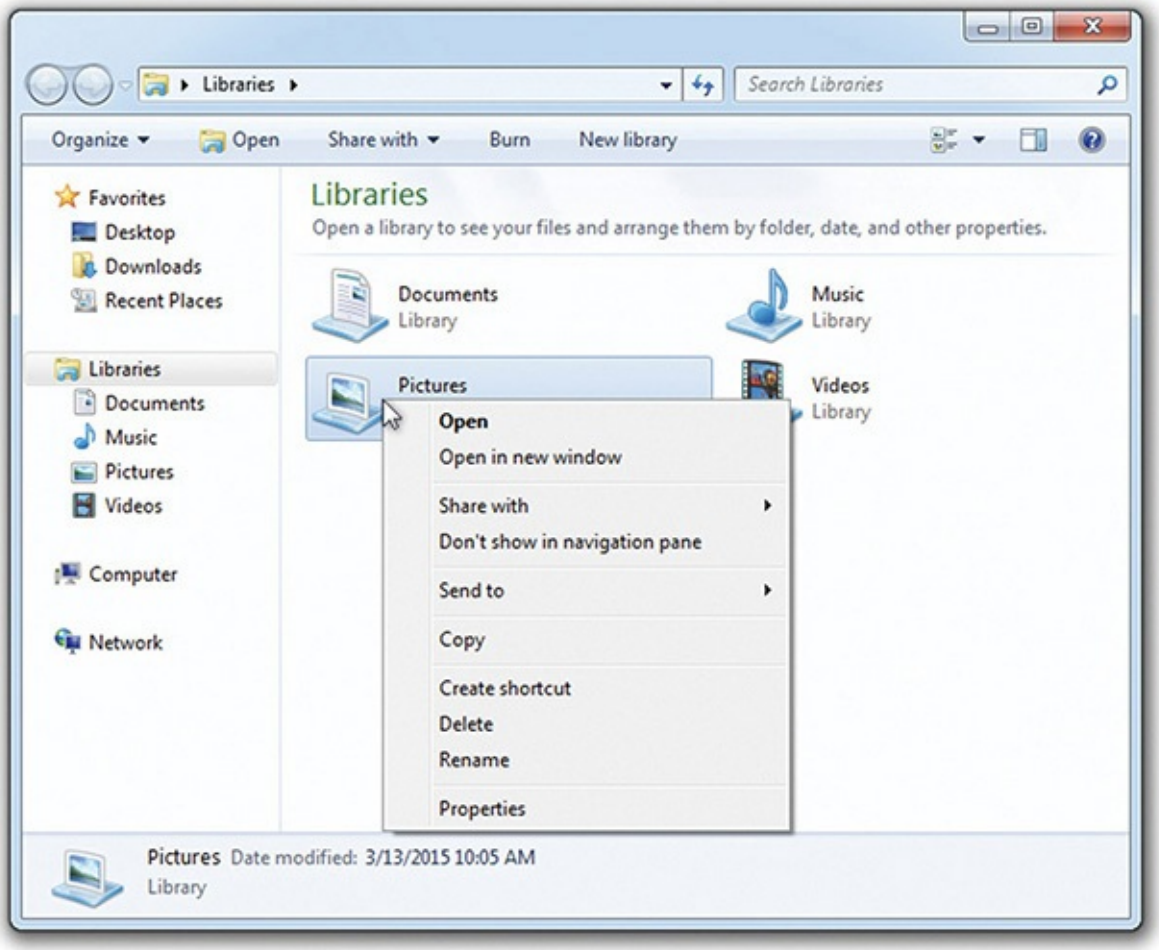


Figure 5-4 Context menu



NOTE The context menu offers options specific to the icon you right-click. Right-clicking a file, for example, gives you a context menu that differs greatly from when you right-click an application.

Windows 8/8.1

Microsoft took a bold chance with Windows 8 (and later 8.1) by making some radical changes. The familiar Desktop is still there, but there is no Start menu.

https://t.me/learningnets

Instead, clicking the Start button opens a Start screen. The *Start screen* covers the entire screen and contains rectangular *tiles* that are shortcuts to *apps*, which are the programs you can run. Note that the screen shows *pinned apps*—the default programs and programs selected by the user—and not all the applications installed on the computer.

The Windows 8 interface, code-named *Metro UI*, works great for touch-enabled devices. The PC becomes in essence a giant tablet. Touch an app to load, drag your finger across the screen to see other apps, and have fun. Figure 5-5 shows the default Windows 8 Start screen.

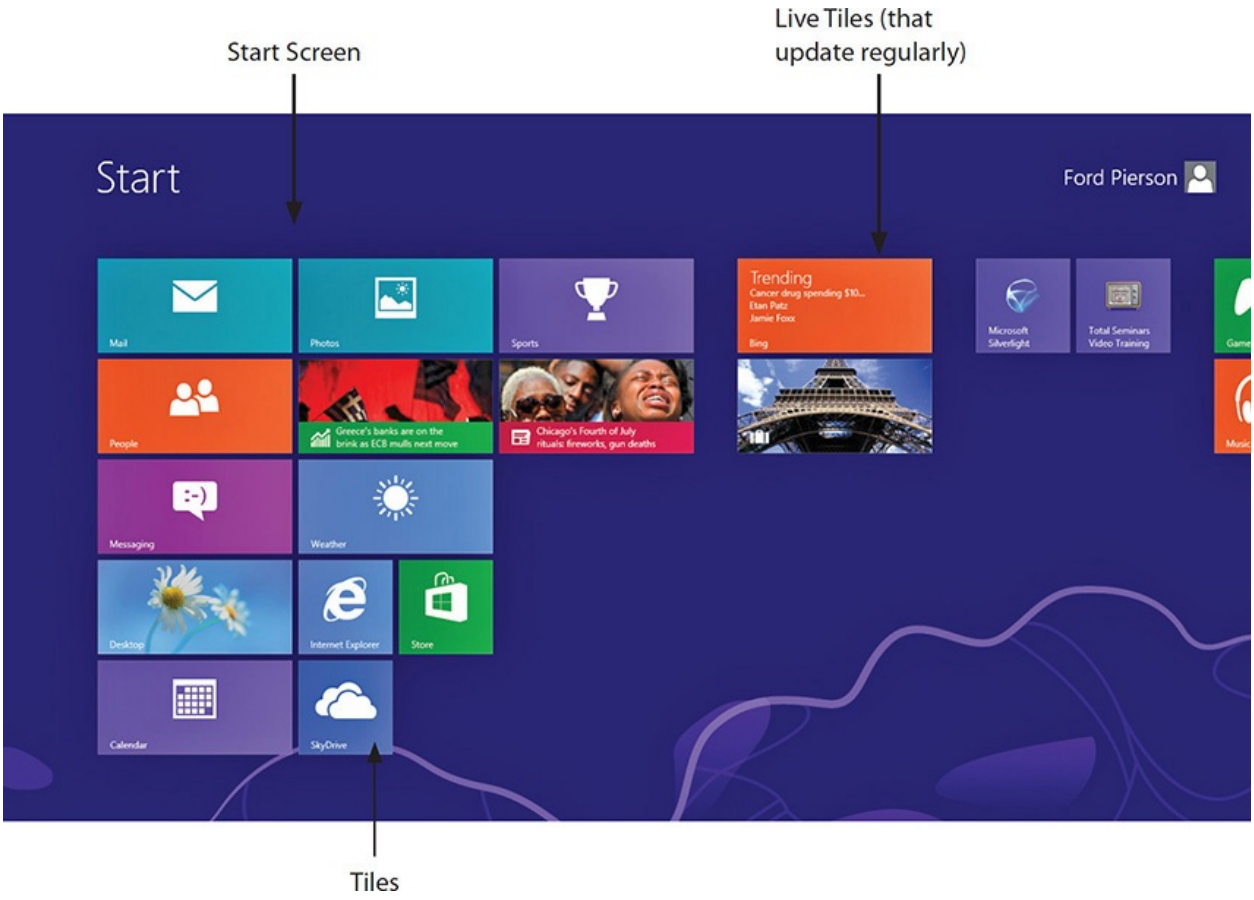


Figure 5-5 The Windows 8 Start screen



NOTE Microsoft dropped the "Metro UI" moniker just before releasing Windows 8 because of legal concerns, replacing it with "Modern UI." A lot of techs and IT industry pros continue to refer to the unique Windows 8/8.1 tiled

https://t.me/learningnets

interface as “Metro.”

Windows 8 also features a more classic Desktop, but it’s one with the noticeable absence of a visible Start button (see Figure 5-6). You access this screen by pressing the WINDOWS LOGO KEY on a standard keyboard.



Figure 5-6 Windows 8 Desktop

Using a keyboard and mouse with Windows 8 bothers a lot of users making the jump from Windows 7. Scrolling with the mouse wheel, for example, scrolls right to left rather than up and down (see Figure 5-7).

https://t.me/learningnets



Figure 5-7 Windows 8 Start screen scrolled to the right

With a series of updates culminating in Windows 8.1, Microsoft brought back features such as the Start button, easy access to a Close button for apps, and the ability to boot directly to the Desktop. Figure 5-8 shows the standard interface for Windows 8.1. Note that it's similar to Windows 7.

https://t.me/learningnets

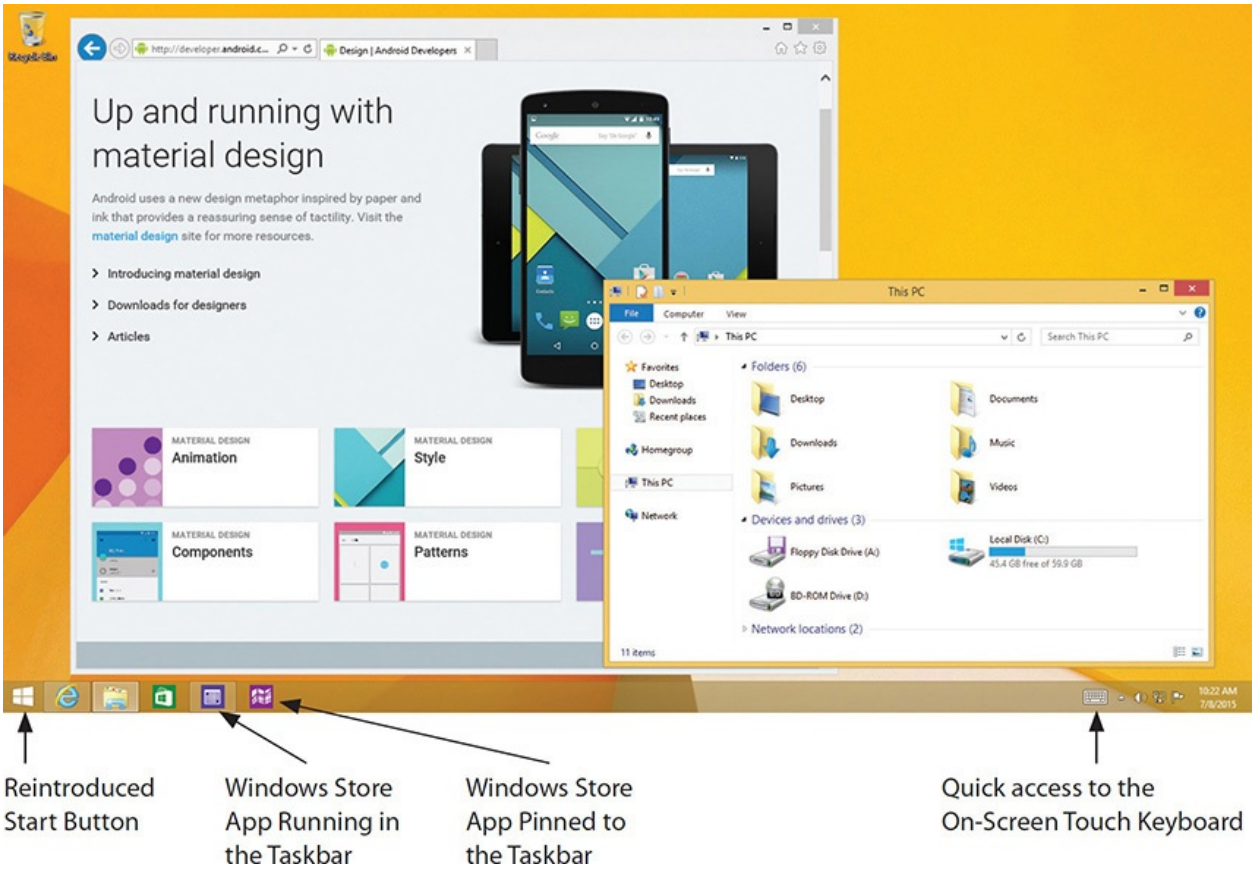


Figure 5-8 Windows 8.1

Windows 8.1 makes it easy to pin apps to the Start screen. Selecting the arrow at the bottom left brings up the Apps pane where you can sort and select apps and utilities (see Figure 5-9). Right-click an icon to pin it to the Start screen.

https://t.me/learningnets

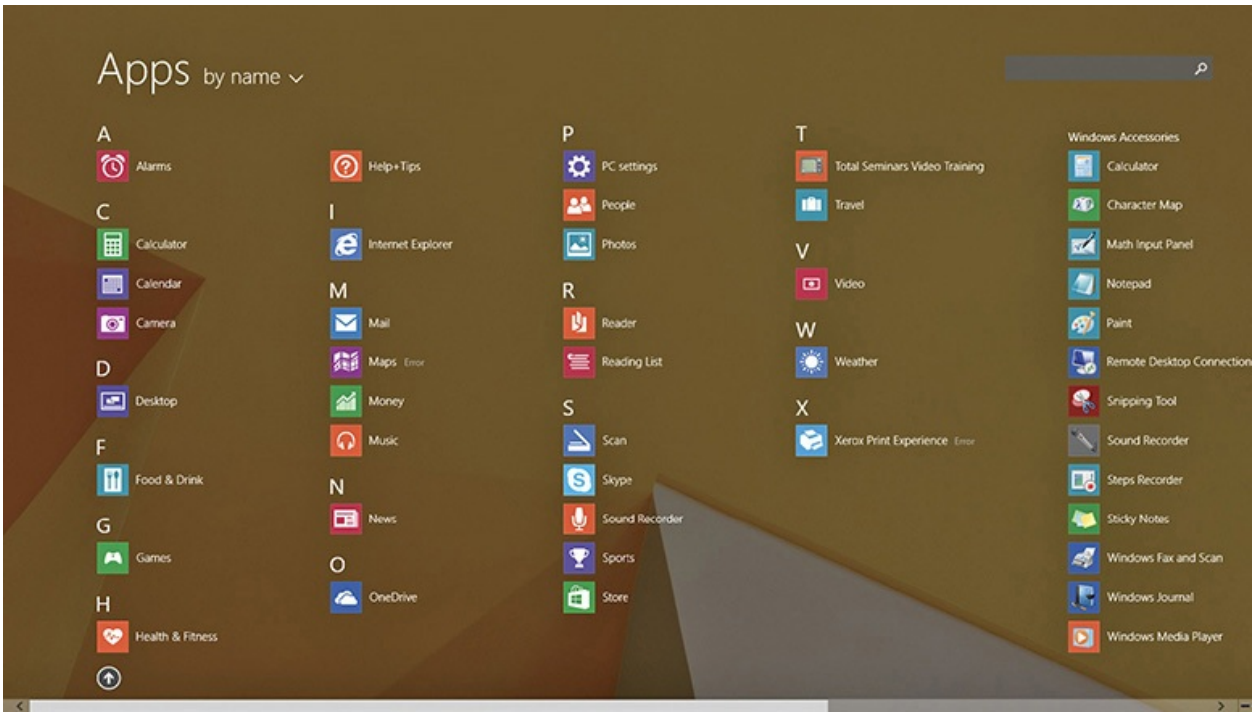


Figure 5-9 Apps sorted by name

Windows 8/8.1 offer lots of hidden interface components that activate when you place the cursor in certain places on the screen. Dropping the cursor to the bottom-left corner, for example, activates the Start button (see Figure 5-10) when in the Start screen.

https://t.me/learningnets



Figure 5-10 Start button magically appears

Placing the cursor in the upper- or lower-right corner of the screen reveals the *Charms bar,* a location for tools called *charms*. See the right side of Figure 5-11. Charms include a robust Search tool that enables a search of the computer or even the Internet in one location. There's a Share charm for sharing photos, e-mail messages, and more.

https://t.me/learningnets



Figure 5-11 Charms accessed by cursor in upper- or lower-right corner

The final version of Windows 8.1 uses the Desktop rather than the Start screen as the default interface. The Start button is visible in the bottom left (see Figure 5-12). You can still access the charms using the cursor and the upper- and lower-right corners of the screen.

https://t.me/learningnets

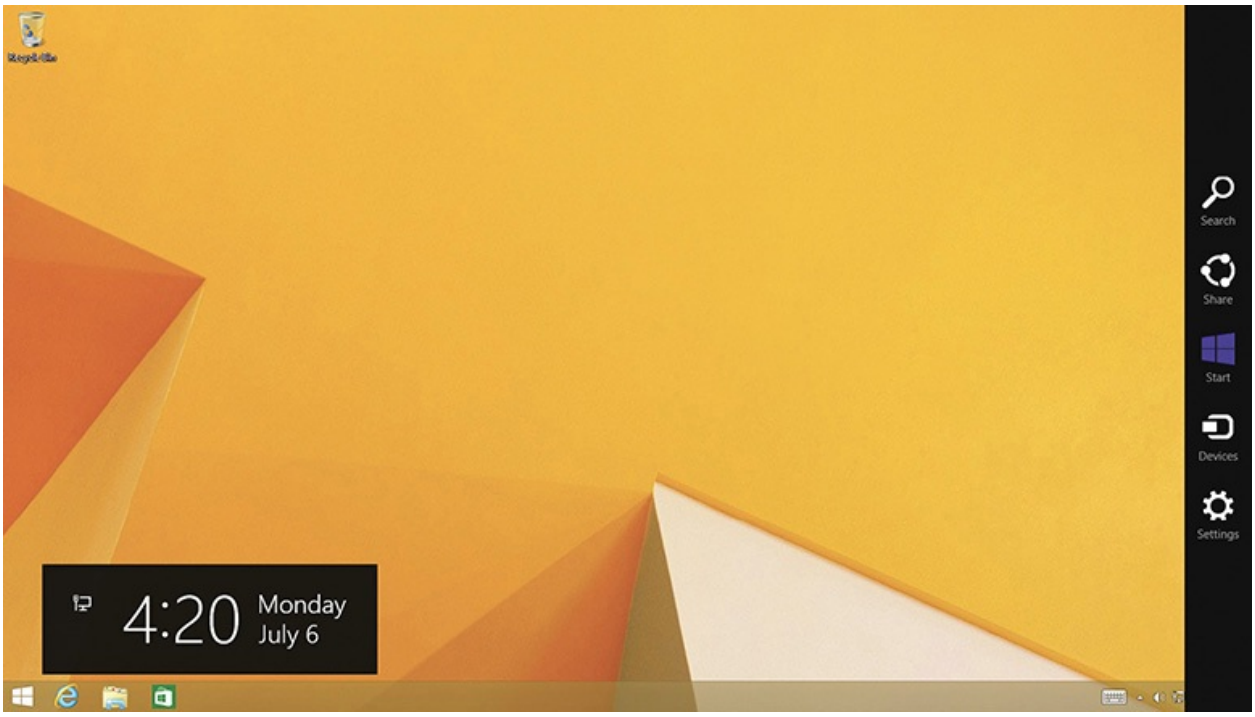


Figure 5-12 Windows 8.1 Desktop

Windows 8.1 also supports a new type of application, called *Modern apps* or *Metro apps*. This type of application resembles the type used on mobile operating systems like iOS and Android. They run full-screen and are optimized for touchscreen use. You download them from the Windows Store, rather than installing them from optical discs or downloads from individual web sites. They install automatically when you choose them from the Store app. Chapter 9 explains how to acquire and install applications. Windows 8.1 also includes a Settings app, which is an alternative to the Control Panel for changing system settings.

Windows 10

Windows 8 and 8.1 were widely criticized for being too different from the familiar Windows environment of Windows 7 and earlier. Consequently, Windows 10 is a compromise between the look and feel of both Windows 7 and Windows 8.1.

Windows 10 has some features of Windows 8/8.1, such as the ability to download and run Modern apps and the Settings app for changing system settings. It has a Start menu (rather than a Start screen), like Windows 7 does, but the Start menu includes customizable tiles like the Windows 8.1 Start screen

https://t.me/learningnets

has. Figure 5-13 shows the Windows 10 interface with an active application in the foreground.

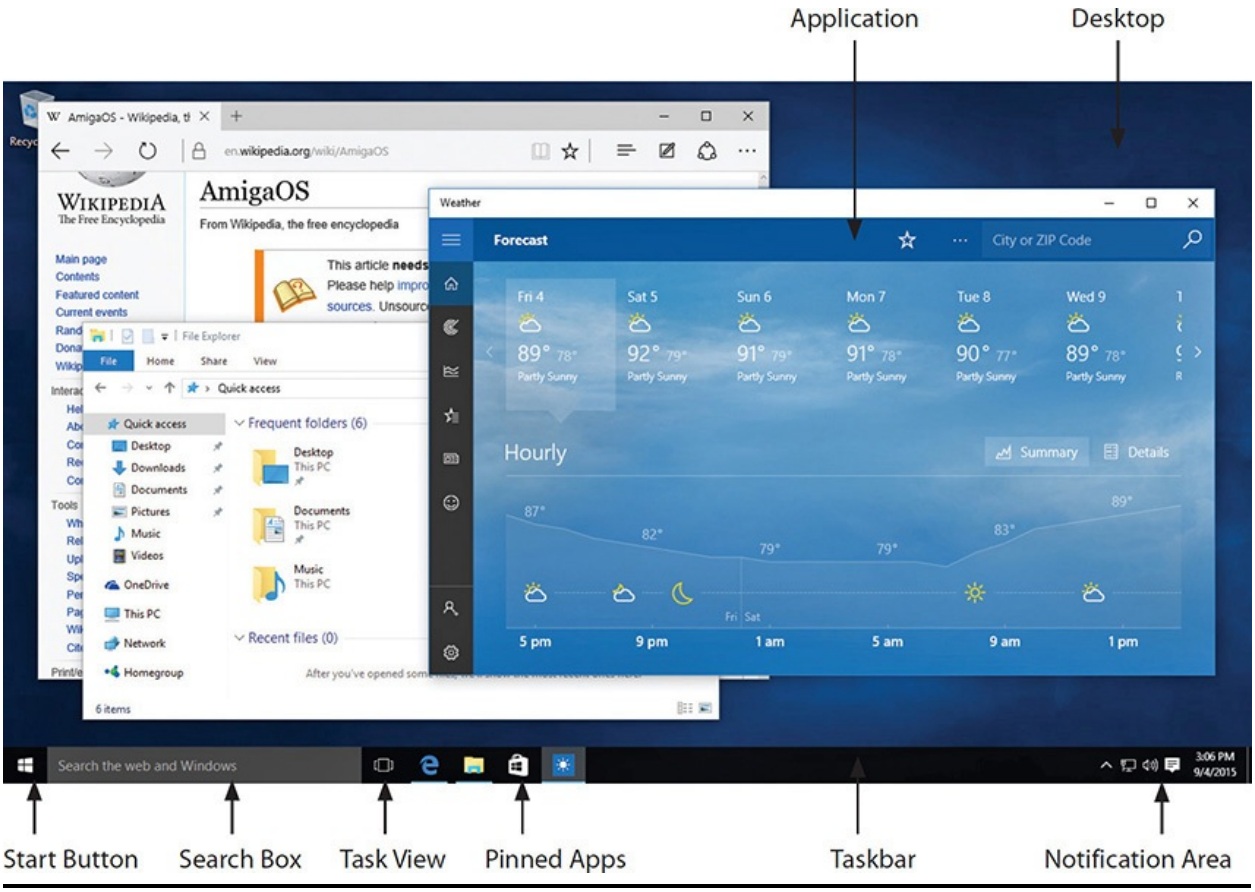


Figure 5-13 Windows 10 with a few applications open

When you press the WINDOWS LOGO KEY on the keyboard, Windows 10 brings up the Start menu with useful tools and your most used apps on the left and pinned apps on the right (see Figure 5-14). Just like with Windows 8.1, you can click the link helpfully named *All apps* (bottom left) to open a list of installed applications. Right-click to pin any app to the Start screen.

https://t.me/learningnets

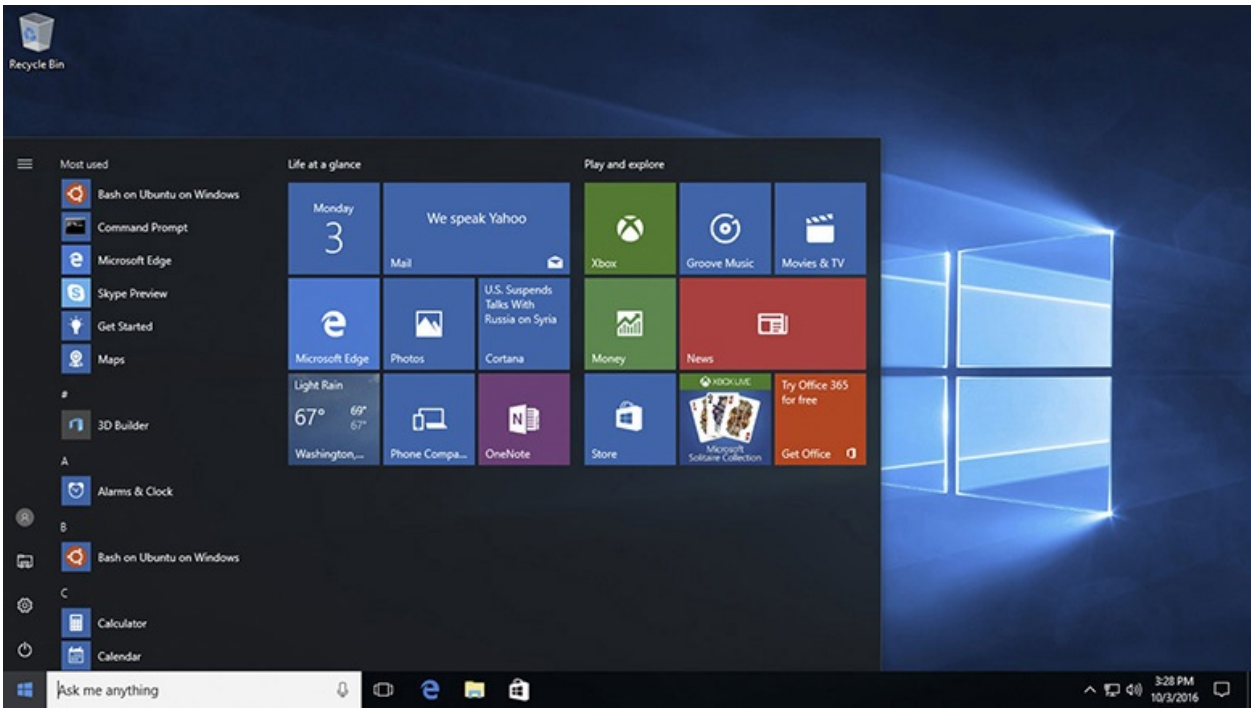


Figure 5-14 Start menu in Windows 10

The macOS Interface

The macOS graphical user interface offers similar functions to those found on Windows. The background of the main screen is called the *Desktop*. macOS has a toolbar (the *Dock*) at the bottom of the screen where you can pin and access frequently used shortcuts as with the taskbar, Start screen, or Start menu in Windows. Running applications appear in the Dock with a small black dot under them.

If the application you want to run doesn't appear on the Dock, you can click the Launchpad to see a complete list of available applications. The active application's menus appear in the upper-left corner of the screen. Regardless of the active application, the Apple menu (open in Figure 5-15) is always available for you to access System preferences, shut down, log out, and so on.

https://t.me/learningnets

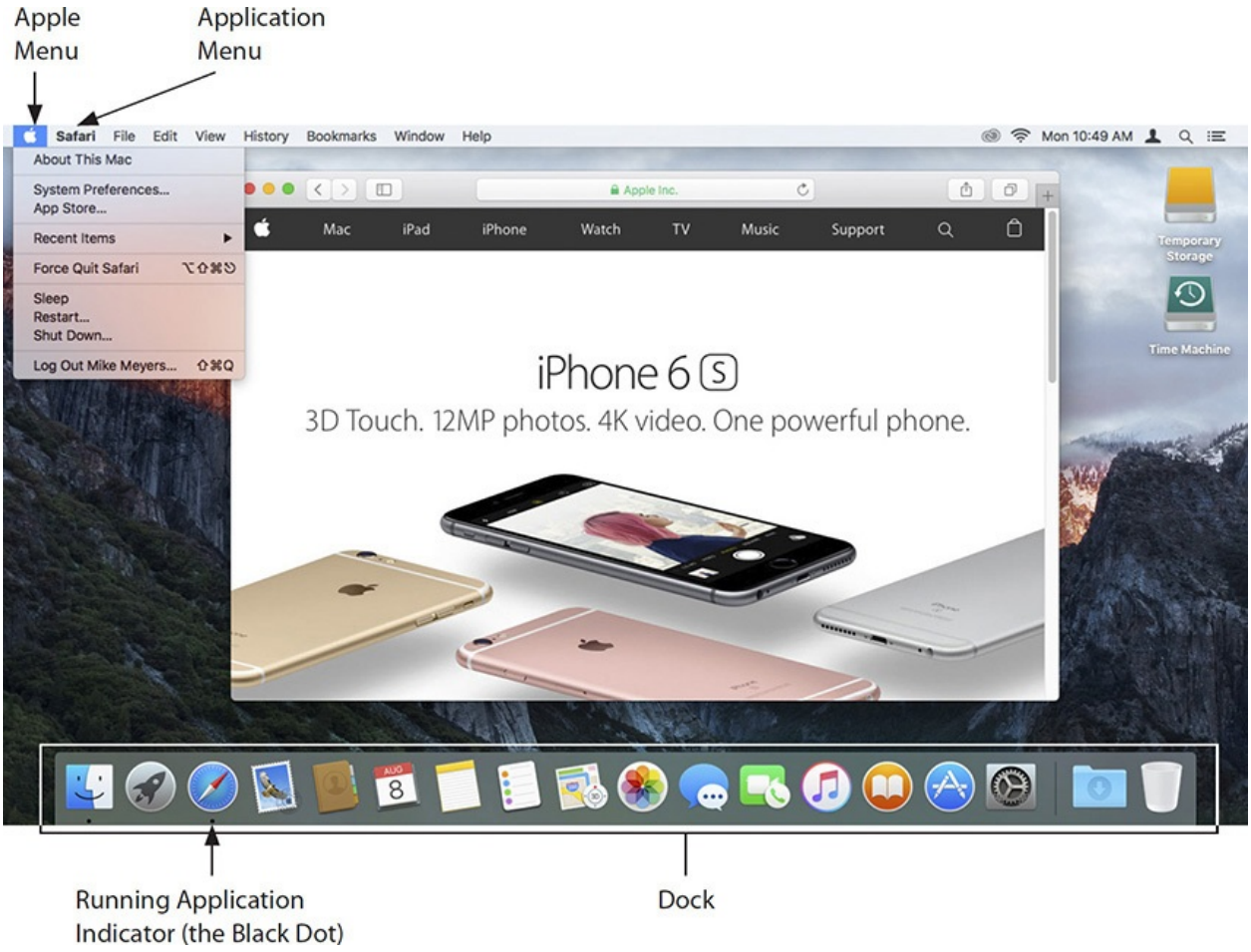


Figure 5-15 macOS Desktop with Apple's Safari web browser running and the Apple menu open

The Linux Interface

At its heart, Linux is a command-line operating system. However, many distributions (*distros*) come with a *desktop environment* (DE) that provides a GUI for Linux users. One of the most popular distros for casual users, Ubuntu, comes with a DE called Unity (shown in Figure 5-16). Several other popular distros also come with this same GUI interface.

https://t.me/learningnets

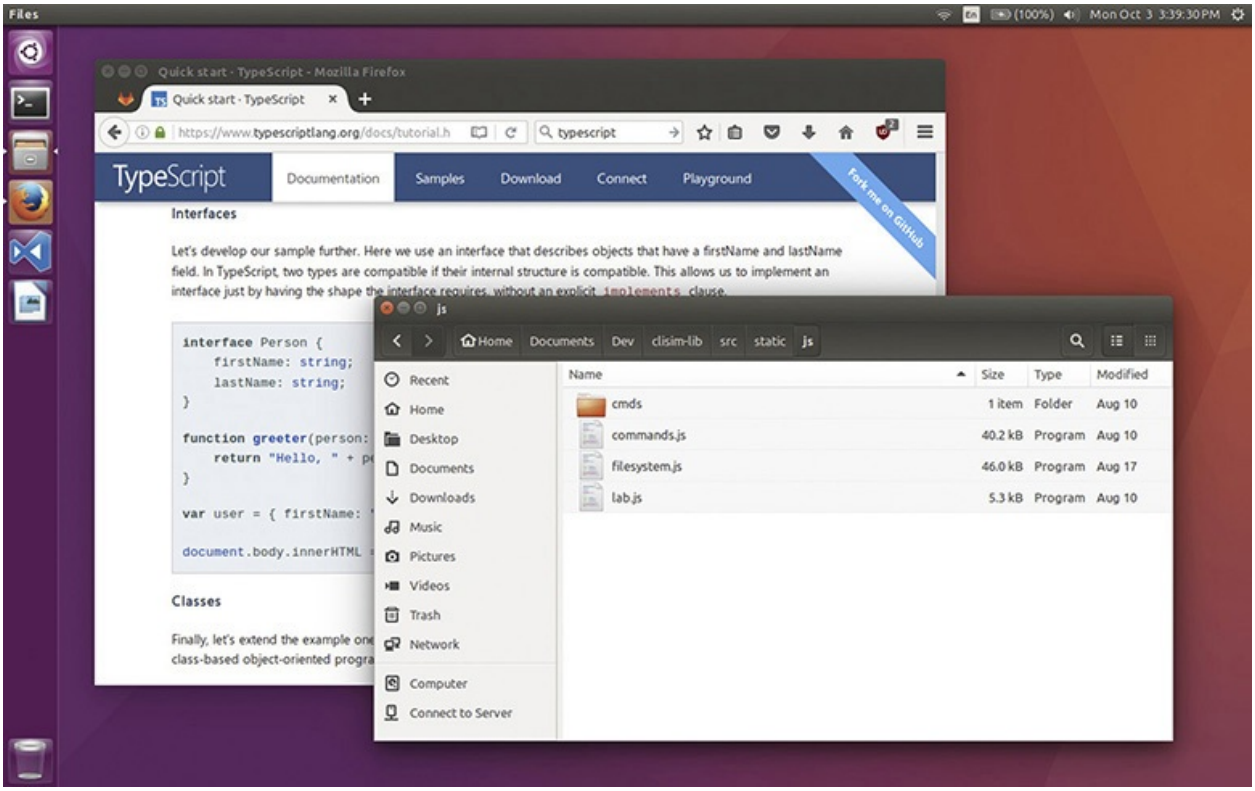


Figure 5-16 The Unity interface, provided with Ubuntu Linux

The *Launcher* is the bar along the left side of the screen. It is similar both to the Dock in macOS and to the taskbar in Windows. When an item is open, as the Files utility is in Figure 5-16, the background to its icon on the Launcher appears dark red, rather than the usual gray.

The topmost Launcher button is the *Dash button*, which is roughly equivalent to the Windows Start button. It opens a Dash panel that includes a Search box and shortcuts (see Figure 5-17). Filter icons called *lenses* appear across the bottom of the pane and let you browse by type of item. For example, in Figure 5-17 we're browsing applications. Notice that the Installed section has icons for installed applications; the More suggestions section suggests applications you may want to download.

https://t.me/learningnets

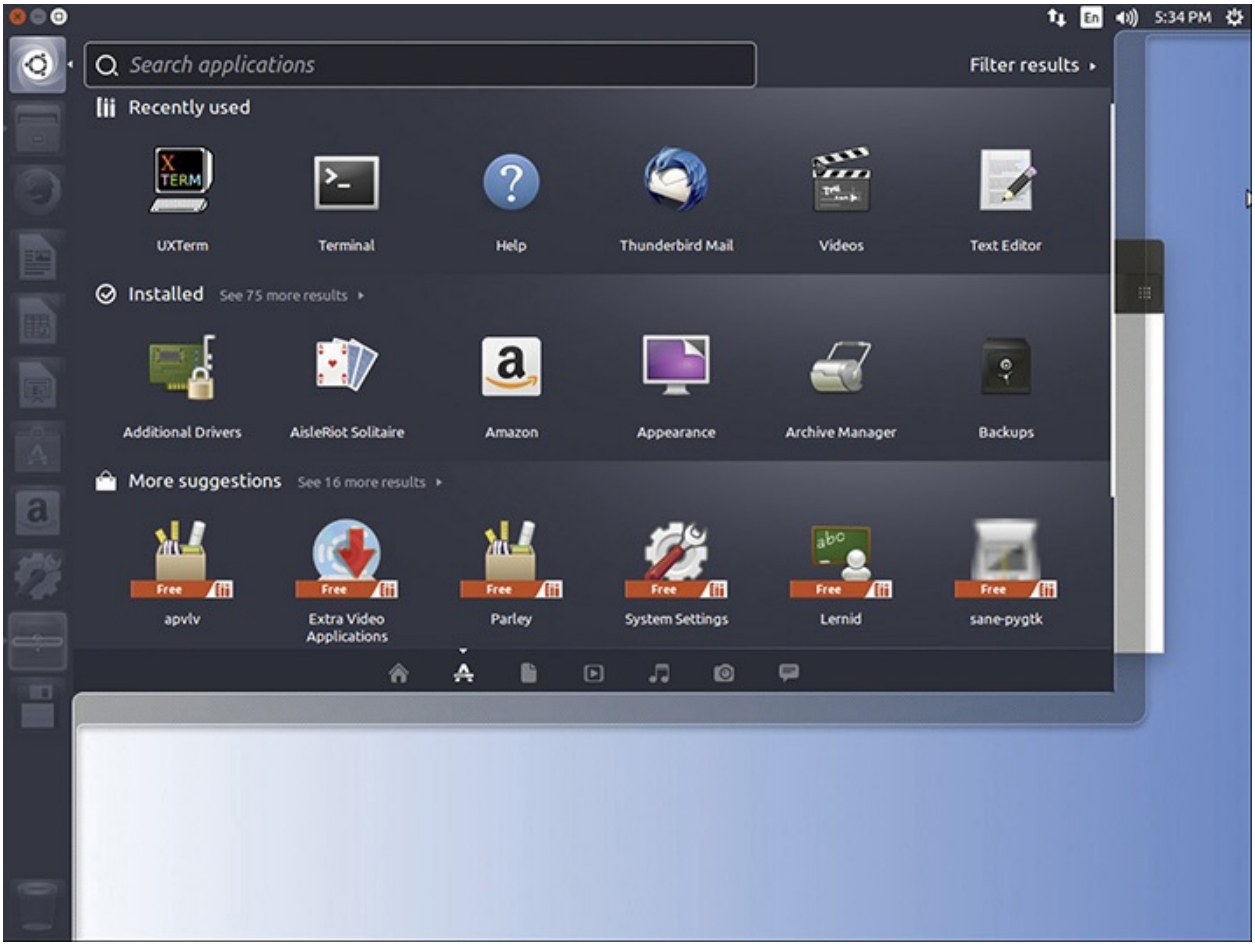


Figure 5-17 The Dash pane

The Chrome OS Interface

On the surface, computers running Google Chrome OS appear to function similarly to computers running other desktop operating systems. Chrome OS features a desktop background. Along the bottom of the screen you'll find the *shelf* with access to frequently used applications, such as the Chrome web browser and Gmail for e-mail. Figure 5-18 shows the default interface for Chrome OS with a browser window open and features labeled.

https://t.me/learningnets

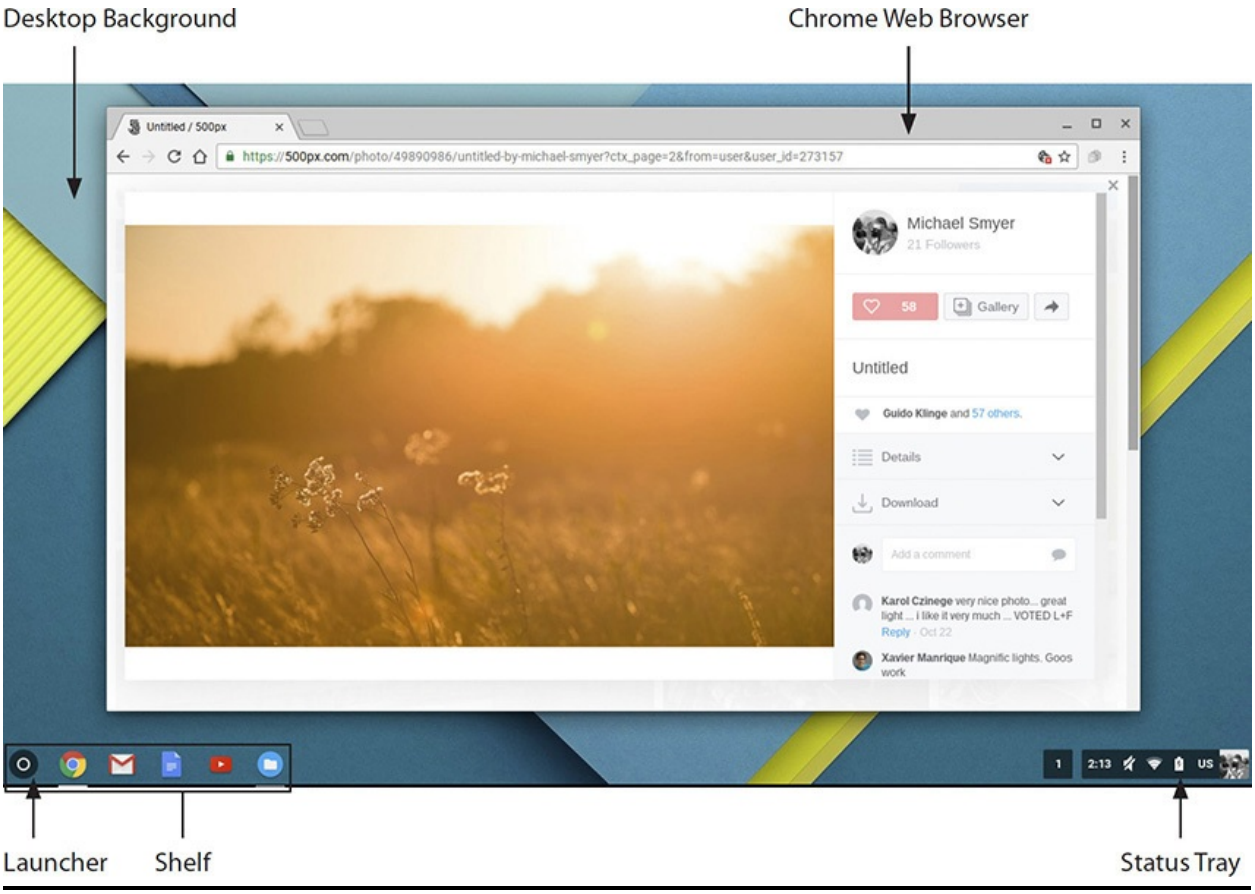


Figure 5-18 Chrome OS

The *Launcher* that you can see in the lower left of the desktop enables you to access all the programs available to the computer. Figure 5-19 shows apps in Launcher. Almost all of the apps are web-based apps tied to your Google account. In fact, the only way to add an app is through the Google web store.

https://t.me/learningnets

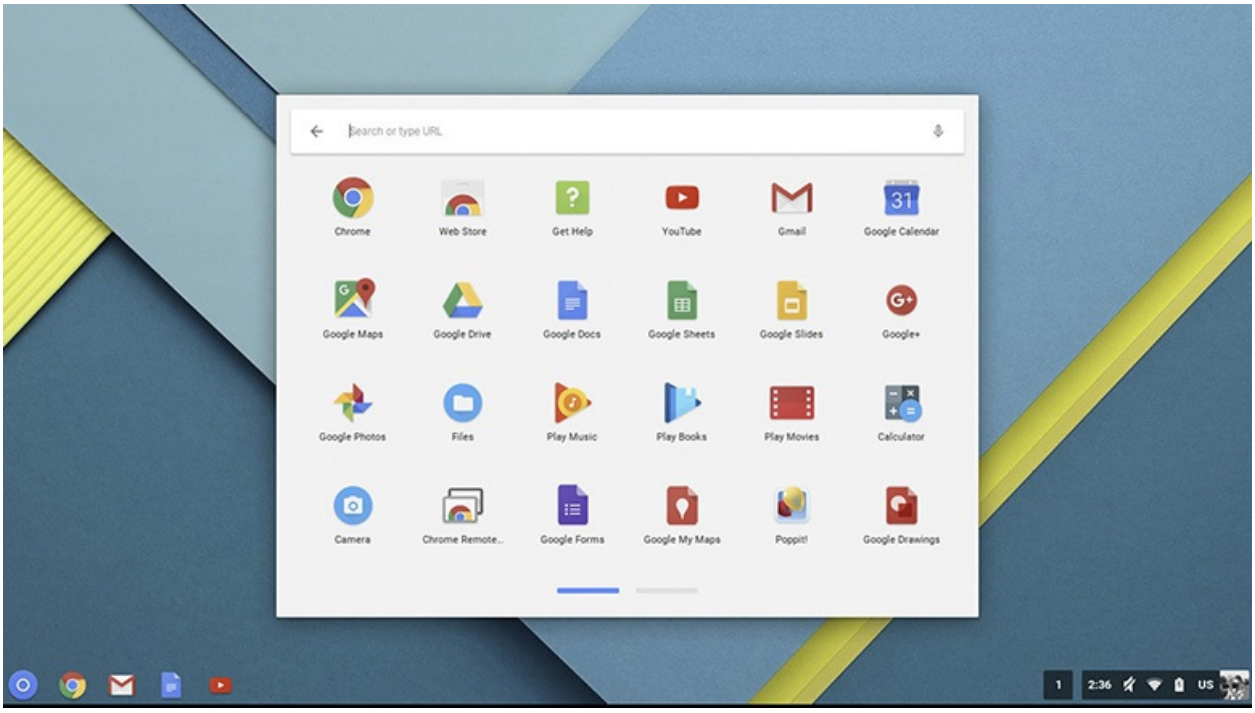


Figure 5-19 Launcher apps

The *status tray* (lower right) shows the status of essential computer elements, such as remaining battery life, wireless network connections (including Bluetooth), and current audio volume; it also gives you access to Settings where you can adjust various system features. Figure 5-20 shows the status tray expanded.

https://t.me/learningnets

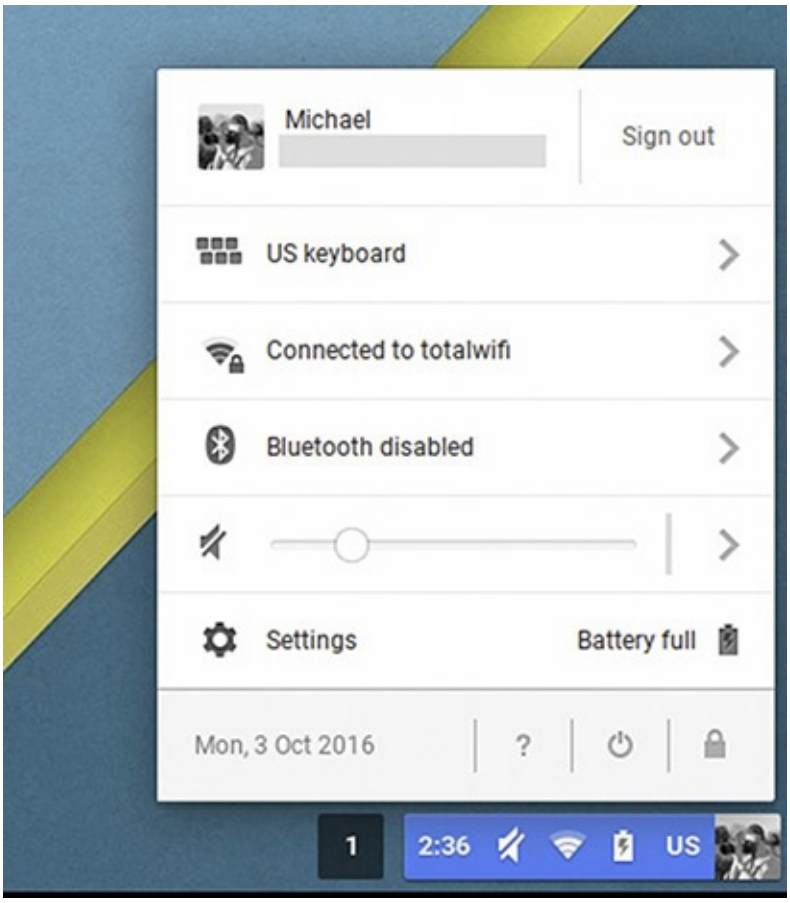


Figure 5-20 Status tray expanded

Although Chrome OS resembles the other desktop operating systems, it differs substantially under the hood. Google designed Chrome OS with the assumption that users would always be connected to the Internet. This means that Chrome OS relies heavily on Internet-based applications and features. Chrome OS computers usually have a small amount of local storage, for example, relying instead on the online Google Drive associated with the user's account for storing files and folders. You can access Google Drive directly or use the Files app (Figure 5-21).

https://t.me/learningnets

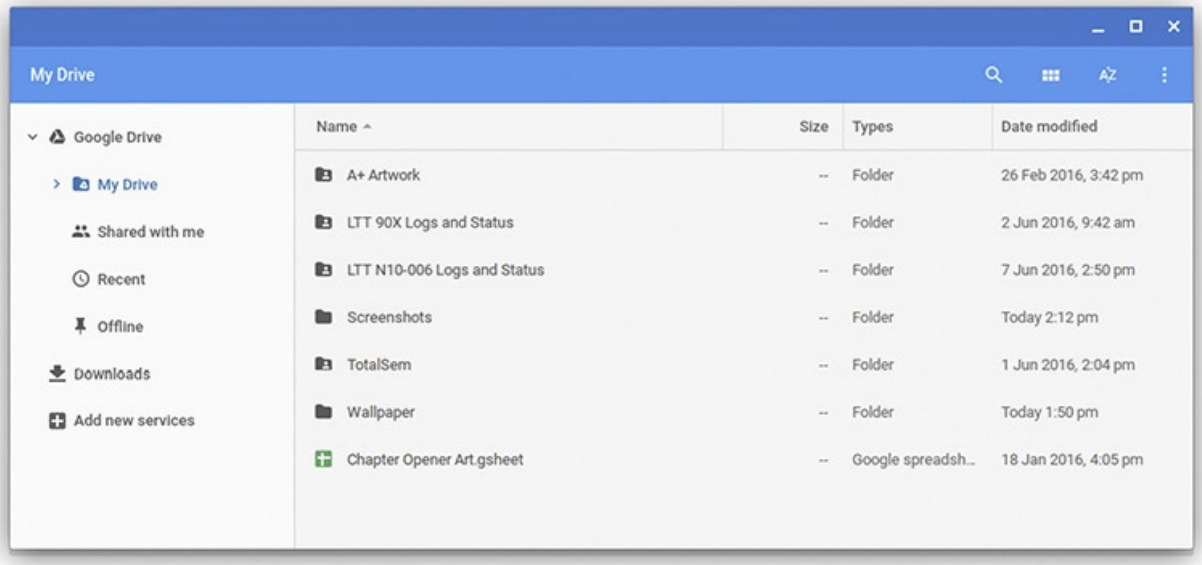


Figure 5-21 Access to the Google Drive contents with the Files app



NOTE Chrome OS gets a bad rep in some circles because of its always-connected nature. The assumption often made is that you can't do any work on a Chrome OS computer when you're not connected to the Internet. That's not true. You can do a lot of things offline; when you go online, Chrome OS will sync your files and folders in Google Drive.

Cross-Referencing Features

Windows, macOS, Linux, and Chrome OS have many of the same tools and features, but they go by different names. Table 5-1 provides a key to finding what you want in one OS if you know what it's called in another.

Feature	Windows	macOS	Linux	Chrome OS
Manage Files	File Explorer	Finder	Files	Files or Google Drive
Browse Programs to Run	Start menu/screen	Launchpad	Dash	Launcher
Change System Settings	Control Panel or Settings	System Preferences	System Settings	Settings

Table 5-1 Feature Equivalents in Windows, macOS, Linux, and Chrome OS

https://t.me/learningnets

The next section looks at some of the common features in these operating systems in more detail. It focuses more heavily on Windows because Windows is by far the most popular, but other operating systems are also mentioned where they differ significantly.

Common Features of Operating Systems

Operating systems, both under the hood and in their user interfaces, have many of the same capabilities. That's expected, because users have the same basic needs (such as running programs, managing files, and connecting to the Internet) no matter which OS they use. Every OS also gives users the capability to navigate with hotkeys, create screen captures, and configure accessibility options.



EXAM TIP Most of the topics in Objective 3.2 pertain to file management, which is covered in Chapter 8.

Executing Programs

All operating systems execute programs (that is, run applications, or apps). That's the point of a computer: to run programs that do something useful. Programs can be executed manually or on a scheduled basis. The Windows task scheduler can be used to schedule programs; in Linux, a CRON job runs scheduled tasks. We cover applications in more detail in Chapter 9. In a GUI OS environment, you run a program in one of these ways:

- Double-click an icon or button for the program (or single-click in some cases).
- Open a menu and select the program from the menu, such as the Windows Start menu shown in Figure 5-22.

https://t.me/learningnets

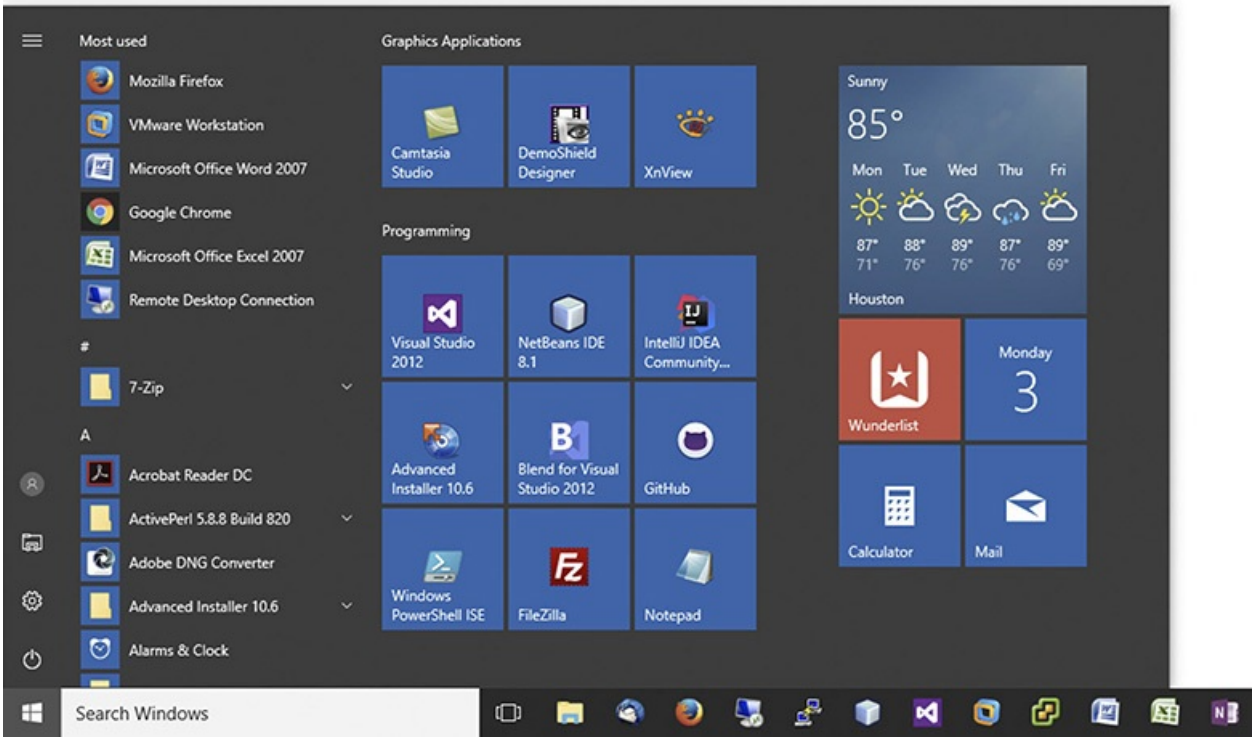


Figure 5-22 In Windows, the most common way to execute a program is from the Start menu.

- Open a file management interface and double-click a data file that is associated with a certain application.
- Press a key combination (a keyboard shortcut) assigned to that program.
- In a touchscreen environment, tap an icon for the program.

Many of the program buttons or icons you see in a GUI environment are not the actual program files but shortcuts to them. A *shortcut* is a pointer that refers to a file. The actual file that runs the program Notepad in Windows, for example, is stored in C:\Windows\System32, but you can access it from a Notepad shortcut on the Start menu/Start screen. Some shortcut icons have an arrow in their lower-left corner to differentiate them from the actual file (Figure 5-23) and have the word *shortcut* in the name, but that's not always the case. Shortcuts are useful because you can have a shortcut in a convenient location while the original file remains protected. You can also have multiple shortcuts that all point to the same program, giving you multiple ways to start the program.

https://t.me/learningnets



Figure 5-23 A shortcut icon may have an arrow on it.

In a command-line environment, you run a program by typing the program's name, a space, and any options needed, and then pressing ENTER.

In a secure computing environment such as those related to law enforcement and military, special OS protection measures might be required. An OS that supports mandatory access control (MAC) uses data labels for resources such as files or network services combined with policies; this determines whether a subject has access to the resource.

Services

Programs that run in the OS background are called *services* in Windows and either *services* or *daemons* in the Linux world. By background we mean the program is not directly started by the user; instead, it is started by the OS. An example of this would be a server hosting a web site. The web server *service* or *daemon* would normally start when the server starts up, thus making the web site accessible.

Optimizing OS performance and security includes removing unnecessary services. This speeds up the machine because fewer programs are running simultaneously, and it reduces the attack surface; less stuff running means fewer possible security holes.

Managing Files

Computing devices that save data files need some type of file management capability. In Windows, this feature is called File Explorer in Windows 8 and

https://t.me/learningnets

later, or Windows Explorer in earlier versions. In macOS, this feature is called Finder; in Linux it's called Files. With Chrome OS, you can access Google Drive directly or use the Files app for file management. Figure 5-24 compares these, and Chapter 8 explains how to manage files in each OS.

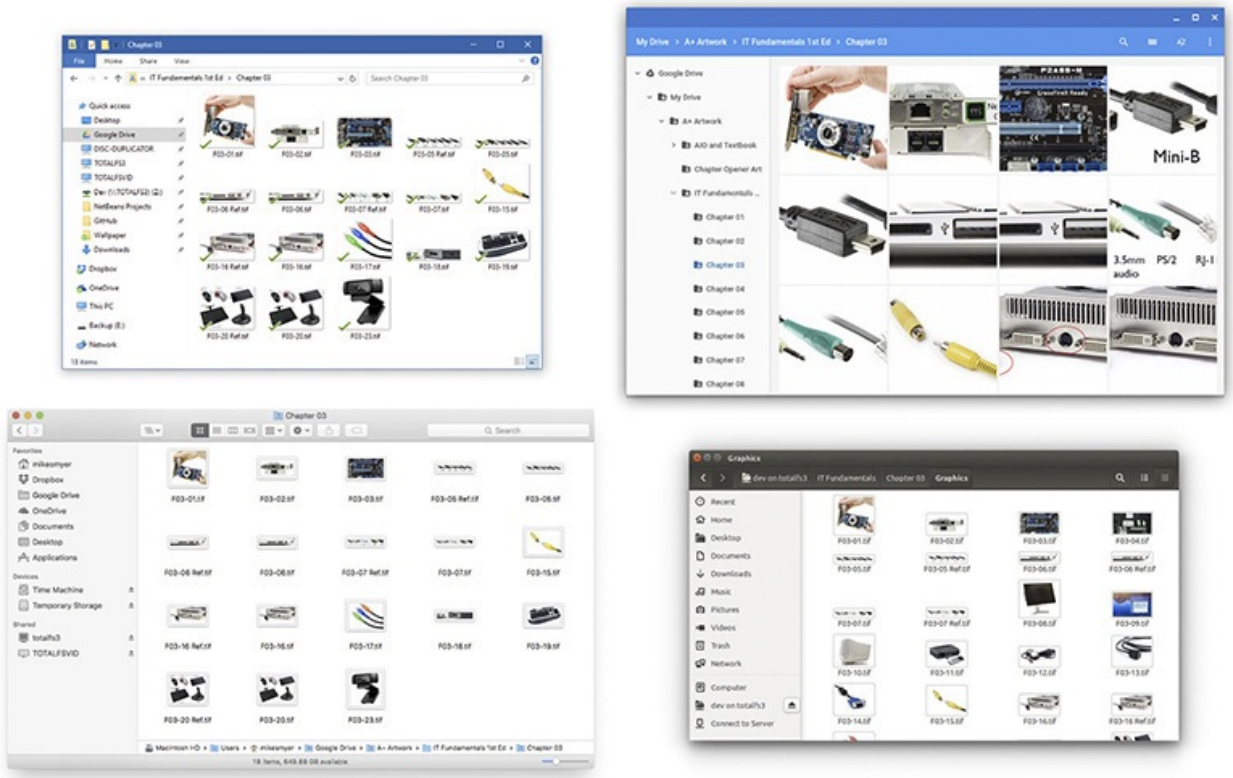


Figure 5-24 File management utilities are similar across operating systems.



NOTE On a simple computing device like a digital music player, you might have to connect the device to a PC to manage files.

Connecting to Hardware

As you learned at the beginning of this chapter, an important OS function is communicating with hardware. Each hardware device has its own language, however, so the OS needs device drivers to translate between them.

Most modern hardware and operating systems support *Plug and Play*, which enables hardware to report its specifications to the OS and enables the OS to

https://t.me/learningnets

assign resources to the device and install a driver for it if one is available. Operating systems come with a collection of device drivers for common devices. That's why when you connect some new hardware to a computer, it seems to work like magic. A message might appear in Windows in the notification area, at the bottom-right corner of the screen, letting you know the device has automatically been set up, as in Figure 5-25.

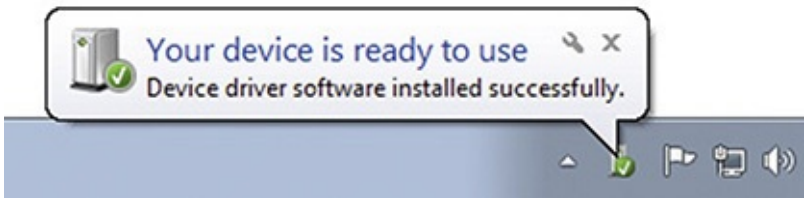


Figure 5-25 Windows has automatically connected to new hardware, and it is ready to use.

If the OS cannot locate a usable device driver for the device, it prompts you to download one or to insert a disc containing the driver. Most devices come with an optical disc containing the needed drivers.



NOTE Chrome OS doesn't do well with many new devices, because you can't install third-party drivers. If the drivers are built into the OS, you're golden; otherwise, features won't work.

Connecting to the Internet

All the major operating systems for computers support Internet connections. Operating systems for desktop and laptop computers generally support multiple ways of connecting, such as with an Ethernet cable, with a wireless Wi-Fi adapter, or using a dial-up modem (an older, slower method). We'll talk more about this in Chapter 10.

Navigating with Hotkeys

Hotkeys, also called *keyboard shortcuts* or *shortcut keys*, enable you to issue commands to the operating system by pressing key combinations on the keyboard. The operating system itself has a predefined set of keyboard shortcuts,

https://t.me/learningnets

and each application also has its own keyboard shortcuts. When you are working in a specific application, its keyboard shortcuts take precedence; when no application is active, the OS keyboard shortcuts are in effect.



EXAM TIP Many Chrome OS apps manifest as tabs in the Chrome web browser, not as separate program interfaces. Getting in and out of them means opening and closing a browser tab. The hotkeys work the same way.

To find out the shortcut keys for an OS, look in the Help system in the OS, or look for a list online. Table 5-2 lists some of the most common ones for Windows, macOS, Ubuntu Linux's Unity interface, and Chrome OS.

Action	Windows	macOS	Linux (Unity)	Chrome OS
Shut down the active app	ALT-F4 from active window	COMMAND-W	CTRL-Q	CTRL-W
Cut the selected item	CTRL-X	COMMAND-X	CTRL-X	CTRL-X
Copy the selected item	CTRL-C	COMMAND-C	CTRL-C	CTRL-C
Paste the selected item	CTRL-V	COMMAND-V	CTRL-V	CTRL-V
Switch between open applications	ALT-TAB	COMMAND-TAB or SHIFT-COMMAND-TILDE (~)	ALT-TAB	SWITCHER
Open Help	F1	COMMAND-?	n/a	CTRL-?

Table 5-2 Some Keyboard Shortcuts (Hotkeys)



NOTE F1 and F4 are in the row of the F1–F12 *function keys* across the top of the keyboard. The OS assigns certain commands to them as shortcuts; consult the Help files for a specific OS to find out what each does. Some applications assign their own shortcuts, both alone and in combination with other keys such as SHIFT, CTRL, and ALT. To add another confusing wrinkle, most laptops and some desktop keyboards have an additional kind of function (FN) key. It's often printed in a distinct color. You can issue extra commands on some keys (indicated by icons of the same color) by holding the FN key when you press them.

https://t.me/learningnets

Creating Screen Captures

A *screen capture* (or *screenshot*) is a digital image of the computer screen. Many of the figures you see in this book are screen captures, and knowing how to create them enables you to teach others how to use an OS or program to accomplish some task. Screenshots also play an important role in showing support staff a problem you're having so they can help you.

Most operating systems include a built-in screen capture feature, involving pressing a certain key or combination of keys. You can also buy third-party applications that capture screenshots with more options. Screen captures are saved with default names (different in each OS) in default locations (which also vary with the OS). Table 5-3 lists the most common procedures.

OS	Keyboard Shortcut	Default Save Location
Windows	WINDOWS-PRINT SCREEN	Pictures\Screenshots
macOS	COMMAND-SHIFT-3 (full-screen) COMMAND-SHIFT-4 (select an area)	Desktop
Linux (Unity)	PRINT SCREEN	Desktop
Chrome OS	CTRL-SWITCHER	Downloads

Table 5-3 Screen Capture Keyboard Shortcuts

Configuring Accessibility Options

Most operating systems include optional configuration settings that make the OS easier for people with certain types of disabilities to use. These are collectively referred to as *accessibility options*. Accessibility options fall into these categories:

- **Movement** Features that help people who have limited mobility or dexterity. A user who can use a keyboard but not a mouse, for example, may engage a feature that enables him or her to move the mouse pointer with the keyboard arrow keys. Someone who can use a mouse but not a keyboard, as a further example, might use an on-screen keyboard utility that enables him or her to type by clicking a mouse button. In addition, keyboard and mouse settings can be enabled that will help people with specific movement limitations. You can slow down the reaction rate and

https://t.me/learningnets

repeat rate of keys, for example, and you can enable a click-lock that locks the mouse button down for dragging.

- **Visual** Features that help people who have limited vision. High-contrast color schemes can help with visibility, as can extra-large mouse pointers and low-resolution display modes. Magnifier utilities can magnify an area of the screen by moving the mouse pointer over it. Screen-reading programs read the contents of windows and dialog boxes aloud.
- **Audio** Features that help people who have limited hearing. For example, the OS can be configured to flash or blink when a sound is played.
- **Voice** Programs that can recognize voice commands and data input. This can be useful both to people with movement difficulties and to people with limited vision.

In Windows, you can set up multiple accessibility options in one place by opening the Control Panel and choosing Ease of Access | Ease of Access Center (see Figure 5-26). In macOS, open the Apple menu in the upper-left corner, and choose System Preferences | Accessibility. Linux (in Unity, at least) has accessibility options under Settings called Universal Access. Finally, you'll find an Accessibilities section in the Settings in Chrome OS.

https://t.me/learningnets

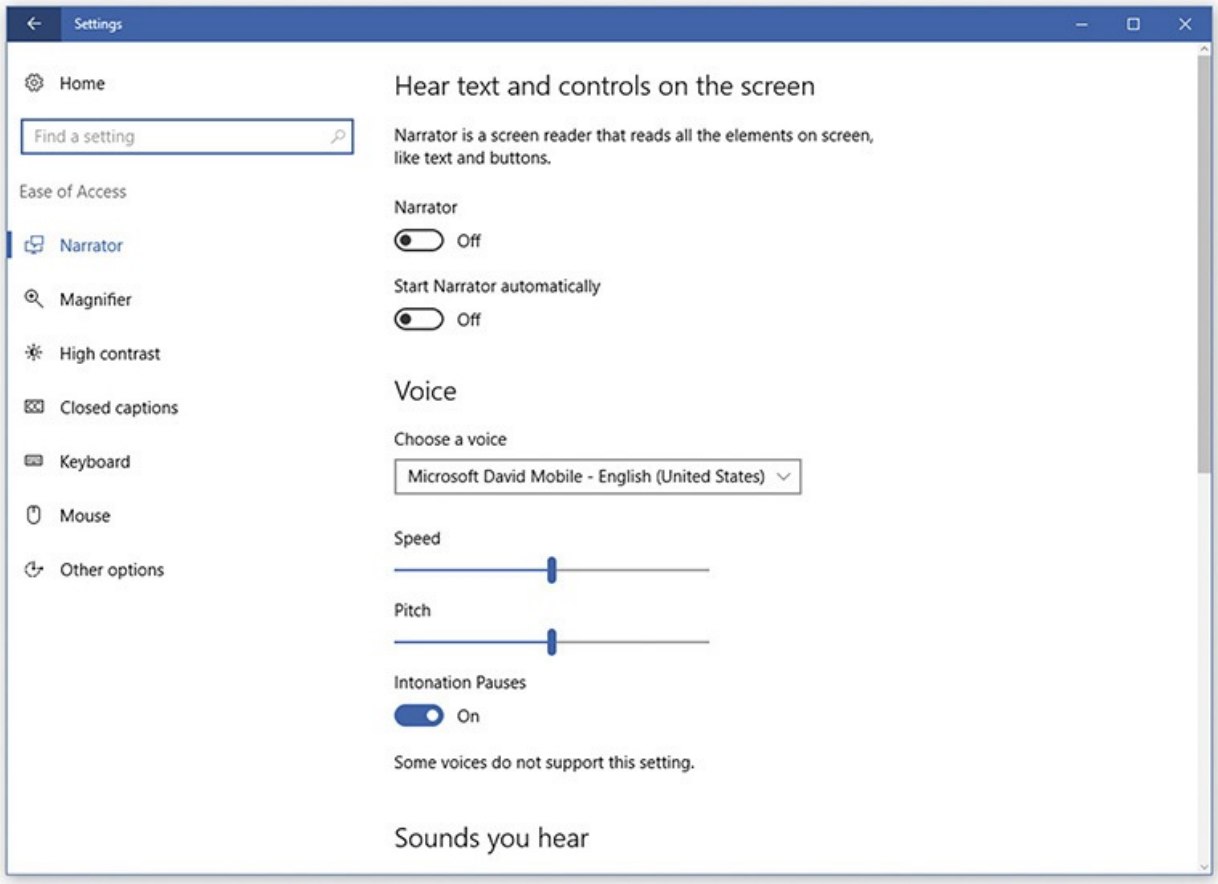


Figure 5-26 The Ease of Access Center helps you set up accessibility options in Windows.

Chapter Review

In this chapter, you learned the five functions of an operating system: providing a machine/human interface, coordinating hardware activities, providing a software environment, monitoring system health, and providing for data management.

You learned about operating system characteristics and how OSs differ from desktop to mobile to server operating systems. Companies release operating systems under one of three licensing options: open source, free, or commercial. Programmers write applications for specific operating systems; you need to get the software that matches the OS you use. Most companies also make both 32-bit and 64-bit editions of their operating systems.

You toured the basic interfaces of Windows, macOS, Unity (the GUI component of Ubuntu Linux), and Chrome OS, including the major features of

https://t.me/learningnets

each desktop environment. You also learned the differences between Windows 7, 8/8.1, and 10, and what all operating systems have in common. You learned about navigation with hotkeys, screen captures, and accessibility options for people with disabilities.

Questions

1. Which of these is *not* one of the five functions of an operating system?
   - **A.** Monitors system health and functionality
   - **B.** Provides an environment for software to function
   - **C.** Coordinates the activities of hardware components
   - **D.** Sends and receives e-mail messages
2. Which of these is an open source operating system?
   - **A.** Windows
   - **B.** Linux
   - **C.** iOS
   - **D.** macOS
3. If you have a PC with a 32-bit CPU, which operating systems will run on it?
   - **A.** 32-bit only
   - **B.** Both 32-bit and 64-bit
   - **C.** Neither 32-bit nor 64-bit
   - **D.** 64-bit only
4. CTRL-Vis an example of what?
   - **A.** Hotkeys
   - **B.** System keys
   - **C.** Function keys
   - **D.** Launch keys
5. Which key combination switches between open applications in Windows and Linux (Unity)?
   - **A.** F1
   - **B.** ALT-F4

https://t.me/learningnets

B. ALT-TAB

B. WINDOWS-PRINT SCREEN

6. Which of these is an accessibility option for people who have limited mobility?

A. Speech recognition

B. High-contrast color scheme

C. Magnifier

D. Windows flashing or blinking when a sound is played

7. What is the defining feature of a commercial OS?

A. Open source

B. Free

C. Not free

D. Public domain

8. The Dock on a Mac is equivalent to what feature of a Windows 8.1 desktop?

A. Start button

B. Notification area

C. Launcher

D. Taskbar

9. What feature in Windows 10 is equivalent to Finder in macOS?

A. File Explorer

B. Control Panel

C. Start screen

D. Start menu

10. A _____ is a pointer that refers to a file.

A. Launcher

B. Taskbar

C. Shortcut

D. GUI

11. Which OS configuration uses data labels to control resource access?

A. Services

https://t.me/learningnets

B. Scheduled tasks

C. Mandatory access control

D. EULA

Answers

1. **D**. An operating system does not send and receive e-mail messages; that is the function of a mail application. All the other items listed are functions of an operating system.
2. **B**. Linux is open source. Windows, iOS, and macOS are all commercial operating systems.
3. **A**. 32-bit hardware will run only 32-bit operating systems.
4. **A**. CTRL-Vis an example of a hotkey, also called a keyboard shortcut. Function keys are the keys across the top of the keyboard that begin with F, as in F1and F2. There is no such thing as system keys or launch keys.
5. **C**. ALT-TABswitches between open applications. F1opens Help in Windows. ALT-F4closes the active application in Windows. WINDOWS-PRINT SCREENtakes a screen capture in Windows.
6. **A**. Speech recognition can help someone who has trouble typing or using a mouse. The magnifier and high-contrast color schemes would help someone with vision limitations. Windows flashing or blinking when a sound is played would be useful for someone with limited or no hearing.
7. **C**. A commercial OS is not free. Open source and public-domain operating systems are free.
8. **D**. The Dock in macOS is like the taskbar in Windows 8.1. The Start button opens the Start screen. The Launcher is the Dock equivalent in Linux (Unity). The notification area is the rightmost section of the taskbar, where icons appear for background programs.
9. **A**. File Explorer in Windows is like Finder in macOS. Control Panel changes system settings. The Start menu helps you run programs in Windows 10. The Start screen is like the Start menu except it's in Windows 8.1.
10. **C**. A shortcut is a pointer that refers to a file. Launcher is the taskbar/Dock equivalent in Linux (Unity). The taskbar is the bar along the bottom of the screen in Windows. A GUI is a graphical user interface.

https://t.me/learningnets

11. **C**. Mandatory access control (MAC) uses data labels to enforce policies that dictate resource access. Services are programs started by the OS and not the end user. Scheduled tasks run programs on a schedule basis, normally for OS maintenance purposes. The end-user license agreement (EULA) is a commercial software license agreement.

https://t.me/learningnets

CHAPTER 6

Setting Up and Configuring a PC

In this chapter, you will learn how to

- Prepare the work area
- Unpack and set up a new desktop computer
- Complete post-setup tasks

Suppose a neighbor or relative calls you, breathless and excited. “I just bought a new computer! Can you come help me set it up?” Of course, you can help. After all, you’re CompTIA IT Fundamentals certified, right? Or you soon will be. Besides, it’ll be fun.

In this chapter, we provide a lot of practical advice on setting up and configuring new computers. You’ll learn how to choose a good location for a desktop computer, how to navigate the computer’s setup process, and what to do after the initial setup to make sure the computer is connected, secure, and ready for users.

Preparing the Work Area

Preparing the work area for a desktop computer takes into consideration several factors. First, you should look at environmental conditions, such as average temperature and level of dust. Second, you should pick an optimal location. Third, you should evaluate comfort issues. Fourth, you should examine possible interference issues. Finally, you should ensure reliable power. Let’s take a look.

Evaluating Room Conditions

Environmental conditions can make a huge impact on the computing experience. You need to analyze the room conditions for temperature, humidity, and airborne particles. Heating, ventilation, and air conditioning (HVAC) can ensure

https://t.me/learningnets

computing systems last longer than they otherwise would.

The *ideal* room for a computer is probably cooler than you would find comfortable. Performance and stability will suffer if the system gets too hot, but as long as the temperature is between 50 and 75 degrees Fahrenheit or so, it should be fine.



CAUTION You want cool but not cold. Condensation can form when cold air heats up around the hot chips and cause short-circuiting.

Humidity is the amount of water vapor in the air. The ideal humidity level is about 50 percent. High humidity reduces electrostatic discharge (static electricity), an enemy of computer chips. However, extremely high humidity, like 75 percent or more, creates dampness, also an enemy of computer chips.

The computer's room should be as clean as possible and free of dust or other airborne particles that could potentially get inside the PC and interfere with its cooling. By airborne particles in a small office/home office (SOHO) environment, we mean pet hair and dander. If you plan to operate the computer in a dusty or hairy environment, you'll need to regularly clean out the inside of the PC. See Chapter 12 for more information about how to clean a computer.



EXAM TIP Make sure you can identify the impact of environmental factors such as airflow, humidity, temperature, and dust/dander when selecting a location for a computer.

Choosing Where to Set Up the PC

Once you choose a room, where will you put the computer? Is there a desk or table you have your eye on? Make sure there is a grounded (three-prong) power outlet nearby. Don't use an extension cord unless it's absolutely necessary, and if you do, make sure it's a grounded one (or better yet, a surge protector power strip, discussed later in this chapter).

https://t.me/learningnets



NOTE A grounded plug has two prongs for electric current, and a third ground prong to avoid fire and electric shock. Prong layouts and voltage (see "Ensuring Reliable AC Power") are common international power differences, so make sure you get the right plug!

When positioning a desktop PC case, make sure there is adequate airflow all around it, especially vents and fans. Don't back up a desktop PC tightly to a wall because the fan on the back won't have enough space around it. Some computer desks have lower cabinets with doors to hide the case, but we don't recommend these because of poor airflow.

While we're on the subject of case placement, make sure that the PC case is not in a location where it is likely to get kicked, bumped, or knocked off a table. Strike a balance between open-air and out of harm's way.

Making a Work Area More Comfortable

Have you ever noticed that when you sit at some desks, you are comfortable all day, but at others your back and arms start to hurt after an hour or so? The difference between a work area that stresses your body and one that doesn't is *ergonomics*, the study of how humans and equipment interact.



NOTE A product marketed as *ergonomic* is (the marketer claims, at least) designed to place less stress on the body during use than a product not marked as such.

Good ergonomic design and positioning of equipment can enable people to use the equipment extensively with no adverse effects on the body. Bad ergonomics can cause eyestrain, neck and shoulder problems, backaches, and tendon problems such as carpal tunnel syndrome.

Here are some tips for good ergonomics at a computer workstation:

- If possible, use an ergonomic keyboard and mouse. For example, some keyboards curve the keys, with half slanting to the left and half to the right, as shown in Figure 6-1. This helps users keep their wrists straight as

https://t.me/learningnets

they type. An ergonomic keyboard may also have a built-in wrist rest.



Figure 6-1 An ergonomically designed keyboard

- The keyboard should either be flat or be tilted toward the user at up to a 25-degree angle, depending on user preference.
- The display should be 16 to 24 inches from the user's eyes. When looking straight ahead, the user's gaze should fall at the top of or just above the display (Figure 6-2).



Figure 6-2 Ergonomically correct monitor placement

- The distance between the floor and the keyboard should be between 23 and 28 inches, or whatever height is necessary for the user's forearms to

https://t.me/learningnets

be perpendicular to the floor while typing.

- If using a traditional chair (with a rigid seat parallel to the floor), the distance between the floor and seat should be 16 to 19 inches, or whatever height is necessary so that the user's thighs are parallel and calves are perpendicular to the floor when sitting upright with feet flat on the floor.

Avoiding ESD and EMI Problems

Electrostatic discharge (ESD) happens when objects with different electrical charges come close enough for the excess charge to jump quickly to equalize the charge between them. A low-charge object experiences this as a high-voltage electrical shock (Figure 6-3). You've experienced it when touching a door knob in the winter time. Ouch!



Figure 6-3 ESD in action



NOTE Voltage is a measurement (in volts) of the strength of the electrical current. Amperage (or amps) is a measurement of the rate at which the current flows.

https://t.me/learningnets

Sensitive computer components can easily be damaged if ESD sends thousands of volts surging into a device designed for somewhere between 3 and 12 volts. The component (or entire device) might not work right after that, or it might be weakened so that it fails sometime in the future. The tricky thing about ESD is that you can transfer enough voltage to damage the device without feeling a thing. You probably won't know you've ruined an expensive motherboard until your computer fails to start.

Touching the outside of a computer won't cause ESD damage, but touching components inside might. Anytime you open a PC's case, touch the frame to equalize the electrical potential between you and the case (Figure 6-4). Do it periodically as you work inside the computer case to dissipate any difference in potential that might build up.



Figure 6-4 Inside the case, touching the power supply to ground the technician

For even better protection, wear an antistatic wrist strap, as shown in Figure 6-5. This is a band you wear around your wrist with a cable that clips to the PC's frame, so electrostatic charge stays the same between the tech and the computer.

https://t.me/learningnets

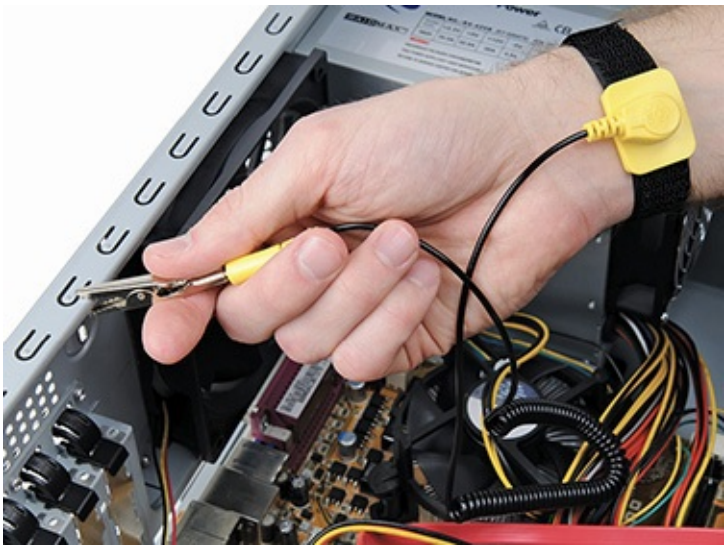


Figure 6-5 An antistatic wrist strap is helpful if you regularly work inside computers.

Other choices can also minimize ESD problems, such as wearing natural fibers and rubber-soled shoes. When possible, work on smooth floor (no carpet). Don’t walk around in polyester socks on nylon carpet before working inside a computer unless you *want* to ruin hundreds of dollars of equipment.

Electromagnetic interference (EMI) occurs when a cable runs too close to something that generates a strong electromagnetic field. EMI is not permanently damaging, but it can garble the data flowing through the cable, and having to retransmit reduces performance. The most common source of EMI is fluorescent lighting; don’t run cables near fluorescent light fixtures. If it can’t be helped, use EMI-resistant cables.



EXAM TIP The IT Fundamentals objectives expect you to know ESD and EMI concepts. Make sure you understand the difference between them and how to minimize or avoid each.

Ensuring Reliable AC Power

Electrical devices rely on the wall outlet to carry a consistent, well-defined voltage. In the United States, standard alternating current (AC) power is between

https://t.me/learningnets

110 and 120 volts, often written as ~115 VAC (volts of alternating current). Most of the world uses 220–240 VAC, so power supplies with *dual-voltage options* work with either standard.

Before you plug a PC into a wall outlet in another country, you should use a power voltage adapter, replace the PC's power supply with a compatible model, or confirm the power supply's voltage selection switch is in the correct position. As shown in Figure 6-6, this switch is next to the power supply's three-prong power port (where you connect the primary power cable from the wall outlet).



Figure 6-6 Make sure the switch on the power supply, if present, is set to your country's AC voltage.

Conditions anywhere between the electric company and your home or office can cause power instability that can damage a computer. A *power outage* is just what it sounds like—power from the electric company isn't reaching your location. Many things can cause this *blackout*, such as storms knocking down power lines.

A *surge* and a *spike* are basically the same thing: a sudden, dramatic increase in the voltage. Computer components are designed to operate at precise low voltages, and they are easily damaged by higher voltages. A lightning strike at or near your home can send a spike of high-voltage electricity through your AC power outlets and into connected devices.

External devices help compensate for these problems. A typical multi-outlet *surge suppressor* (Figure 6-7) can absorb excess power during a surge or spike to prevent it from reaching the plugged-in devices. Surge suppression capacity is measured in *joules*. The higher the joule rating, the greater the protection provided by the surge suppressor. Many (but not all) grounded power strips are surge suppressors; read the package carefully.

https://t.me/learningnets



Figure 6-7 A surge suppressor

A *power sag* is insufficient voltage. Power sags don't usually damage hardware, but they can cause it to temporarily malfunction, resulting in memory storage errors that can cause the operating system to unexpectedly freeze up or restart. When that happens, you may lose unsaved data in open applications.

A *power conditioner* enhances the features of a surge suppressor by storing extra voltage in a capacitor and then releasing it onto the power line to smooth out power sags.



EXAM TIP Collectively, CompTIA IT Fundamentals calls these outages, surges, spikes, and sags *power limitations*. Make sure you know these conditions and which devices can correct them.

An *uninterruptible power supply* (UPS) combines a surge suppressor, a power conditioner, and a battery backup. A UPS (shown in Figure 6-8) can protect against surges and spikes and provide power briefly to deal with sags and power outages. This helps avoid problems (such as storage errors) that occur when a computer can't shut down correctly. A typical UPS connects to the PC (usually via universal serial bus [USB]) so the operating system (OS) can shut itself down automatically when the UPS reports a power outage.

https://t.me/learningnets



Figure 6-8 An uninterruptible power supply

Setting Up a Desktop PC

Unpacking a new PC, even if it's somebody else's, always feels like Christmas morning to us. Carefully unwrapping the protective plastic, removing the little tape tabs and Styrofoam protectors…there's nothing like it. You may not share our geeky enjoyment of this task, but there's nothing to fear. The following sections provide some tips for making the setup as painless as possible.

Physical Connections

Unpack things carefully, preserving the packing materials in case you have to return it. Save every plastic bag and every hunk of Styrofoam.

Plug the cables in snugly, referring to the instructions that came with the PC or using your own knowledge from Chapter 3. The basic connectors are as follows:

- **Keyboard and mouse** Any USB port. Figure 6-9 shows a USB connector ready to be plugged into one of several USB ports on the back of a desktop PC.

https://t.me/learningnets



Figure 6-9 Connect USB external devices to any USB port on the PC.

- **Monitor** Digital Visual Interface (DVI) or High-Definition Multimedia Interface (HDMI) port if available; Video Graphics Array (VGA) is your backup plan. On a Mac, use Thunderbolt or Mini DisplayPort.
- **Internet** Connect an *Ethernet cable* to an RJ-45 port on the router or broadband modem and another on your system, or plan to set up a wireless connection to a wireless modem or router later.
- **Speakers** 3.5-mm speaker jack. Make sure you use the one for speakers and not the similar-looking input port for a microphone. Most manufacturers use green for the speaker port and pink for the microphone.



EXAM TIP Make sure you know which ports to connect which components to on a desktop PC. Practice this by unplugging all the cords on the back of a desktop PC (turned off) and then reconnecting them.

https://t.me/learningnets

Cable Management

With all the connections you've just made, you may have a tangle of cables on the back of the PC, running every which way. There's nothing wrong with that, as long as the cables don't become a trip-and-fall hazard or a dust-bunny hideout.

If ugly haphazard cables aren't acceptable (for example, a computer out in the open on a receptionist's desk) or you're worried about stray cables as hazards, the solution is cable management. That sounds fancy, but it really just means adding channels for cables to run through in an orderly way or binding groups of cables with cable ties.

Cable management is a much bigger deal in businesses where many computers share a fairly small space and cable proliferation can get out of hand. Figure 6-10 shows a particularly messy bunch of cables in need of some organizing. Figure 6-11 shows a well-ordered mass of cables on a network panel sorted out with cable ties.

https://t.me/learningnets

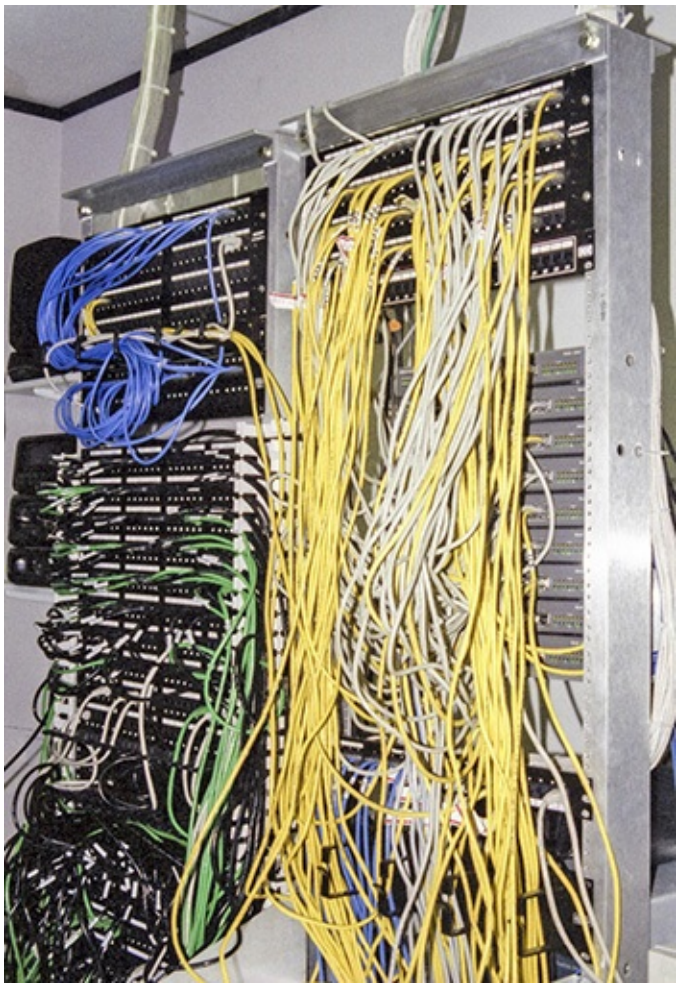


Figure 6-10 Disorganized cables

https://t.me/learningnets

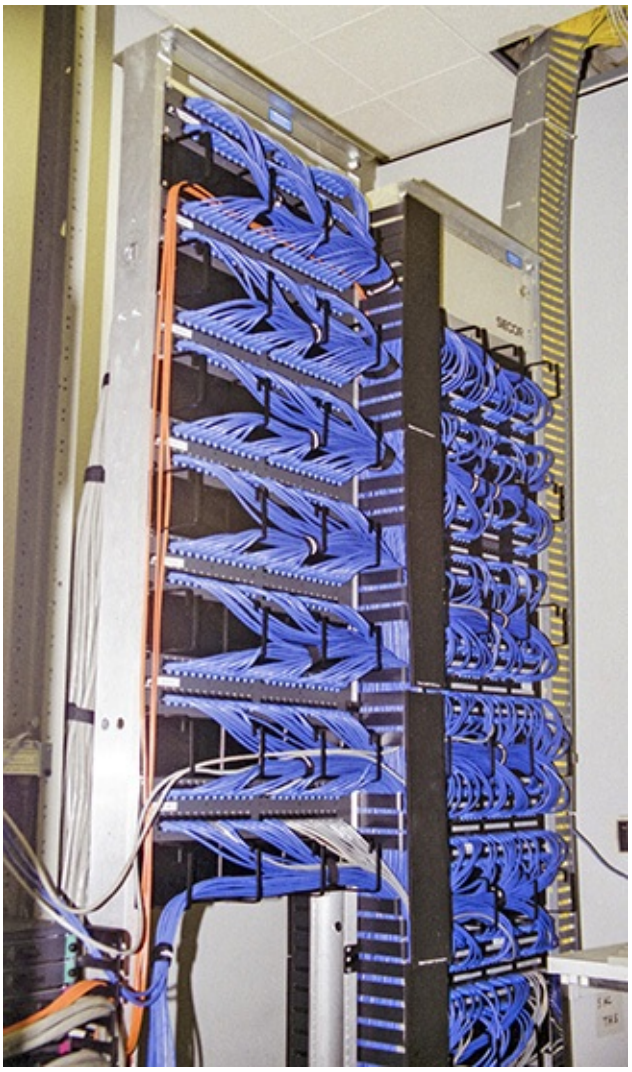


Figure 6-11 Well-organized cables

Operating System Setup

The first time you press the power button to start a new computer, a setup program runs for the already-installed operating system. The specifics will vary by OS and version, but it generally configures the following:

- **Localization** What time zone are you in, and does the time change for daylight saving time in your area? What country are you in? (Country affects the default currency symbol and some other details.)
- **Screen resolution** This is selected for you automatically and silently; the setup program detects your display adapter and monitor, determines the maximum resolution, and sets the OS to that resolution.

https://t.me/learningnets

- **Audio settings** Like screen resolution, your audio hardware settings are also autodetected and set up in the OS.
- **Internet connectivity** The setup program looks for an Internet connection and asks whether you want to use the connection it finds. If it doesn't find one, the setup program may prompt you to configure an Internet connection or to skip that step for now.
- **User account** Most operating systems support multiple user accounts on a computer. The setup program will insist that you create at least one user account to start. This default user account will have full administrative permissions. You can create more accounts later.

This step isn't brain surgery; just follow the prompts and skip anything optional that you don't understand.

Completing Post-Setup Tasks

You need to take several other steps to prepare a PC for use, such as installing security software, making sure the network connections are working, configuring peripherals, and installing additional software. You might also want to set up other user accounts. The following sections explain each of these tasks.



EXAM TIP You should be able to list the post-installation tasks involved in setting up a new PC, covered in the following sections.

Verify and Configure the Internet Connection

If the OS found an Internet connection during its initial setup, great. If that connection is wireless, make sure it's secure. Connecting to a wireless access point that doesn't require authentication can put your computer at risk for snooping by anyone who happens to be nearby on that network.

If you own the wireless access point, enable its security. If you are using someone else's unsecured Wi-Fi, at a minimum you should turn off File and Printer Sharing in your operating system so others cannot browse your files. See Chapter 10 for more on both of these.

https://t.me/learningnets

Install Security Software

Before you start using the PC, make certain it has adequate security software installed. Windows comes with a program called Windows Defender, which provides basic antivirus and anti-malware protection, and it's enabled by default. However, depending on your situation, you may want to install a more full-featured security program, such as one that your employer or school provides. Chapter 11 explains security software and how it works in more detail.

Run Software and Security Updates

Between the time the OS was installed on your new computer and now, some updates have probably been released. It's important to have the latest OS updates because many of the updates fix security holes. So before you go any further, you should make sure your OS is up to date. By default, Windows is set to download and install updates automatically.

In Windows, use the Windows Update feature to download and install updates. Here's how to run it in the last several Windows versions:

- **Windows 7/8/8.1** Open the Control Panel, click System and Security, and under the Windows Update heading, click Check for updates.
- **Windows 10** Click Start | Settings, click Update & security, and under Windows Update, click Check for updates, as shown in Figure 6-12.

https://t.me/learningnets

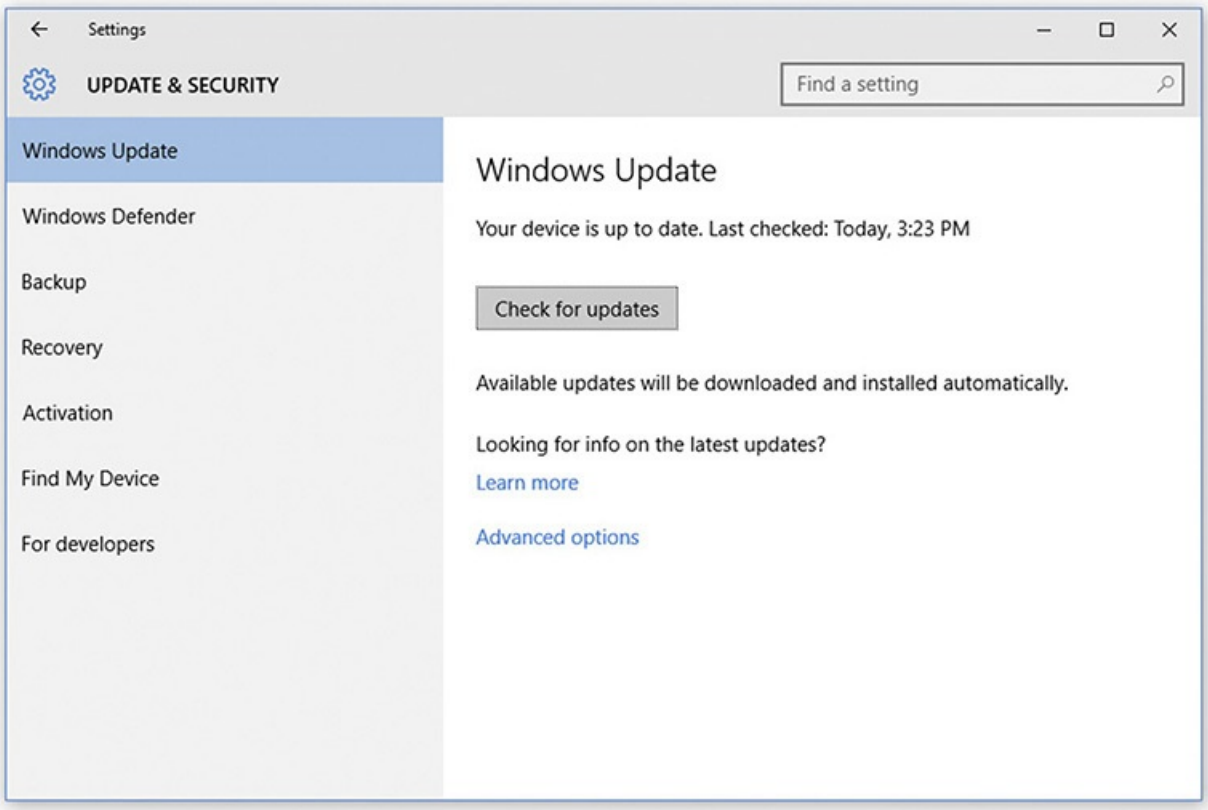


Figure 6-12 Checking for Windows updates

On a Mac, you get OS updates via the App Store. Open the App Store and then click Updates. If any OS updates are available, they will appear in the list of available updates. Apple will push some important OS updates to you more aggressively so that a message pops up on the screen inviting you to install the update.

Configure Peripherals

You might have additional hardware that you want to set up on the new PC. Many folks add an additional input device (such as a touchpad) or output device (such as a printer). In many cases you can plug a new device into a USB port and the OS will automatically recognize and install a driver for the device.

If a peripheral comes with its own setup disc, that disc may contain helpful applications. A scanner might include an optical character recognition (OCR) application that converts images of scanned text to text you can edit in a word processing program. Pop the disc in the PC's optical drive and let it run its setup program. If you don't have a disc, download the latest version of the device's

https://t.me/learningnets

setup program from the device manufacturer's web site.



CAUTION The included software is occasionally essential, especially for less common devices or ones with special features that only work with the manufacturer's software. Read the instructions before you connect the device to the PC for the first time; you may need to run the setup program first and connect the device only when the setup program prompts you.

Many modern peripherals such as network printers and a wide variety of Internet of Things (IoT) devices (such as home automation solutions) can be configured over an IP connection. You can connect to the device over a TCP/IP local or wide area network using a web-based configuration GUI. Alternatively, if available, you might use a small local LED display on the device with buttons to configure its settings.

After you've installed a peripheral such as a network printer, you can configure it in the OS settings. For a standard input device like a keyboard or mouse, you can use the Options dialog box from the Control Panel for that particular device type (for example, Mouse Properties in Figure 6-13). For devices with proprietary software, run the software to configure the device. If the device has a memory-resident component, there may be an icon for the device in the notification area in Windows. If you see one, right-click the icon and choose Properties or Options (or similar) to configure the device's settings.

https://t.me/learningnets

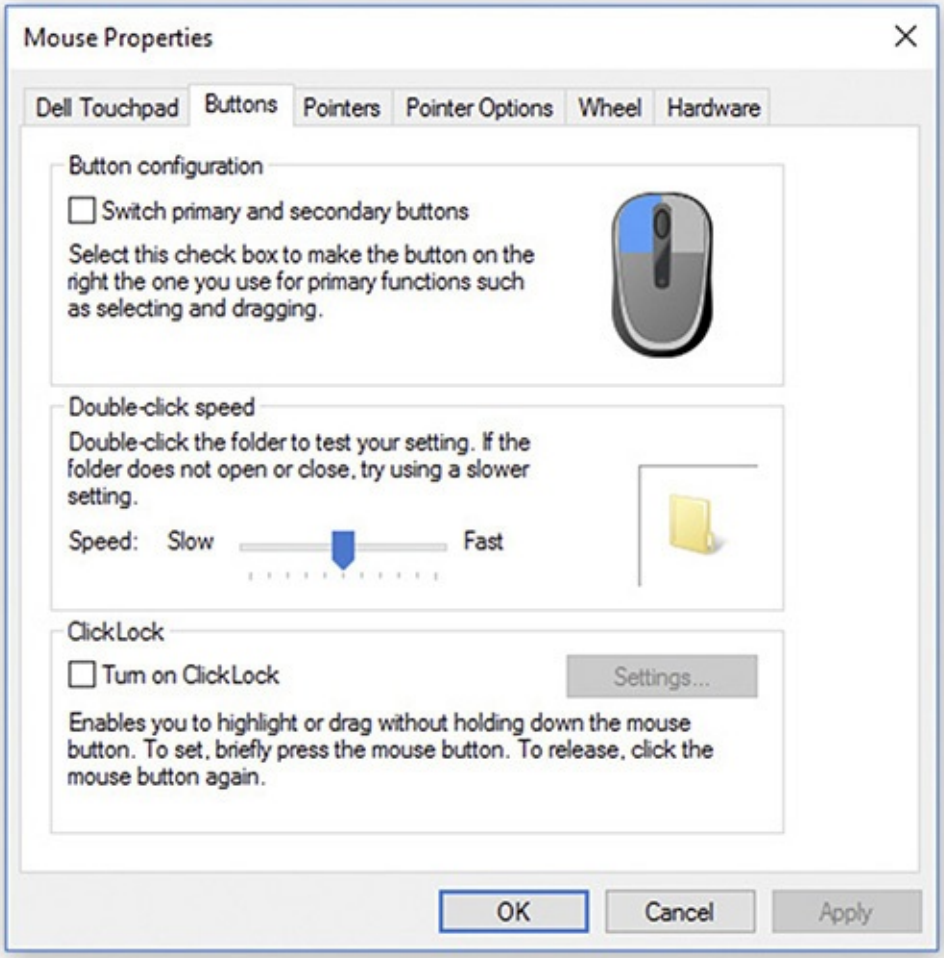


Figure 6-13 Configuring a device via its Properties box

Uninstall Unneeded Software

Many new computers come with what technicians not so affectionately refer to as *bloatware*—applications most people don't need (or want) preinstalled because their developers paid the PC manufacturer. This can include trial versions of useful software, marginally useful software, and stuff that is downright annoying. Part of the post-setup cleanup is removing some of this bloatware.

To remove an application in Windows, open the Control Panel and run the Programs and Features applet. Select the application you want to remove and then click the Uninstall button (or Uninstall/Change in some cases), as shown in Figure 6-14. Then just follow the prompts to uninstall it.

https://t.me/learningnets

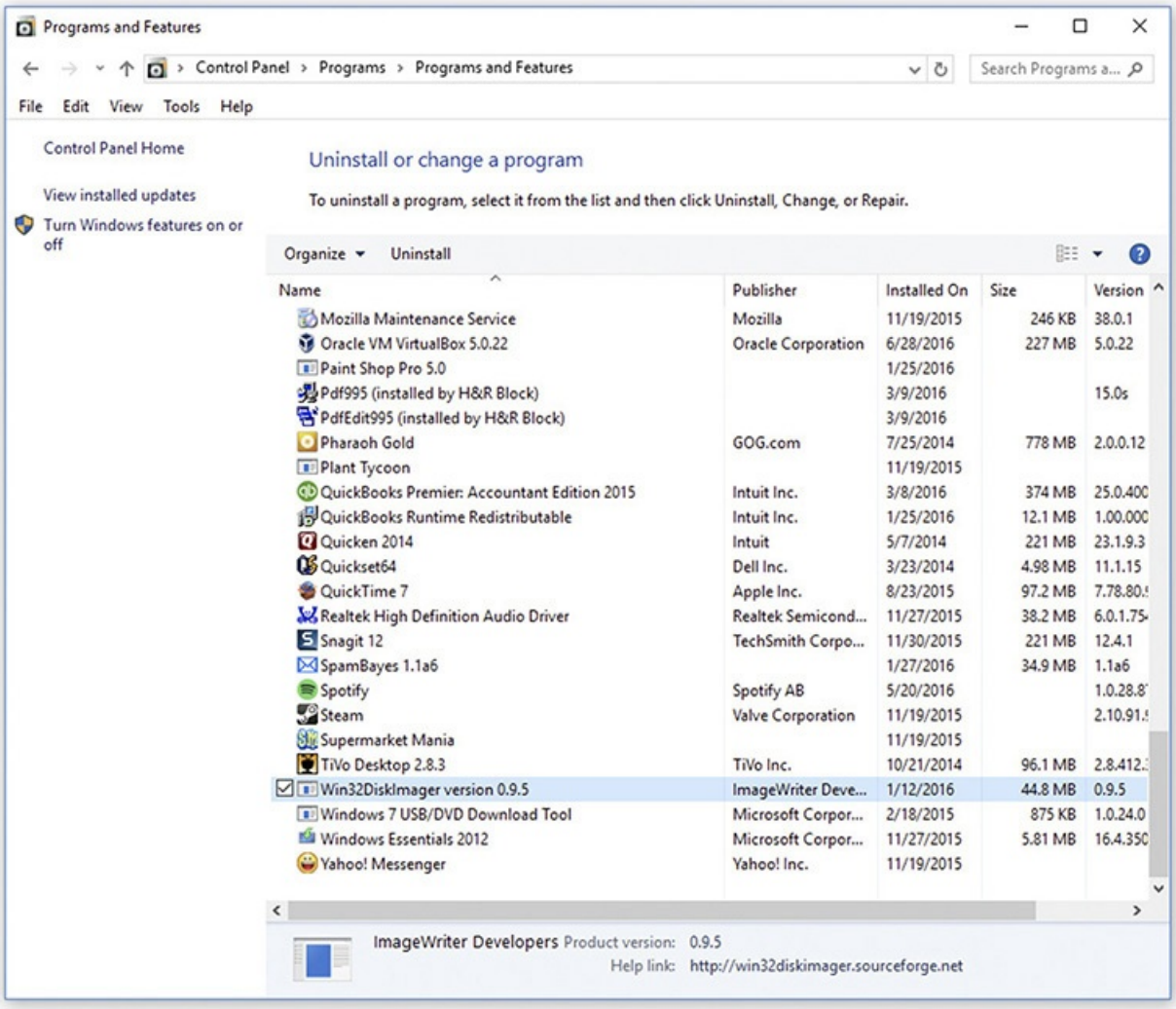


Figure 6-14 Uninstalling unwanted applications



EXAM TIP It's mostly for advanced users, but Programs and Features can also add and remove optional *OS features*. Just click Turn Windows features on or off and check or uncheck the specific features. Don't mess with these unless you understand a feature's risks and benefits or are following instructions from a tech who does.

To remove an application in macOS, open Finder and choose Applications in the navigation pane on the left. Then right-click an application to remove and

https://t.me/learningnets

choose Move to Trash. You might need to type your password to confirm.

Install Additional Software

Now it's time to install software you actually want on the new computer, such as applications you bought for a previous computer. To install an application from disc, insert the disc and follow the prompts that appear. If nothing happens, open Windows Explorer, File Explorer, or Finder (or equivalent file management program) and double-click the icon for the optical drive. If a file listing appears, double-click the Setup file in that listing.



NOTE The Setup file may appear as Setup.exe. The .exe part is the file's extension. Extensions identify file types; .exe is short for "executable" (in other words, a program). You'll learn more about file types and extensions in Chapter 8.

In some cases, the file that starts the setup program isn't named Setup. It might be Install, RunMe, or some other intuitive name.

Increasingly, you can just download software. You download a setup file and then run that file to install the application. If you still have a setup file on an older computer, you can transfer it to the new computer via USB flash drive, a writeable optical disc, or a network connection. It's best to use this as a fallback, though, since the programs will likely be out of date and may be vulnerable to widely available exploits until you update them.

Create More User Accounts

The user account that you set up when you do the initial computer setup has Administrator privileges. That means the account can install and remove software, change system settings, and do anything else that needs to be done. "Great!" you may be thinking. "I never have to worry about not having high enough permission levels to do whatever I want to the computer."

Using an Administrator account all the time increases the security risk. If malware infects your computer and tries to make changes to system files, for example, it can do serious damage with the power of an Administrator account. For this reason, Microsoft recommends you create a Standard account for daily use. A Standard account can change settings that affect only that one account.

https://t.me/learningnets

Microsoft recommends that you sign into your Administrator account only when you need to make system changes, such as installing new software or updating device drivers. You can also create Child accounts (Mac calls these Managed with Parental Controls), which are like Standard accounts except you can restrict what web sites they can visit, what times of day they can use the PC, and so on.

In Windows 8.1 and 10, user accounts are tied to an e-mail address registered with Microsoft. These accounts are also known as *Microsoft accounts* because Microsoft manages the account permissions and passwords online. A Microsoft account has advantages such as access to your OneDrive and Windows settings from any PC you sign into.

An alternative is a Local account, which is not registered with Microsoft and exists only on the local PC. Microsoft tries to discourage this type of account by making it more difficult to set up.

To create a new account in Windows 10, click Start | Settings | Accounts. Click Family & other users. To add a family member (such as a Child account), click Add a family member. To add other users, click Add someone else to this PC. Then just follow the prompts, which differ for Microsoft accounts and Local accounts. The prompts are also affected by whether an e-mail address has already been registered with Microsoft on some other computer.

Chapter Review

In this chapter, you learned about the process of setting up a new computer. Before you begin, it's important to pick out a work space that is good for the computer (good airflow, cool temperature, low dust, appropriate humidity, reliable power, and so on) and has good ergonomics for the user. During setup, maintenance, and operation, make sure you take steps to protect the system from ESD and EMI.

The setup process itself begins with carefully unpacking the components in case you need to return the system, physically cabling and connecting the components, and using any desired cable management devices to keep all of the cords and cables in order. Once all of these are connected, you're ready to insert the operating system's installation media and follow the on-screen prompts.

There are a few things left to go over once the OS is up and running. First, you need to verify that the system has a functioning, secure Internet connection. Once you have a secure Internet connection, you can install current security software as needed and update your OS and applications to fix known security issues.

https://t.me/learningnets

Now that the system is protected, you can install additional peripherals, remove any preinstalled software you don't need, install the applications you plan to use, and create user accounts for anyone else who'll be using the system. The next time someone asks you for help with their new PC purchase, you will be prepared to walk them through the process with confidence.

Questions

1. In which environment would a desktop computer be safest and operate the best?
   - **A.** Inside a small, tightly sealed cabinet
   - **B.** In a clean room with a powerful air conditioner running
   - **C.** On the balcony at a tropical beachfront condo
   - **D.** On a TV tray in a living room
2. How far should a user's face be from a monitor screen for most comfortable viewing?
   - **A.** 10 to 12 inches
   - **B.** 12 to 16 inches
   - **C.** 16 to 24 inches
   - **D.** 24 to 32 inches
3. Which of these is the flow of static electricity?
   - **A.** EMI
   - **B.** ESD
   - **C.** AC
   - **D.** DC
4. What device can help correct power sags?
   - **A.** Power supply
   - **B.** Power strip
   - **C.** Surge suppressor
   - **D.** UPS
5. What kind of cable is most often used to connect a PC to a broadband modem or router?
   - **A.** VGA

https://t.me/learningnets

B. DVI

C. Ethernet

D. RJ-11

6. What should you install before you download and install additional software on a new PC?

A. Security software

B. Nothing

C. Updates to other applications

D. Drivers for hardware devices

7. What component protects against occasional electrical spikes?

A. Surge suppressor

B. Motherboard

C. Hard disk drive

D. Printer

8. Where in Windows can you access the configuration settings for hardware devices like mice and printers?

A. File Explorer

B. EMI

C. Start menu

D. Control Panel

9. Where in the Control Panel can you remove unwanted applications?

A. Programs

B. Ergonomics

C. Setup

D. Start menu

10. Which of these is a type of Windows user account?

A. Kid

B. Standard

C. Supervisor

D. Normal

https://t.me/learningnets

Answers

1. **B**. A computer would operate very well in a clean room (no dust) with a powerful air conditioner (cold). A tightly sealed cabinet would not allow enough airflow. A balcony in a tropical location would be too warm and humid. A TV tray would be unstable and easy to knock over.
2. **C**. The optimal distance is 16 to 24 inches.
3. **B**. ESD is short for electrostatic discharge, the flow of static electricity. EMI is electromagnetic interference, a magnetic field that can cause problems to nearby data. AC is alternating current, the power from a wall outlet. DC is direct current, the power used by computer components.
4. **D**. A UPS combines a power conditioner, battery backup, and surge suppressor. None of the other options listed does anything for sags, although surge suppressors can help with power surges and spikes.
5. **C**. An Ethernet cable is used to connect to a broadband modem or router. VGA and DVI are used for monitors. RJ-11 is used for dial-up modems.
6. **A**. You should make sure security software is installed before downloading anything else.
7. **A**. A surge suppressor can protect against power surges and spikes.
8. **D**. Use the Control Panel to configure hardware devices. File Explorer is the file management interface. EMI is electromagnetic interference, which is not a Windows feature. The Start menu does not contain settings for hardware devices.
9. **A**. Uninstall applications from the Programs section of the Control Panel. None of the other options listed is a section in the Control Panel.
10. **B**. Standard is one of the Windows user account types. The others listed are not.

https://t.me/learningnets

CHAPTER 7

Setting Up and Configuring a Mobile Device

In this chapter, you will learn how to

- Describe features that mark mobile devices
- Set up and manage mobile device security
- Establish wireless connectivity and pairing
- Configure e-mail
- Configure synchronization
- Install and remove apps

Writers and teachers on computing devices tend to focus on the desktop computers running Windows or macOS. Some might tip the hat to laptops or Chromebooks, but those devices run standard desktop operating systems.

The vast majority of consumers around the world, on the other hand, use a radically different computing device—a mobile device like a smartphone.

The CompTIA IT Fundamentals exam likewise focuses on Windows PCs, but you need to understand a lot about mobile devices to function in today's mobile world. This chapter goes a little beyond the exam objectives but offers relevant information for any computer user.

The chapter starts with an overview of mobile devices. It then hits five major aspects of the mobile computing experience:

- How to set up a mobile device
- How to establish wireless connections
- How to configure e-mail
- How to sync with other devices
- How to install and remove apps

https://t.me/learningnets

We have a lot of ground to cover, so let's get started.

Mobile Devices: A Quick Overview

Mobile devices have three features that distinguish them from desktop computing devices: size, interface, and OS.

Size matters. Mobile devices come in four basic formats, all designed to hold in your hand or wear like jewelry:

- Smartphone
- Tablet
- Phablet
- Wearable

A *smartphone* combines a mobile phone and a small handheld computer, and a *tablet* is a slate-style touchscreen device, which may or may not have cell phone capability. Tablets that have phones in them are referred to as *phablets*. There are also several kinds of specialty mobile devices, such as mobile media players, fitness trackers, and e-readers, but they are less popular because smartphones and tablets can do the same things they do and more. A *mobile media player* is a device that plays music or videos but does little else.



EXAM TIP Objective 2.6 of the CompTIA IT Fundamentals exam mentions streaming media devices. A decade or so ago, you would find mobile music players like iPods in almost every pocket, but they are a dying breed in everyday life today because smartphones and tablets play video and audio so well.

Mobile devices have *touchscreen* interfaces (which you know from earlier chapters), but you can also use a pen-like input device. A simple *stylus* affects most touchscreens like a finger would, but a few devices with advanced digitizers support a pressure-sensitive stylus tailored for digital writing, drawing, and painting on the device.

The major operating systems for mobile devices are Android, iOS, and Windows. Android enjoys the most market share with about 77 percent, probably because it is free (so Android devices tend to be more affordable).

https://t.me/learningnets

Apple's iOS comes in second at around 19 percent. Mobile Windows devices use special versions of Windows that differ from the Windows you know as a desktop and laptop operating system. Windows Phone has a paltry 0.5 percent of the market. This chapter focuses on Android and iOS, though it touches on potential exam questions about the others.



NOTE These statistics refer to June 2017 through June 2018 and come from http://gs.statcounter.com/os-market-share/mobile/worldwide. The exact figures change constantly, but the general trend holds steady: Android and iOS are the main mobile operating systems, and everything else trails far behind.

Setting Up the Device

When you unpack a new mobile device, connect it to alternating current (AC) power and press its power button to turn it on and start the setup routine. Some devices require you to hold the power button down for a few seconds until something appears on the screen or until you feel the device vibrate briefly. Check the documentation to find the power button if needed.

The device will go through a setup process the first time you turn it on, which may include entering information about yourself and your location, calibrating the touchscreen, and granting permission for the device to use certain online services and apps. Just follow the prompts.

Understanding the Interface

Both Android and iOS use the same basic desktop metaphor for navigation. The Home screen features a collection of icons. Each icon represents a different feature or app. You can customize this Home screen by reordering the icons and creating groups to organize them. Figures 7-1 and 7-2 show the Android and iPhone interfaces, respectively.

https://t.me/learningnets

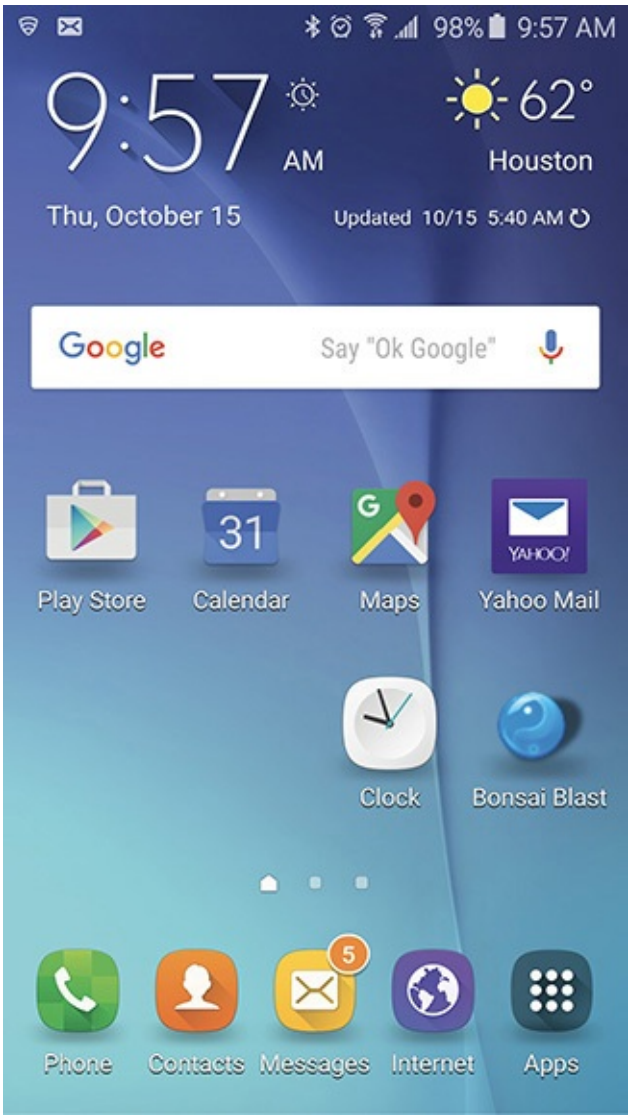


Figure 7-1 Android smartphone Home screen

https://t.me/learningnets



Figure 7-2 iPhone Home screen



NOTE The iOS experience is fairly consistent because it runs only on Apple hardware, but Android runs on so many different brands of hardware that there are different procedures. For example, some Android phones have a hardware Home button, and others don't. Most companies customize the version of Android that they put on their devices. (Like Linux, Android is open source.) If you have an Android device that doesn't work as described, it's probably because of some brand-specific differences; check your device's documentation or online support site.

To return to the Home screen, press the Home button, which may be a

https://t.me/learningnets

hardware button on the device or an on-screen icon (Figure 7-3). Returning to the Home screen does not exit open apps.

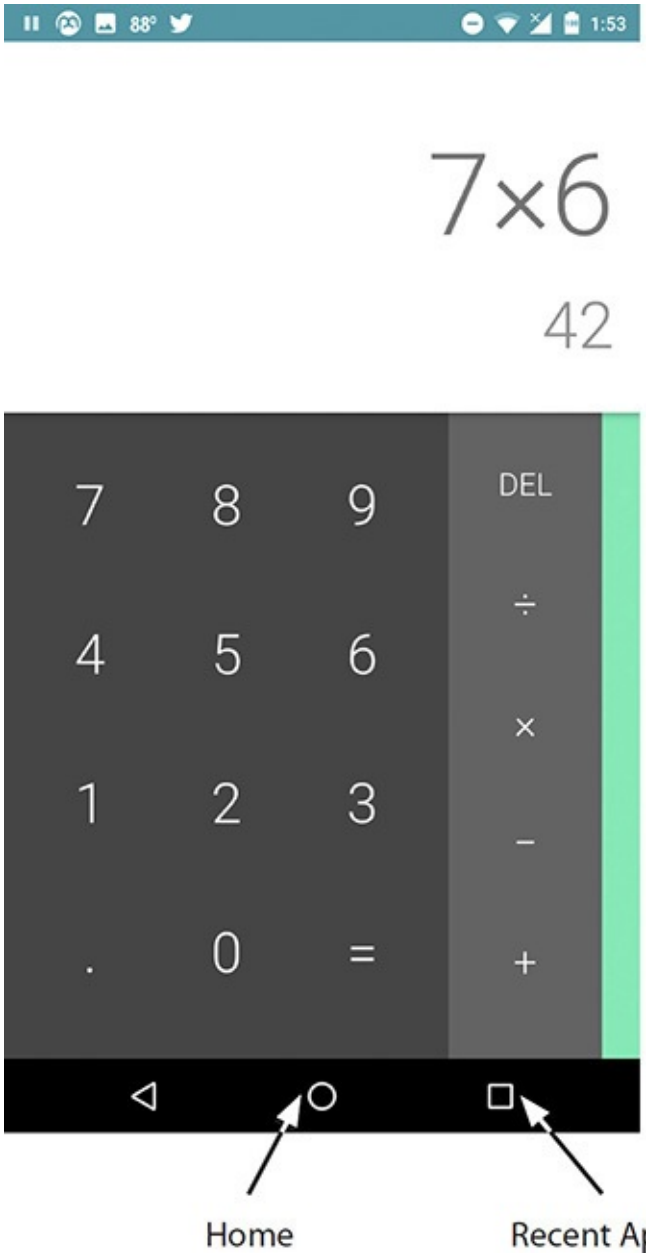


Figure 7-3 Home and Recent Apps icons

To switch among open apps in Android, tap the Recent Apps icon at the bottom of the screen or press and hold (also called a *long press*) the Home button, depending on the device. Small images (*thumbnails*) of the open apps appear. Tap the one you want.

https://t.me/learningnets

In iOS, double-press the Home button (Figure 7-4). Images of the open apps appear, as shown in Figure 7-5. You can page through them by swiping left or right and then tap the one you want. To close an open app, swipe upward on it when in this view.



Figure 7-4 Home button on an iPhone

https://t.me/learningnets

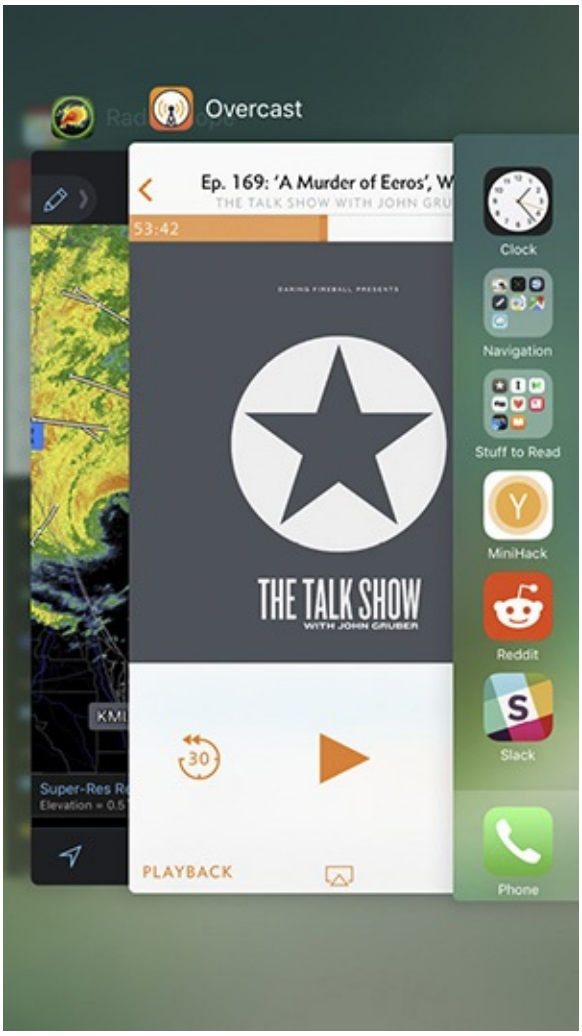


Figure 7-5 Swipe through the open apps and tap the one you want in iOS.

Using Gestures

Gestures—various actions using one or more finger—enable you to interact with a touchscreen. These input options are called *gesture-based interaction*. Here are some examples:

- **Tap** Briefly touch the surface with a fingertip.
- **Double-tap** Rapidly touch the surface twice with a fingertip.
- **Swipe** Touch the screen and then drag your finger across it in a certain direction. For example, you could swipe left or right. In some apps, swiping left (that is, moving your finger from right to left) goes back to the previous screen or page.
- **Pinch** Touch the surface with two fingers spread apart and then pinch

https://t.me/learningnets

them closer together to zoom out. To zoom in, start with your fingers together and spread them apart. Some people collectively call these pinch in/closed and pinch out/open gestures *pinch-to-zoom*.

- **Rotate** You can touch the surface with two fingers as you would to zoom out but then rotate them on the screen. This is often used to rotate images in photo-viewing/editing programs or to rotate the map orientation in a navigation app.

Understanding Kinetics

Many mobile devices include *kinetics*—electronic sensors that track the device's position and movement in 3D space. You don't have to do anything to these sensors. They just exist, doing their jobs and reporting their data to any apps that ask for it.

The sensors inside a typical smartphone or tablet include the following:

- **Accelerometer** Determines how fast the device is moving through space, like a speedometer does for an automobile.
- **Magnetometer** Works like a compass to detect the device's orientation relative to the earth's magnetic north.
- **Gyroscope** Measures the rotational velocity and position along three axes (in 3D space). This is also called the *attitude* sensor or the *rotation* sensor. This is the sensor that, among other things, senses the orientation of the device and rotates the screen.

Controlling Screen Orientation

By default, smartphone and tablet screens change their orientation automatically depending on the orientation of the device. So, for example, if you turn your iPhone clockwise, the interface rotates and changes to wide-screen mode. You can optionally lock the screen in either portrait (tall) or landscape (wide) orientation if you prefer.

In iOS, you can lock or unlock the screen orientation by doing the following:

1. If you want to lock the screen to a particular orientation, start in that orientation.
2. From the Home screen, swipe upward from the bottom.
3. Tap the Orientation Lock icon (Figure 7-6).

https://t.me/learningnets

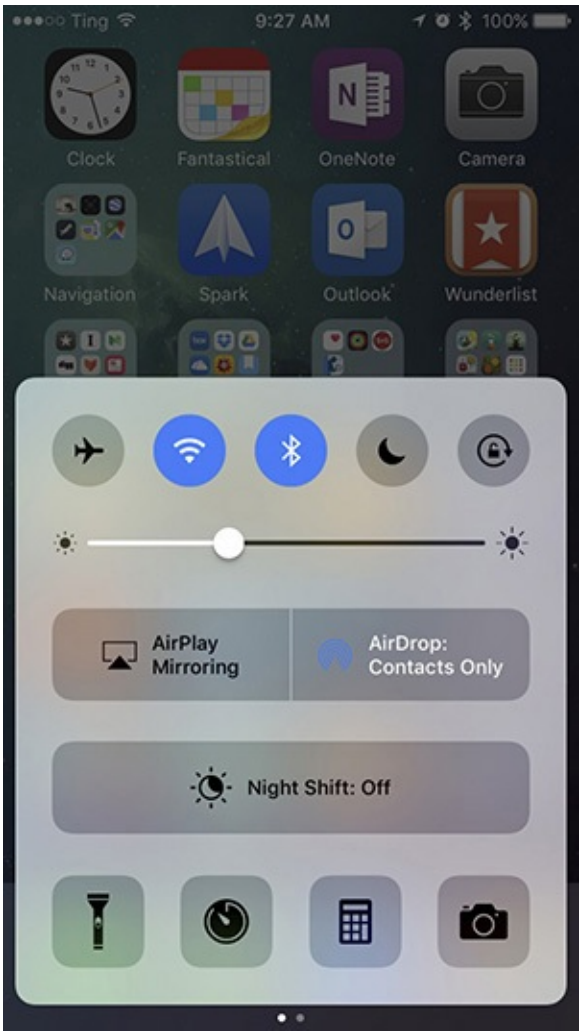


Figure 7-6 Orientation Lock icon

Here’s how to do the same thing in Android:

1. If you want to lock the screen into a particular orientation, start in that orientation.
2. Swipe down from the right side of the top panel.
3. Tap the Auto Rotate button.

Alternatively, in Android you can go to Settings | Accessibility and select Auto-rotate screen.

Security Features

https://t.me/learningnets

All modern tablets and smartphones include security capabilities that keep unauthorized users out of your device. The following sections explain some of the security features you can employ.



EXAM TIP Chapter 11 covers more security features on both mobile and desktop computing devices, such as disabling unused features like Bluetooth so they cannot be used by attackers.

Setting and Changing a Lock Passcode

If you set a device's *screen lock*, it will always wake up to the *lock screen*. You can just swipe to unlock the simplest screen locks, but more secure locks prompt you for a password or short *passcode*, as in Figure 7-7.

https://t.me/learningnets



Figure 7-7 Prompting for a passcode

Depending on the OS type and version, different passcode options may be available. For example, you might be able to choose between a four-digit number, a six-digit number, or an alphanumeric code (letters and numbers). A six-digit alphanumeric combination offers the highest security. Figure 7-8 shows these options on an iPhone. On some newer devices you can authenticate your identity with a fingerprint reader.

https://t.me/learningnets

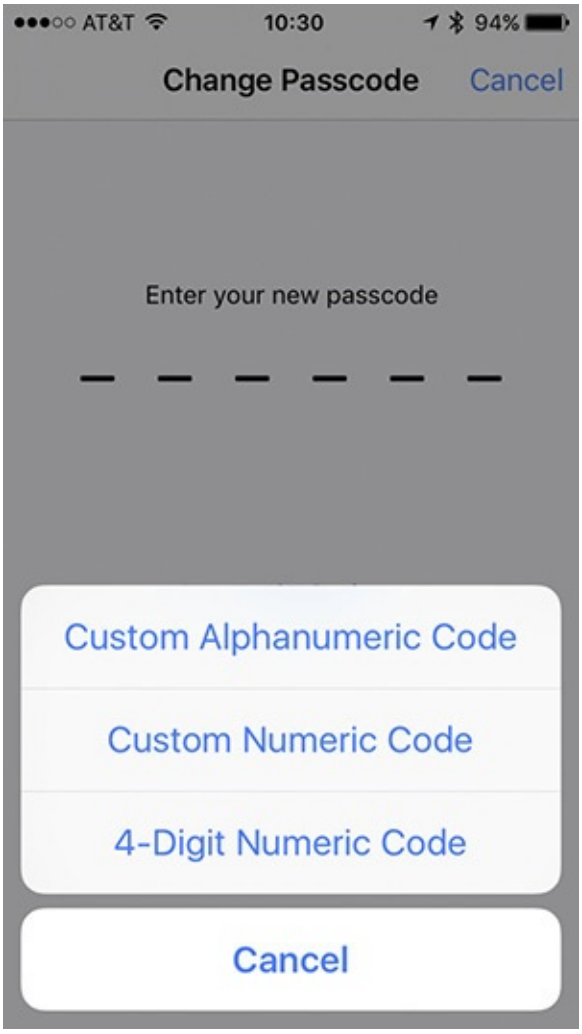


Figure 7-8 Choose the level of passcode security you want to use.

On an Android phone, tap the Settings icon and tap Lock Screen to access the passcode options. In iOS, tap the Settings icon (which looks like a gray cog) and then tap Touch ID & Passcode. From there you can set and change your passcode.



TIP You might also want to change the lock timeout (how long the device can idle before the screen turns off and locks). A shorter time makes for better security, but a longer time is more convenient.

https://t.me/learningnets

Configuring Account IDs and Passwords

Some activities require extra authentication beyond unlocking the phone. When you make purchases in an app store using a stored credit card number, for example, the store typically prompts you for a password. For an Android phone, this is your Google Account. For an iPhone, this is your Apple ID.

Managing Lost Device Security

So, you've lost your smartphone or tablet, and you are panicking—not so much for the loss of the device itself, although that's an inconvenience, but for the violation of your privacy. Maybe you had all your account passwords stored there for various web sites, or your deepest darkest secrets were kept in your phone's diary.

If it's an Android device signed into a Google account, you can use a web browser and navigate to https://www.google.com/android/find to show your device's location (Figure 7-9). For this to work, the device needs to have a WiFi or mobile data connection and an active SIM card. In other words, whoever holds the device can just turn it off or pop the SIM card out to keep you from locating it. The Android Device Manager also allows you to remotely ring, lock, or erase the device.

https://t.me/learningnets

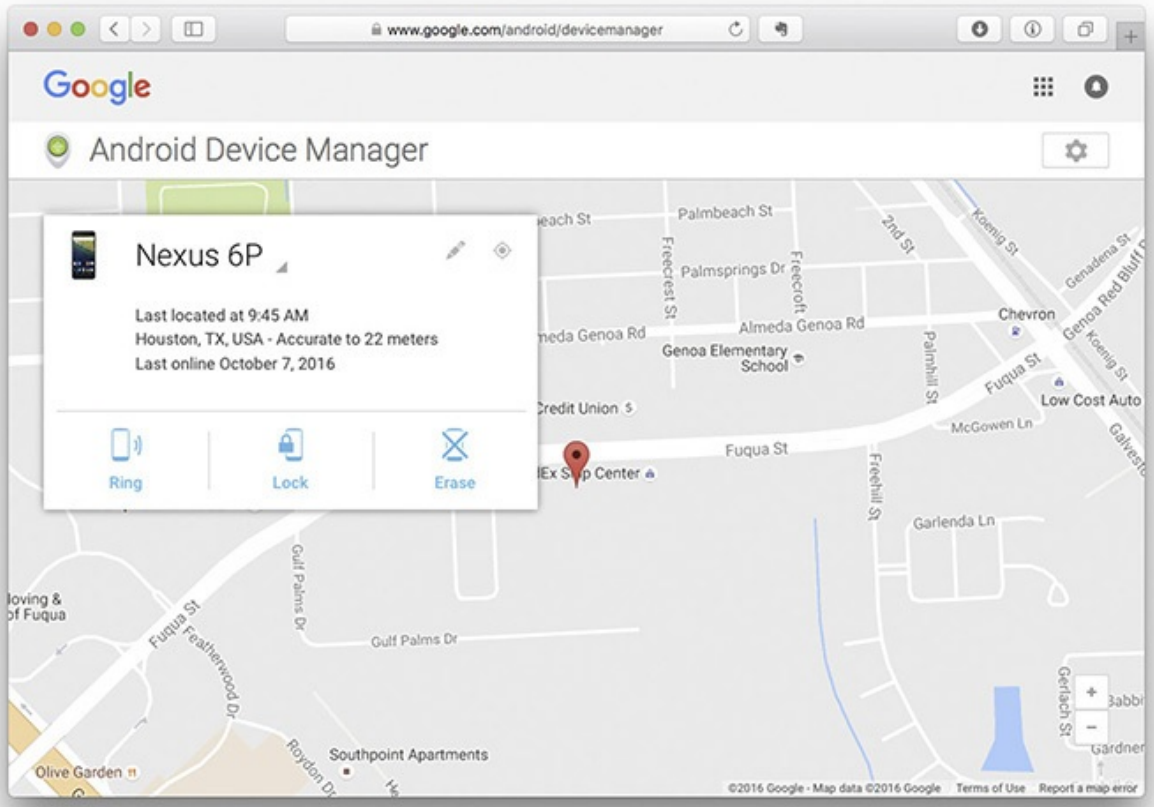


Figure 7-9 Android Device Manager finding a lost smartphone

If you successfully locate it, you can opt to have the device ring or receive a notification (Figure 7-10), to lock it, or to remotely erase it. This is good (for you) if *someone else* has managed to access your Google account and is using it to locate you, but if *someone else* has the device, they may notice that you're locating the device. If you're coming to wipe private information, be prepared to act swiftly.

https://t.me/learningnets

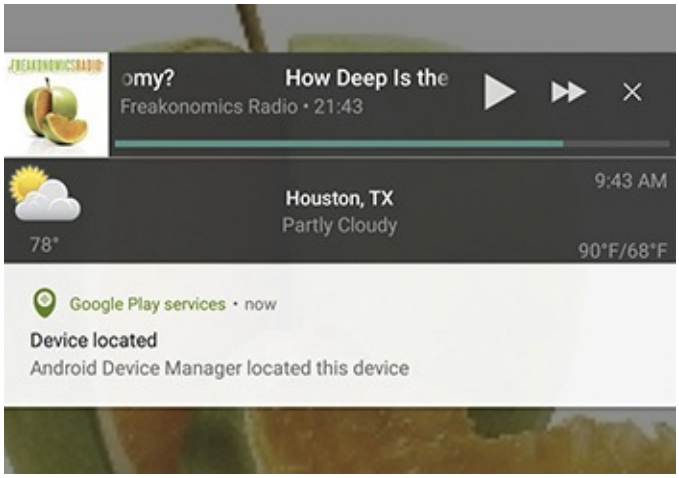


Figure 7-10 Android phone receiving a notification that it has been located

On an iOS device, sign into iCloud using a web browser and select Find iPhone. Then click All Devices and select the desired device (Figure 7-11).

https://t.me/learningnets

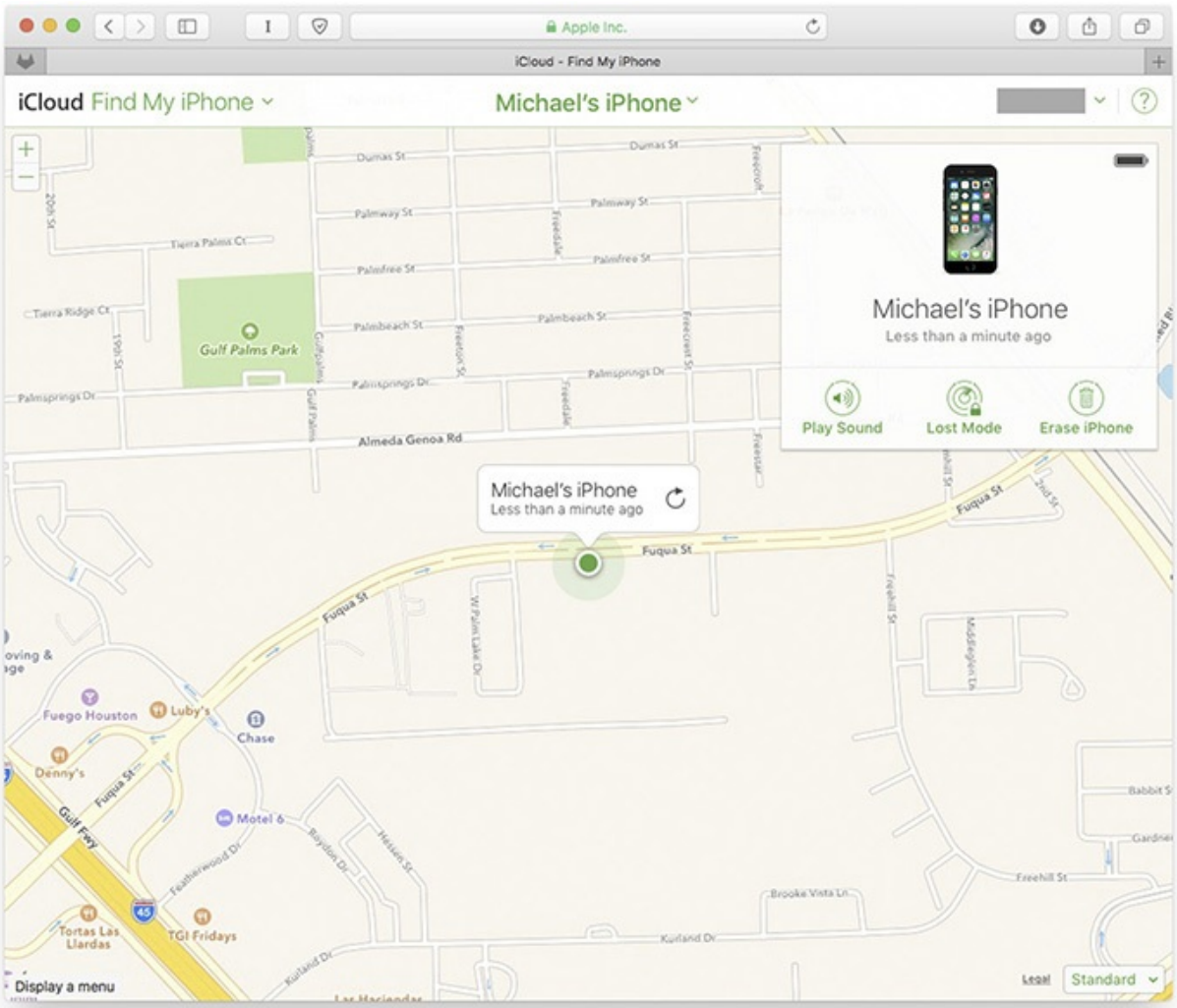


Figure 7-11 iCloud finding a lost iPhone

The next step depends on whether you think the phone was lost or stolen. If you think it's lost and the person who has it might want to return it to you, click Lost Mode. Lost Mode locks the device with a passcode (if you didn't already have one set) so that others can't access your personal information. It also displays a custom message on the screen, such as how to contact you. If you think it was stolen and you want to delete all the data on it, click Erase iPhone.

Wireless Connectivity

Mobile devices typically support multiple wireless connectivity types, including 4G/LTE, Bluetooth, and WiFi. You should know how to configure each of these on a mobile device.

https://t.me/learningnets

Cellular, sometimes referred to as *3G*, *4G,* or *LTE,* is wireless service from a cellular phone network, accessed via cell phone towers in your area. You get this kind of connectivity when you pay a monthly fee for phone service with a provider such as AT&T or Sprint. This type of service can include voice calls, text messages, and Internet data. The amount of data you use (in gigabytes) is metered, and if you exceed the amount specified by your plan, you are charged extra.

Bluetooth is a short-range wireless connection used for wireless peripherals like headsets and wireless speakers. Bluetooth can also be used for data transfer between two Bluetooth-enabled computing devices, such as a smartphone and laptop. There are different classes of Bluetooth devices, with different maximum ranges. Most devices are Class 2, with a range of approximately 10 meters (33 feet).

WiFi is a friendlier name for the IEEE 802.11 standard of wireless networking. This is the type of connection that most people associate with Internet connectivity, as the Internet wireless access points in most businesses and public accommodations use WiFi. Most mobile devices support WiFi, but it might not be on by default.



EXAM TIP The list of IT Fundamentals acronyms in the exam objectives says WiFi is short for "wireless fidelity." WiFi (also referred to as *Wi-Fi* with a hyphen) is a play on *hi-fi* (short for "high fidelity"*)*, a term used for stereo equipment and recordings. WiFi isn't technically short for anything. It's just a marketing name, like *Kodak.*

Near Field Communication (NFC) is a specialized, low-power, short-range wireless communication method. It is built into some Android devices. If your device has one, you can use the Android Beam app to share certain kinds of files with other nearby Android phones. It works great with photos, but it doesn't share most other types of files. More recent iPhones have NFC hardware, but they can't share files this way because it's only included to support Apple Pay (a way to pay at credit card terminals with your phone); some Windows Phone devices, however, can join in on the fun.

https://t.me/learningnets

Verifying Wireless Capabilities

To find out what wireless capabilities your device has, look in its Settings app. There will be configuration options there for each kind of wireless connectivity that the device supports. For example, in Figure 7-12, you can see that this smartphone supports WiFi, Bluetooth, and cellular.



Figure 7-12 Check a device's Settings app to see what kinds of wireless it supports.

Pairing via Bluetooth Devices

Pairing establishes a connection between two Bluetooth-enabled computing devices. Pairing can occur between two computing devices (such as tablets) or between a computing device and a peripheral (such as a smartphone and a wireless headset). Pairing with a wireless device enables a safer way to use a phone while driving, called *hands-free calling*; in some states it's the only *legal* way to use a phone while driving.

To pair devices, you must first enable Bluetooth on both devices. Many devices have Bluetooth disabled by default to extend battery life, though some peripherals may have no way to disable it. You'll find a Bluetooth setting in the Settings app. In iOS, you can also swipe up from the Home screen and tap the Bluetooth icon to toggle Bluetooth on or off.

Some Bluetooth devices are automatically discoverable by other devices whenever Bluetooth is enabled. On other devices (like laptops), you must issue a

https://t.me/learningnets

separate command to put them in Pairing (or Discovery) mode. Consult the documentation for each device to find out how to do this. (Look for Bluetooth in the Settings app on Android and iOS devices.) Figure 7-13 shows a Windows 10 laptop pairing with an iPhone.

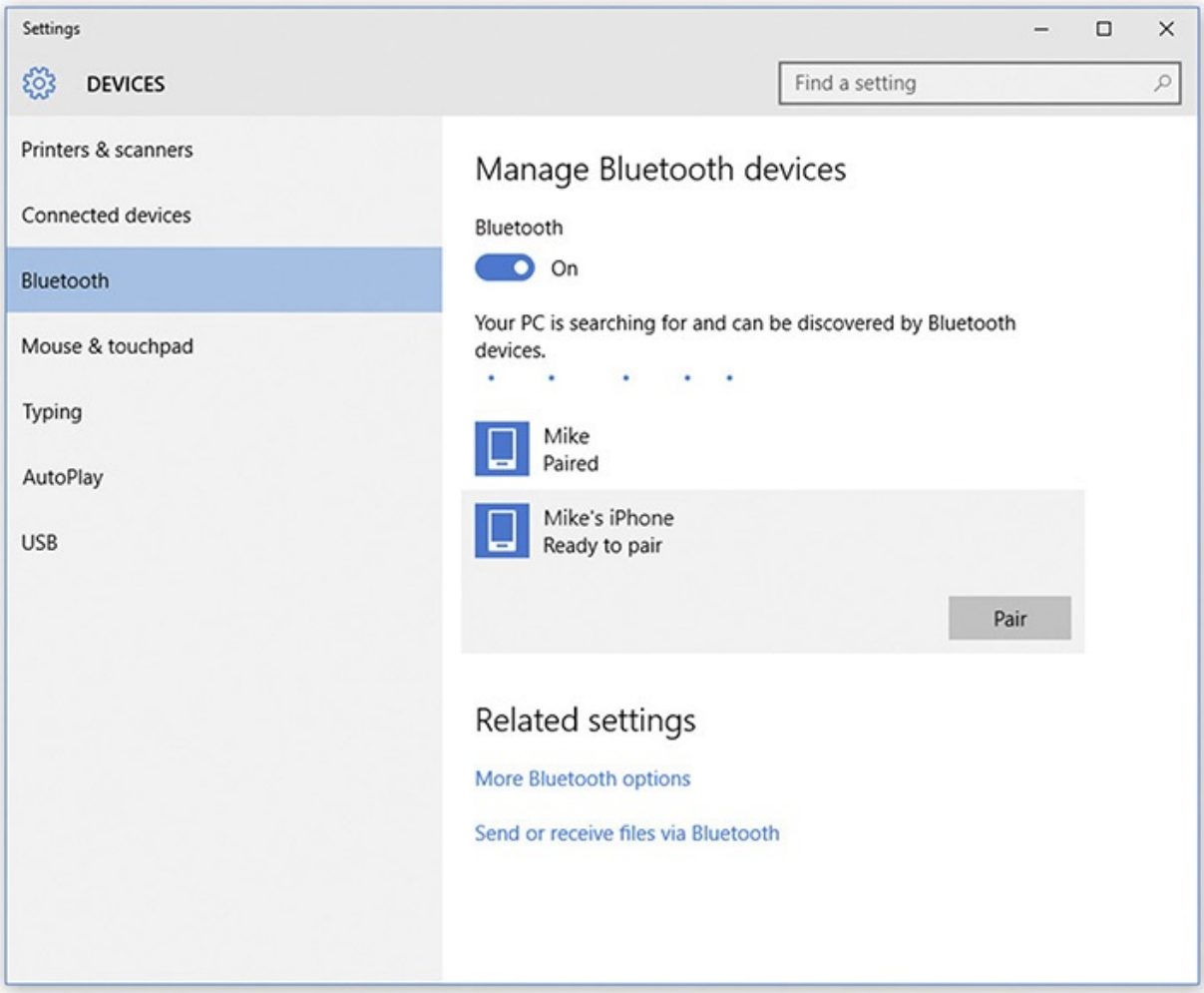


Figure 7-13 Use the Bluetooth app on your device to pair with another device.

Some devices require a security confirmation when pairing. This happens most frequently when both devices have a display screen. One device will provide an authorization code on-screen, and that same code must be confirmed on the other device. Figure 7-14 shows an authorization code in Windows 10 for the pairing initiated in Figure 7-13.

https://t.me/learningnets

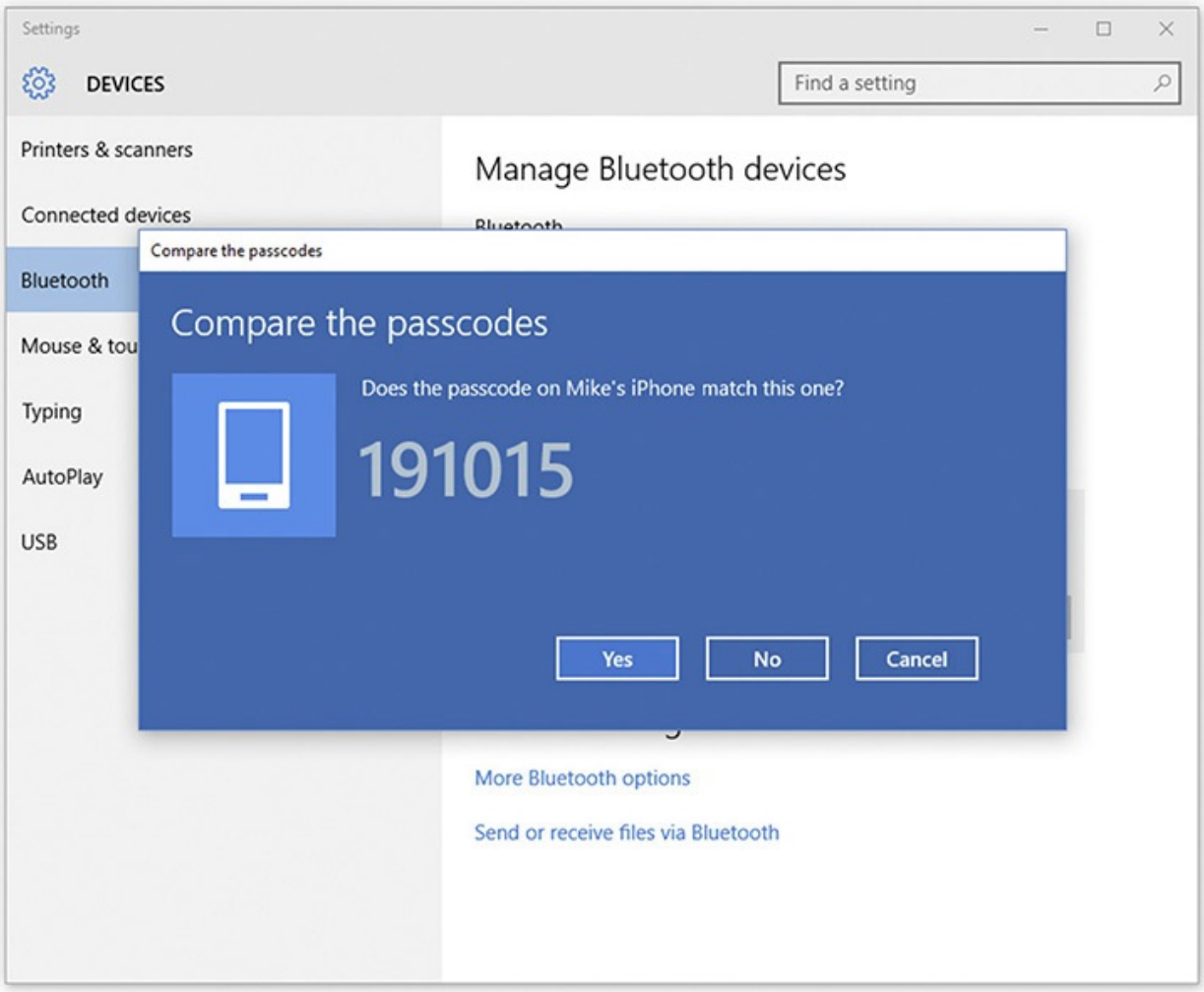


Figure 7-14 Some Bluetooth pairings require an authorization code.



NOTE Bluetooth can be finicky. For example, if a nearby device is already paired with a Bluetooth speaker, trying to pair with the speaker from a different Bluetooth device might fail. Disconnect the nearby original Bluetooth device from the speaker. You may also sometimes need to "forget" a Bluetooth connection on your mobile device and rediscover local Bluetooth devices to make a successful paired connection.

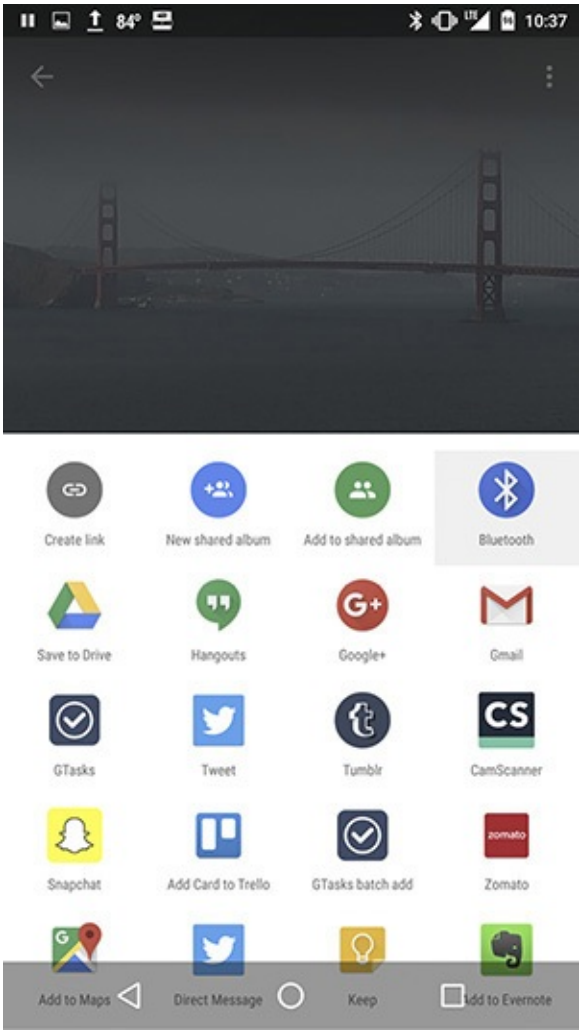
Transferring Data with Bluetooth

If you are accustomed to sharing files wirelessly between computers on a WiFi

https://t.me/learningnets

network, you might expect to be able to do the same when the two computers are connected via Bluetooth—just open File Explorer and drag and drop the files between locations, right? Unfortunately, Bluetooth file transfer doesn't work that way. Bluetooth file transfer is not true network sharing of a location; it's only the sending and receiving of individual files.

Android, Windows Phone, BlackBerry, and the Apple iOS all support Bluetooth file transfers in some way. In some cases, the capability is built into a specific app and is not OS-wide. Among the operating systems that do support Bluetooth file transfer, you must use the Share feature to share the file with another nearby Bluetooth device. In Android, for example, you would open the Gallery app, select a photo, tap Share, and then select Bluetooth (as shown in Figure 7-15). You will be prompted to set up the Bluetooth pairing between the devices if needed.



https://t.me/learningnets

Figure 7-15 Sharing a photo via Bluetooth on an Android smartphone



TIP Bluetooth isn't a great way to share lots of files. A better way is to connect your smartphone or tablet directly to a personal computer (PC) via universal serial bus (USB) cable or use an Internet file-sharing service (cloud service) like OneDrive, Google Drive, or Dropbox.

Connecting to a WiFi Network

WiFi is a type of wireless Ethernet networking, the kind of network used to share files and printers between personal computers in homes and businesses all over the world. A WiFi connection connects your device to a router, which in turn provides access to other networks (such as the Internet).

Enabling WiFi on a Mobile Device

Most mobile devices support WiFi, but many have the WiFi transmitter/receiver turned off by default to increase battery life.

To turn on WiFi, do one of the following:

- From the iOS Home screen, tap Settings and then tap WiFi. If the WiFi slider is not set to On, tap or drag it to turn it on.
- On an Android device's Home screen, tap Apps and then tap Settings. Ensure that the WiFi setting is On. If it's not, tap or drag it to turn it on.

Selecting a WiFi Access Point

Next, choose a *wireless access point* (WAP) to which to connect. Depending on where you are, there may be more than one WAP to choose from. Each one has a name, which is set by the WAP's owner, called the service set ID (SSID). The SSID might be generic, like Linksys for a Linksys-brand access point, or it might be set to the name of the business or family that owns it.

Each available wireless network within range appears on a list (see Figure 7-16) below the WiFi slider. Next to the SSID will be an icon showing how strong the wireless signal is and whether the connection is secure.

https://t.me/learningnets

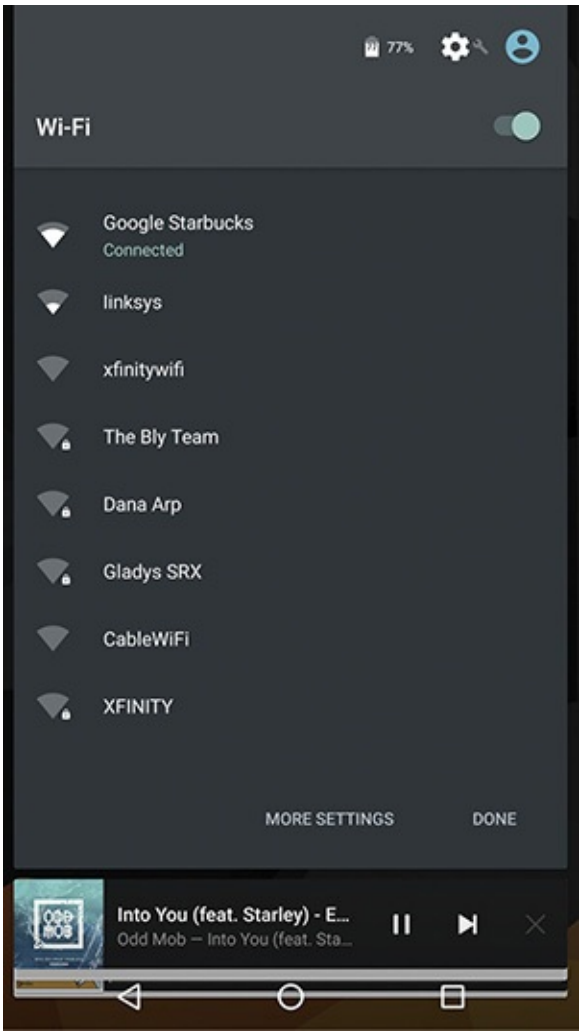


Figure 7-16 Choose from the available connections.



NOTE Chapter 10 discussed WiFi networking in further detail.

Some access points are open; you don't need a password to connect. Most are protected with some type of security and require a password (see Figure 7-17). The device remembers the password for future connections. You can tell whether an access point is protected or not by looking for a Lock icon next to it on the list of available connections. In Chapter 11 you will learn how to configure a wireless access point to use security and to set the password.

https://t.me/learningnets

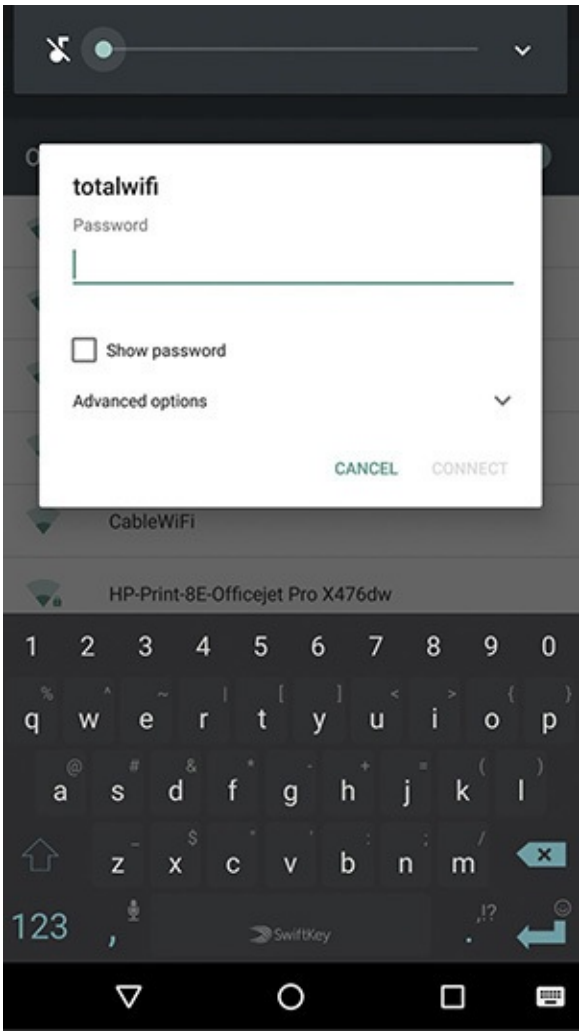


Figure 7-17 Enter the password for a secure access point.

After you establish the connection, verify Internet access by opening a web browser and trying to visit a few web sites. If you can't, either your device isn't connected correctly to the access point or the access point doesn't have Internet access.



NOTE Most wireless access points are also routers, so the terms *wireless access point* and *wireless router* are roughly synonymous in practical use.

Sharing a Phone's Cellular Connection with Other

https://t.me/learningnets

Devices

A smartphone with cellular data service and WiFi capability can turn itself into an impromptu wireless access point, allowing other nearby WiFi enabled devices to share it. Depending on the OS, this is called either *tethering* or *personal hotspot*. In iOS, this feature is called Personal Hotspot, and it's accessed from the Settings app. In Android, open the Settings app, find the Wireless Networks section, tap More and then tap Tethering & portable hotspot.

Disabling All Wireless Connections with Airplane Mode

When you fly on an airplane, you are supposed to turn off all electronic devices for takeoff and landing because some wireless signals can interfere with the plane's navigation system. If you put the device into airplane mode, however, you don't have to power it down because Airplane Mode disables all wireless capabilities.

Both Android and iOS have an Airplane Mode setting you can access from the Settings app. In iOS, you can also swipe up from the Home screen and tap the Airplane Mode icon to turn it on or off.

Configuring Mobile E-mail

You can send and receive e-mail on a mobile device via its Mail app. Setting up an e-mail account on a mobile device enables you to send and receive e-mail on the go, even when WiFi is not available. Mail can be sent and received through the cellular data service that the device itself uses. You must configure each e-mail account separately if you have more than one.



EXAM TIP Objective 2.7 of the CompTIA IT Fundamentals exam includes three *protocols* (standards) for sending and receiving e-mail: Post Office Protocol 3 (POP3), Internet Mail Access Protocol (IMAP), and Simple Mail Transfer Protocol (SMTP). The technical differences aren't important to understand, but remember that POP3 and IMAP receive e-mail and SMTP sends e-mail.

https://t.me/learningnets

You should also be aware that when you set up an e-mail account on your mobile device, the setup process will ask which type of account you have. In some cases, it might also ask for the address of the POP, IMAP, and/or SMTP server. You can get these addresses from your e-mail provider. Most have three parts separated by periods, as in pop.secureserver.net.

Setting up e-mail does not start with the Mail app, as you might expect, but with the Settings app. The steps vary somewhat between Android and iOS.

In Android, here are the steps:

1. From the Home screen, tap Settings.
2. Scroll down to the Personal section, tap Accounts & sync, and then tap Add Account.
3. Tap the type of account you want to set up. You can choose Microsoft Exchange, IMAP, or POP. If you don't know what kind of account it is and you can't easily ask someone, tap E-mail for general settings.
4. The steps diverge at this point depending on the type of account you chose. Follow the prompts, filling in the information requested to complete the process.

In iOS, here are the steps:

1. From the Home screen, tap Settings.
2. Scroll down and tap Mail, Contacts, Calendars; then under the Accounts heading, tap Add Account. A list of popular mail services appears.
3. If your service appears on the list, tap it and fill out the form that appears to connect your phone with the service. It asks for different information depending on which service. If you don't see your service on the list, tap Other and then tap Add Mail Account. Then fill out the forms that appear to follow the setup process to its completion.

After setting up your mail accounts, use the Mail app to send and receive mail. The way the Mail app works varies depending on the operating system, but they all have the same basic features.

You can return to the Settings app later to fine-tune the way the Mail program handles mail. For example, you can choose whether it organizes messages by thread, whether it asks before deleting messages, and which e-mail account it uses by default for sending new messages.

https://t.me/learningnets

Configuring Synchronization

Synchronization means updating data between two locations so that both locations contain the same files and versions. You might have photos you've taken using your mobile device's camera, for example, and synchronizing your mobile device with your laptop PC might copy those photos to the laptop. There are several ways to keep data synchronized, depending both on the mobile OS and on the type of data being synced.

Synchronizing with a Cloud Service

You can employ a cloud service to synchronize data between devices automatically. The advantage of this method is that it's "set it and forget it." You configure automatic synchronization, and then it just happens going forward.

For Android, you can synchronize with your Google account to keep your contacts, system settings, apps, calendar, and e-mail data coordinated. For Apple, you use iCloud, an Apple-provided cloud service.

In Android, open the Settings app and tap Privacy. Check the boxes for Back up my settings and Automatic restore. Choose your Google account for the Backup account.

In iOS, open the Settings app, select iCloud, and enter your Apple ID and password. This signs you into iCloud on that device and enables synchronization across all your Apple devices that use iCloud. (That's mainly Apple devices, but there are also iCloud apps you can install in other operating systems, like Windows.)

Synchronizing Photos

In Android, Google's Instant Upload service handles photo synchronization. When that feature is enabled, any photo or video you take is uploaded to Google+ in a private album called From the Phone. You can enable or disable Instant Upload via the Settings app.

In iOS, there is a separate cloud app for photos called iCloud Photo Stream. To configure it, open the Settings app, choose iCloud, choose Photos (or Photos & Camera), and then turn My Photo Stream on or off. When it is on, new photos you take are uploaded to iCloud when your device is connected to the Internet using WiFi.

https://t.me/learningnets

Synchronizing with a Computer

When you connect your mobile device to a computer via a USB cable, you can synchronize all data and settings between the two devices. This includes music and video, which is essential if you use your mobile device as a mobile player.

For iOS devices, the iTunes app provides computer syncing capabilities. Download and install iTunes if needed (from Apple.com) and then connect your iOS device to the computer using a USB cable. Right-click the device's icon in the navigation bar in iTunes and choose Sync. See Figure 7-18.

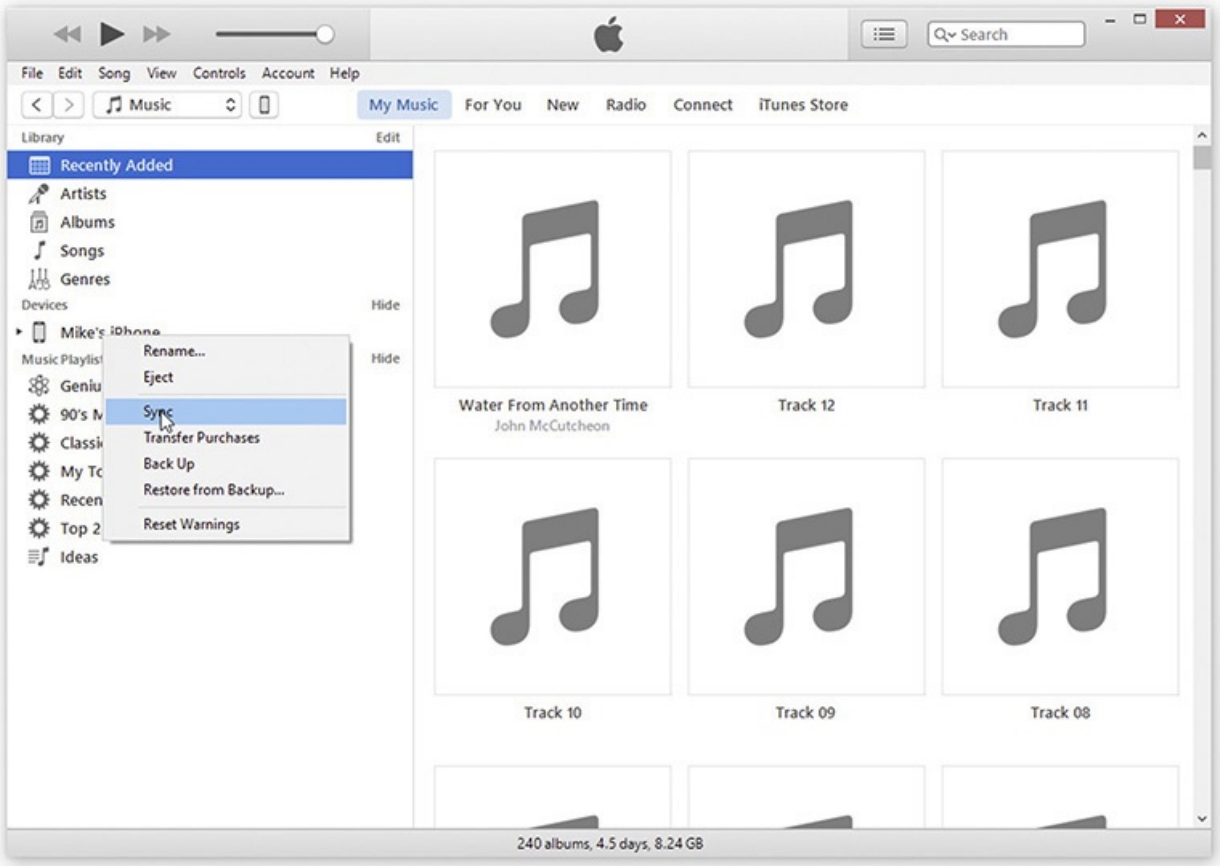


Figure 7-18 In iTunes, right-click the device and choose Sync.

For Android, you'll need to work with a third-party app to synchronize music and videos. One of the most popular is called doubleTwist. You might even have it installed already; some phone services like T-Mobile make it available on the Android phones they sell.

If you are syncing with a Windows 10 PC, you can also use the Phone

https://t.me/learningnets

Companion app that comes preinstalled with Windows. (That goes for both Android and iOS devices.)

Installing and Removing Apps

Installing an app is probably one of the more important skills to have when using any mobile device. Apps allow you to extend your device's capabilities, adding everything from scientific calculators to mindless games.

Finding and Installing an App

The same app may be available for both Android and iOS, but they are not interchangeable. You get Android apps from the Google Play Store or other third-party app stores. You get iOS apps from the Apple Store (Figure 7-19). Each of those stores is an app on your device. To download a new app, you open the store app and make your selection.

https://t.me/learningnets

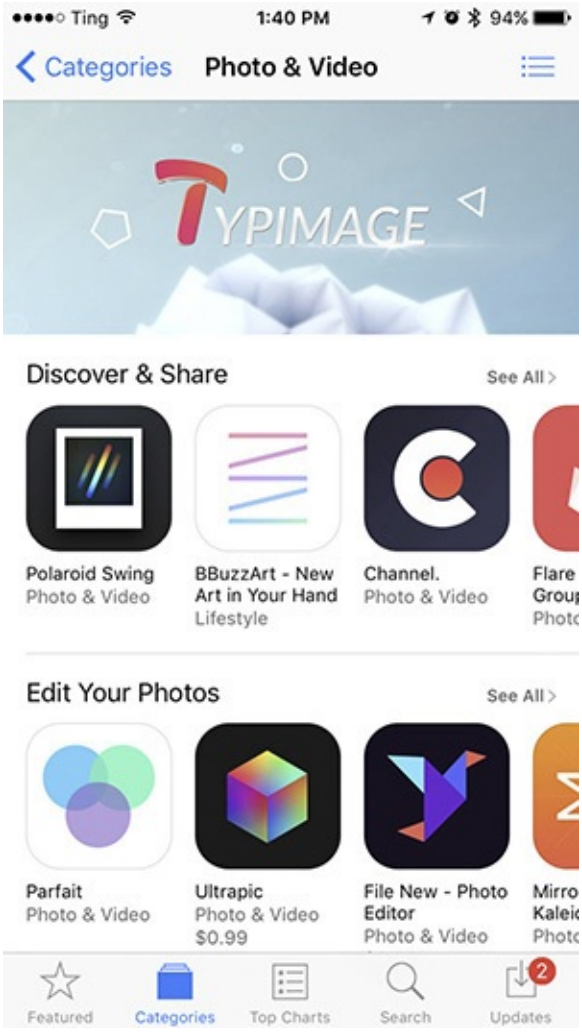


Figure 7-19 The Apple Store



TIP When installing an app, you should connect your device to WiFi if possible so you don't use your cellular plan's data (unless, of course, you are on an unlimited data plan). An app download can use tens or hundreds of megabytes.

Some apps cost money (usually less than $10), but many are free. Free apps are more likely to have advertisements in them or have limited features to entice you to pay for a premium version. When you shop for apps, pay attention to the costs.

https://t.me/learningnets

If you pay money for an app, the store will automatically charge whatever credit card you have on file for your Google or Apple account. The first time you open the store app, you may be prompted to sign in with your Google or Apple account and to set up a payment method.

In Android, to open the Play Store, tap the Apps icon at the bottom of the Home screen and then swipe left and right to locate the Play Store app and tap it. Once you get into the store, tap Search (magnifying glass) and type the name of the app you're looking for or a keyword.

In iOS, tap the App Store icon on the Home screen to open the Apple Store. In the store, tap Search at the bottom of the screen and type a name or keyword.

Once you find an app that looks interesting, follow the prompts to get it. The app will download and install on your device, and you'll find its icon on the Home screen.

Removing an App

So that app you downloaded didn't turn out to be so great? Dump it! It's easy to remove (uninstall) an app in a mobile OS.

In Android, open the Settings app, and then tap Apps, Applications, or Application Manager (depending on version). Select the Downloaded (or Downloads) tab to see only the apps you have downloaded. Find and tap the app you want to delete, and tap the Uninstall button.

On iOS, it's even easier. On the Home screen, press and hold the app you want to get rid of. When the icons start shaking, tap the *X* in the upper-left corner of the app's icon. A confirmation appears, as in Figure 7-20. Tap Delete. Then press the Home button again to stop the other icons from shaking and return to normal use.

https://t.me/learningnets

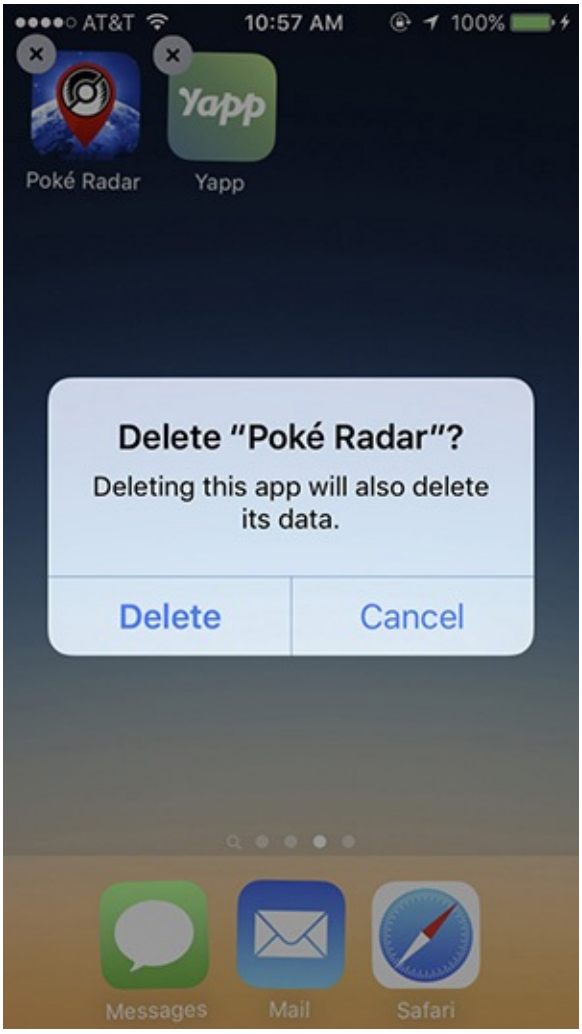


Figure 7-20 In iOS, hold your finger on an app icon and then tap the *X* in its corner to uninstall it.

Resetting a Mobile Device

You might need to reset a mobile device to troubleshoot or make the device fresh for a new owner. *Reset* means two very different things, called soft and hard.

A *soft reset* is basically just a reboot. Sometimes when a device locks up or starts acting all squirrelly, a soft reset will do the trick. A *hard reset* wipes out everything on the device and takes it back to its original factory settings. Avoid *hard resets* if at all possible because you'll lose time setting the device up again and any data, files, and preferences you don't have backed up elsewhere. The only time you should prefer a hard reset is when you give or sell your phone to someone else.

https://t.me/learningnets

Performing a Soft Reset

To perform a soft reset in Android, press and hold the Power button until a message appears offering to turn the device off. Select Power off or select Restart. See Figure 7-21. If the device is locked up, though, that method won't work. With a locked-up device, you need to do a *force restart*. One way is to take the battery out for a few seconds if it's removable. If it's not, try holding down the Power button and the Volume button at the same time until the screen goes black. Then hold down the Power button until the device restarts.

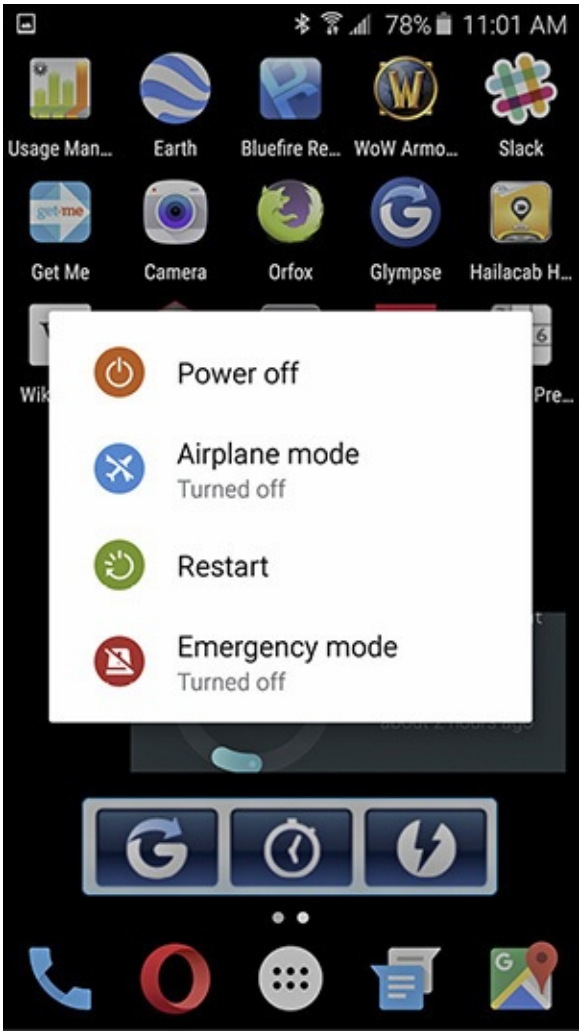


Figure 7-21 Powering off an Android phone

On an iOS device, if it will respond at all, press and hold the Sleep/Wake button until the red slider appears. Then drag the slider to turn the device completely off. After the device turns off, press and hold Sleep/Wake until you

https://t.me/learningnets

see the Apple logo. If the device is locked up, press and hold both the Sleep/Wake and Home buttons until you see the Apple logo (ten seconds or longer).

Performing a Hard Reset

Now you'll learn to reset the device the hard, ugly way—the way you have to do when you are out of other options.

On an Android device, you will want to access the Factory data reset screen. The tricky part is that different phone brands and models access this screen differently. Look up the exact steps for your model online. On one phone, for example, with it powered off, hold down Volume Down and Power together. When you see the brand logo, release the Power button only and then immediately press it again; then release both buttons when the Factory reset data screen appears. If that sounds as awkward as a game of Twister, it is. It's difficult on purpose so you don't do it accidentally.

On an iOS device, you need a computer with iTunes installed. Connect the device to the computer and open iTunes. Then press and hold Sleep/Wake and Home at the same time, but *don't* release the buttons when you see the Apple logo. Keep holding them until you see the Recovery Mode screen. A message appears in iTunes that there's a problem with the phone that requires it to be updated or restored. Click Update and wait for iTunes to fix the device.

Getting Your Data Back After a Hard Reset

If you're lucky enough to have backed up or synced the phone's settings before the disaster occurred, you can restore them as follows.

On an Android device, after a hard reset, you are prompted to walk through a setup process. As part of it, you're prompted to sign in to Google. When you do so with the same Gmail account you used for syncing, your data is automatically restored to the device.

On an iOS device, when the device comes back up after a hard reset, the Setup Assistant runs. Go to Set up your device, tap Restore from a Backup, and sign in to iCloud. Tap Choose backup and then select the backup you want to use and follow the prompts.

Chapter Review

In this chapter, you learned how to set up and navigate a smartphone or tablet

https://t.me/learningnets

interface. While Android is the most popular mobile OS, iOS is a strong second-place contender. You learned about gestures for interacting with a touchscreen, such as tap, swipe, pinch, and rotate, and you learned how kinetic sensors such as gyroscopes, magnetometers, and accelerometers help a mobile device orient itself spatially.

You learned the importance of basic security measures like assigning a lock passcode on a device; to access this and most other settings, use the Settings icon on the main screen. You learned what to do if your device is lost or stolen and how to reset a malfunctioning device.

We reviewed wireless technologies in mobile devices, including Bluetooth, WiFi, and NFC, and you learned how to pair a Bluetooth device to a phone or tablet and how to establish and configure a WiFi connection and set up e-mail. You also learned how to configure synchronization with a cloud service and how to install and remove apps.

Questions

1. What is the gesture where you touch the surface with two fingers spread apart and then drag them closer together?
   - **A.** Rotate
   - **B.** Tap
   - **C.** Pinch
   - **D.** Spread
2. Which of these terms is *not* associated with kinetics?
   - **A.** Magnetometer
   - **B.** Gyroscope
   - **C.** Barometer
   - **D.** Accelerometer
3. How is screen orientation determined, if it is not locked?
   - **A.** The user sets it once, and it never changes.
   - **B.** Orientation hardware button.
   - **C.** Orientation command.
   - **D.** Physical orientation of the device.
4. Which of these passcodes is more secure?

https://t.me/learningnets

A. Six-digit alphanumeric.

B. Six-digit number.

C. Four-digit number.

D. All are equally secure.

5. 3G, 4G, and LTE are all kinds of what kind of wireless communication?

A. WiFi

B. Bluetooth

C. Cellular

D. NFC

6. What kind of wireless connectivity is Bluetooth best suited for?

A. Sending and receiving phone calls

B. Connecting to a wireless headset

C. Connecting to the Internet

D. Connecting to a computer in a nearby building

7. Connecting a Bluetooth peripheral to a smartphone is known as:

A. Pairing

B. WiFi

C. 4G

D. NFC

8. The name of a WiFi access point is its:

A. POP

B. IMAP

C. NFC

D. SSID

9. Which of these is *not* a protocol for sending or receiving e-mail?

A. IMAP

B. SMTP

C. POP3

D. NFC

10. What app does an iPhone use to synchronize music and videos from a computer?

https://t.me/learningnets

A. iMusic

B. iTunes

C. Google Play

D. doubleTwist

Answers

1. **C**. Dragging fingers closer together is called *pinching*.
2. **C**. A barometer is not a kinetics term; all the others are.
3. **D**. When screen orientation is not locked, the physical orientation of the device determines the screen orientation.
4. **A**. An alphanumeric passcode is most difficult to guess and therefore most secure.
5. **C**. 3G, 4G, and LTE are types of cellular communication.
6. **B**. Bluetooth works well for pairing a wireless headset. It would not work for any of the other activities listed.
7. **A**. Connecting a Bluetooth peripheral to a device is called *pairing*.
8. **D**. An access point's name is its service set ID (SSID).
9. **D**. Near Field Communications (NFC) is not an e-mail protocol; the others are.
10. **B**. The iTunes app is used to synchronize music and videos with an iOS device.

https://t.me/learningnets

CHAPTER 8

Managing Files

In this chapter, you will learn how to

- Manage file storage
- Manipulate files and folders
- Protect files

The operating system (OS) enables you to store, organize, and retrieve data files—working with files is one of its primary functions. Your primary hard drive contains a ton of files, files that make up the OS, the apps, and the data. You can replace the OS and apps pretty easily, but the data needs protection. This chapter looks at organizing, manipulating, and backing up data.



NOTE Unless specifically noted otherwise, *hard drive* in this and other chapters includes both magnetic hard disk drives and flash-based solid-state drives.

Managing File Storage

Operating systems organize hard drives into volumes that can span one or more physical disks. A disk volume could also comprise only a portion of a physical disk; in other words, you can carve up a disk into multiple volumes if the disk is large enough. Most users in Windows at least have a C:\ drive as their primary volume, whereas Linux users would refer to the file system root using a slash (/).

Understanding Folders and Paths

Each volume can store files, commonly organized into *folders* (also called *directories*). For example, Windows computers have a Windows folder for the

https://t.me/learningnets

OS files, a Users folder to hold user profile information and data, and a Program Files folder to hold installed applications. Any folder can have many layers of subfolders nested inside it.

A *path* or *file path* describes the location of a particular file on a volume. It starts with the drive letter and then lists each folder and subfolder and ends with the filename. Each folder name is preceded by a backslash (\) in a path. Here's a Windows OS example, where C:\Users\Mike\Documents\Projects\ is the path and Invoice.xlsx is the filename:

```
C:\Users\Mike\Documents\Projects\Invoice.xlsx
```

The same path in Linux would look something like /users/mike/documents/projects/invoice.xls. It doesn't have to be lowercase in Linux; it could be any case. Also, notice the absence of a drive letter; that's because Linux doesn't use drive letters.

Organizations tend to establish file and folder naming standards to make file management easier. For example, files related to a cost center with a code of "ABC123" might use this text as a filename prefix. OSs also enforce filenaming rules. In Windows 10, for instance, path and filenames are not case-sensitive like they are in Linux, but generally the path and filename together cannot exceed 260 characters. We say "generally" because with specific OS editions new features are made available, such as increasing the maximum path and filename length.

In Windows, the address bar in File Explorer shows file paths with arrows rather than slashes, like this:

```
C: > Users > Mike > Documents > Projects > Invoice.xlsx
```

In a graphical file management interface like File Explorer in Windows or Finder in macOS, folders are represented by icons that look like paper folders. When you display the contents of a folder, subfolders also appear as folder icons.



EXAM TIP Make sure you understand the hierarchical way folders are nested on a volume and how to navigate between levels to find files.

At the top of the file hierarchy is the *root directory* of the volume—that is, the

https://t.me/learningnets

top level, not inside any other folder. Under the root directory are folders, along with any files stored in the root directory. (A few system files may be stored there, depending on the OS.) In a path, the root directory appears as a backslash all by itself (no folder name), as in C:\.



CAUTION Avoid storing data files in the root directory of your system volume (your main hard drive). If you get into the habit of manipulating files in that location (for example, renaming them or deleting them), it becomes all too easy to accidentally delete an important system file.

Because folder structures can be complex, involving multiple layers of nesting, it is sometimes easier to look at a folder structure as a tree. In Windows File Explorer, you can see a graphical view of the tree structure in the Navigation pane (the left pane). Figure 8-1 shows this tree structure.

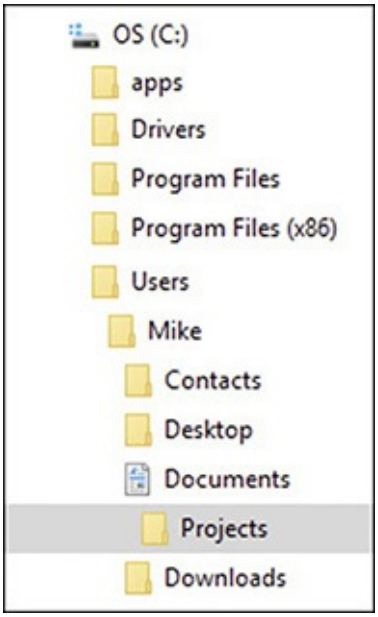


Figure 8-1 A graphical tree helps visualize the folder structure in some file management utilities.

File Management Tools

In Windows 8 and later, File Explorer handles the file management chores.

https://t.me/learningnets

Earlier versions of Windows came with a similar tool called Windows Explorer. Look for the following features of File Explorer in Figure 8-2:

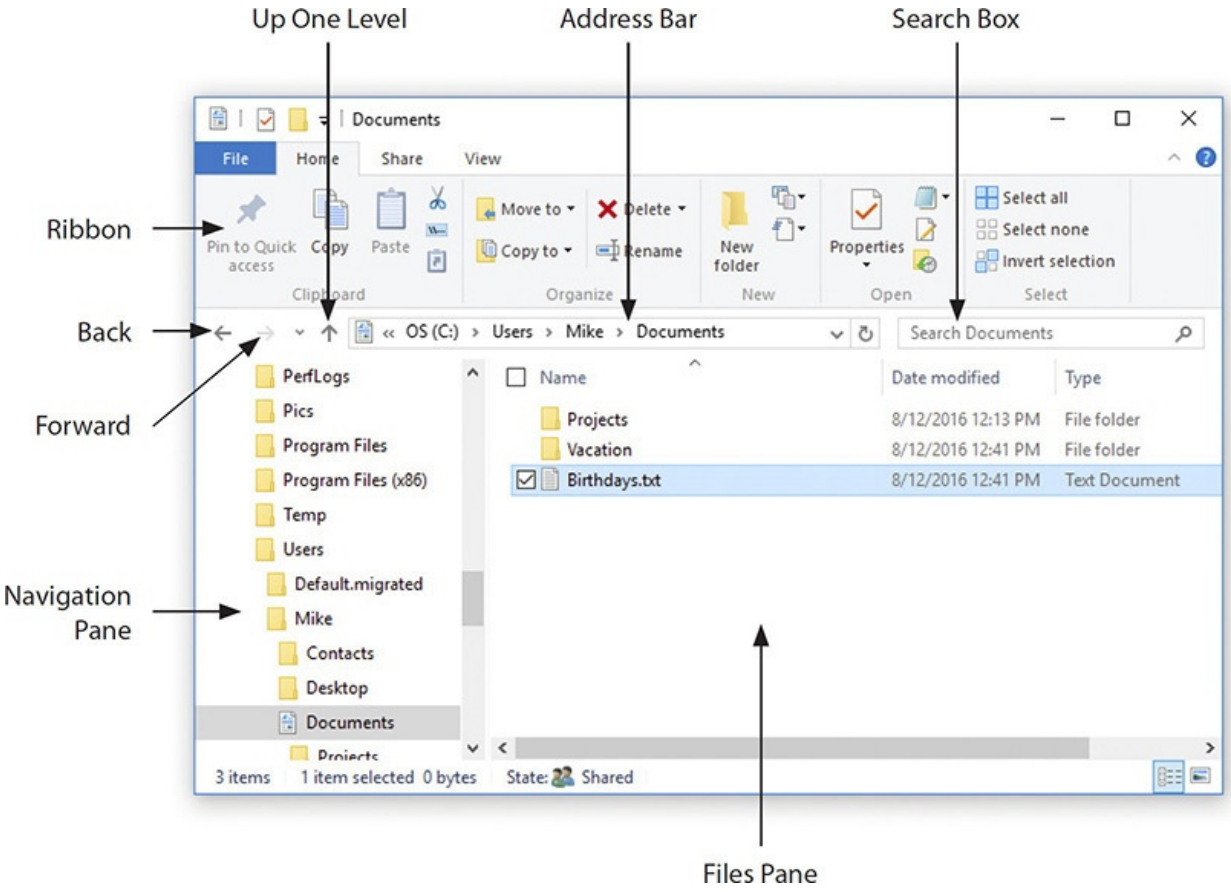


Figure 8-2 File Explorer in Windows 10

- **Address bar** This shows the current location's path.
- **Navigation pane** This shows the folder tree and shortcuts to common locations.
- **Files pane** This lists icons for files and folders in the current location.



TIP Drag the divider between panes to adjust their relative sizes.

- **Ribbon** This multitabbed toolbar provides commands you can issue.
- **Back and Forward buttons** Click the Back button to return to the

https://t.me/learningnets

previously displayed location. This activates the Forward button, which you can click to get to the next location.

- **Up One Level** Click here to move up one level in the folder hierarchy (that is, one step closer to the root directory).
- **Search box** Click here and type a keyword to search for a file or folder.

In macOS, the Finder utility manages files. It has many of the same features as File Explorer. A toolbar across the top provides buttons for changing the view, adjusting settings, sharing files, and changing file properties. A Navigation pane at the left provides shortcuts to some locations, and a Search box enables you to search for a specific file or folder. Back and Forward arrow buttons are present as well.

Finder doesn't have an expandable folder tree (like the one in Figure 8-1) in its navigation pane, but you can see an expandable tree (shown in Figure 8-3) if you choose the List view (from the View buttons at the top of the window).

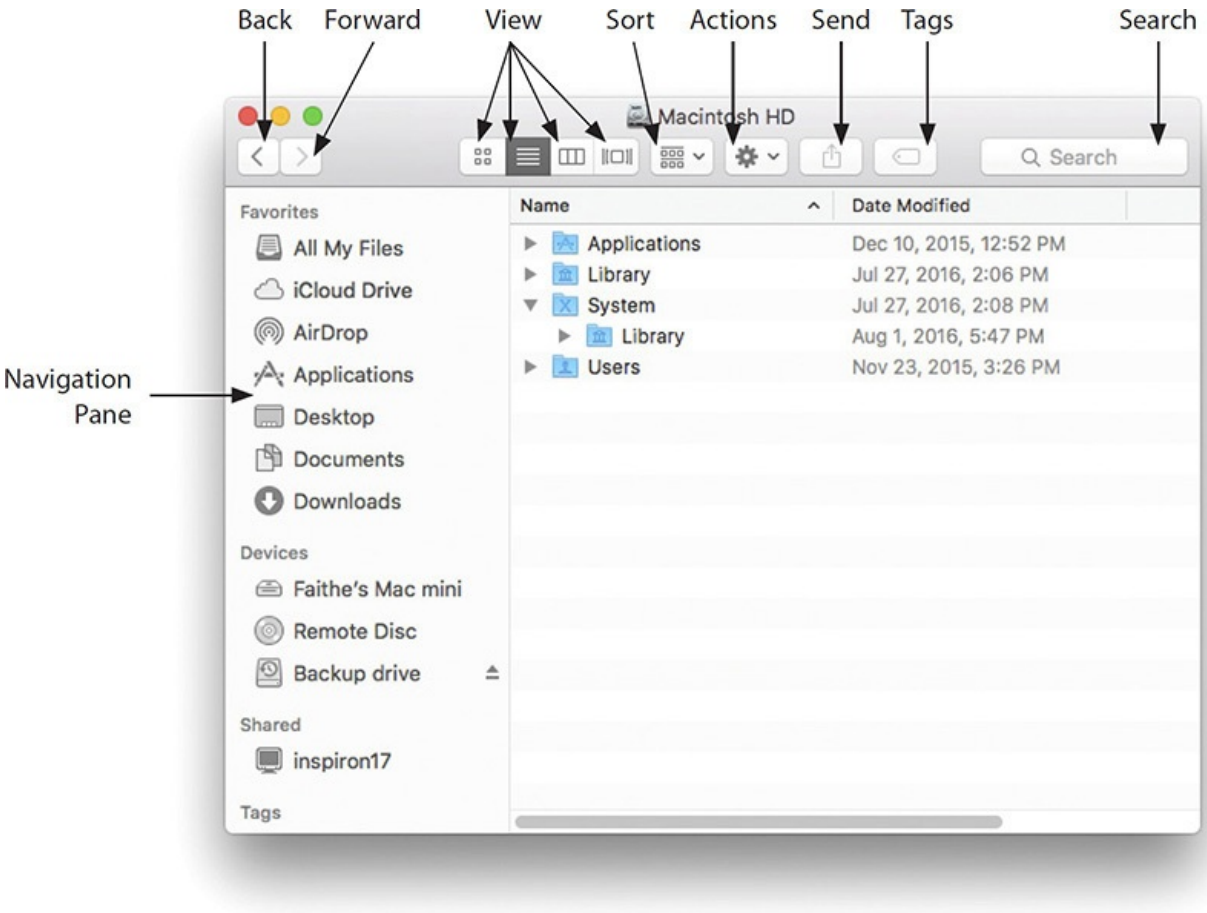


Figure 8-3 The Finder utility in macOS provides a graphical user interface

https://t.me/learningnets

(GUI) file management interface.

The Files utility in the Linux Unity GUI has a navigation pane without an expandable folder tree. It also indicates the current location in the path bar (though you can't click into it to manually edit the path without jumping through a few hoops). Figure 8-4 shows the Files utility's interface.

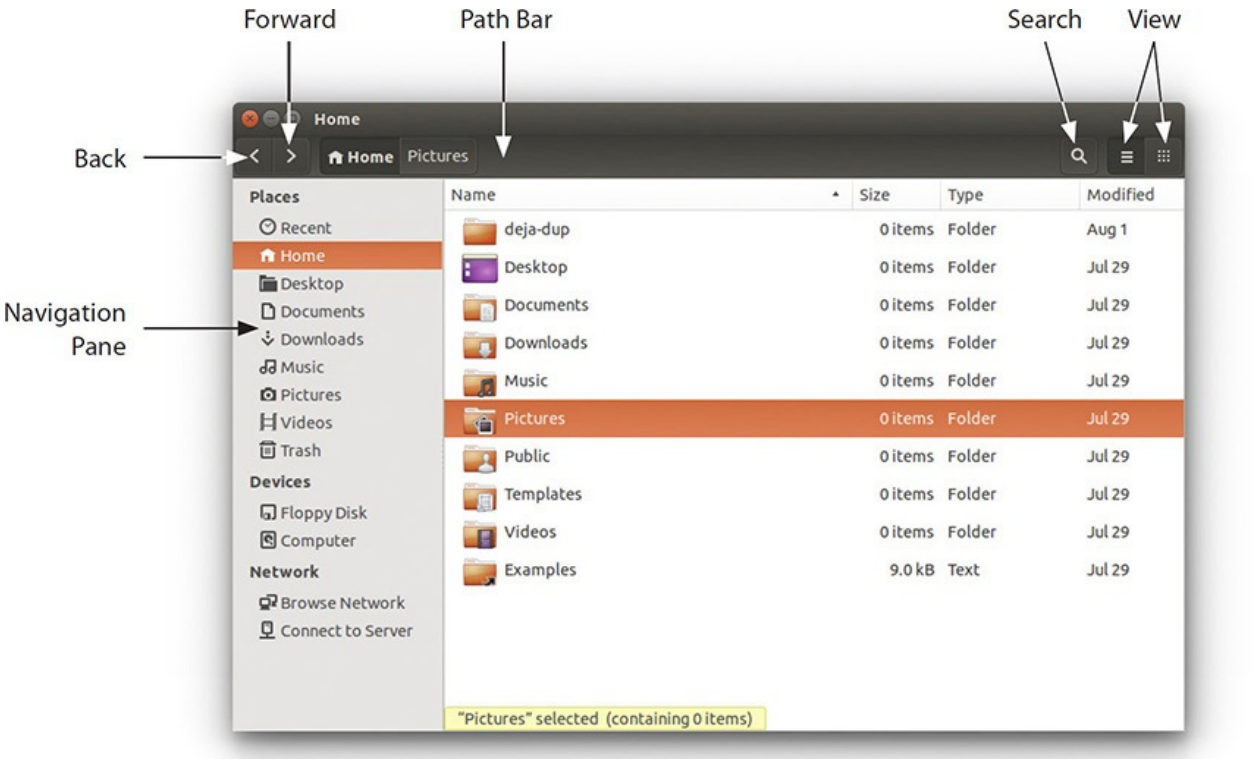


Figure 8-4 The Files utility in Unity provides a simple file management interface.

Any of these file management utilities can perform the actions you'll learn about in the "Manipulating Files and Folders" section later in this chapter, but the steps may differ slightly. The rest of this chapter focuses on the more common Windows interface.



EXAM TIP As you prepare for the CompTIA IT Fundamentals exam, you

https://t.me/learningnets

might want to explore the macOS and Linux file management utilities on your own. See whether you can perform the actions in this chapter on each OS.

Navigating a File Structure

You can navigate between locations in a file management utility in many ways. The easiest way is to click the location's shortcut in the Navigation pane. In Figure 8-2, for example, you can jump from the Mike\Documents folder to the Temp folder by clicking Temp in the Navigation pane.



EXAM TIP Navigating a file structure means moving between file storage locations—from folder to folder and from volume to volume. If someone provides you with a path, you should be able to open that location in a file management utility.

At the top of the Navigation pane in File Explorer is a Quick access section, shown in Figure 8-5. Shortcuts appear here for recently used locations, as well as some common locations such as Documents, Pictures, and Desktop. You can also drag your favorite folders and files from the Files pane into the Navigation pane's Quick access section to "pin" them there. You can modify the look and feel of File Explorer to suit your needs. Figure 8-5 shows File Explorer with the banks and Books folder shortcuts added. Locations without a pushpin icon, by the way, appear temporarily because they have been used recently and may scroll off over time.

https://t.me/learningnets

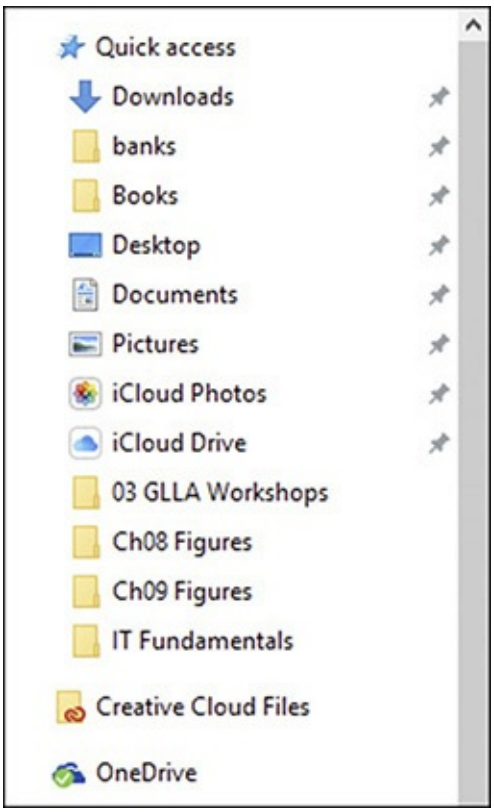


Figure 8-5 The Quick access list in the Navigation pane is a customizable place for shortcuts to folders you use frequently.

If the Navigation pane doesn't contain a shortcut to the desired location, you can browse for the location by starting at the top level of the volume and drilling down. In Windows 10, click This PC (called Computer in earlier Windows versions) in the Navigation pane to see a list of the local volumes in the Devices and Drives section of the Files pane. Double-click the desired volume, then double-click the desired folder, and keep double-clicking until you arrive at your destination.

You can also navigate to a folder by clicking its name in the path in the Address bar. Clicking the arrow between two folder names in the Address bar opens a menu of subfolders in the folder left of the arrow (see Figure 8-6); click a folder on that menu to jump to it.

https://t.me/learningnets

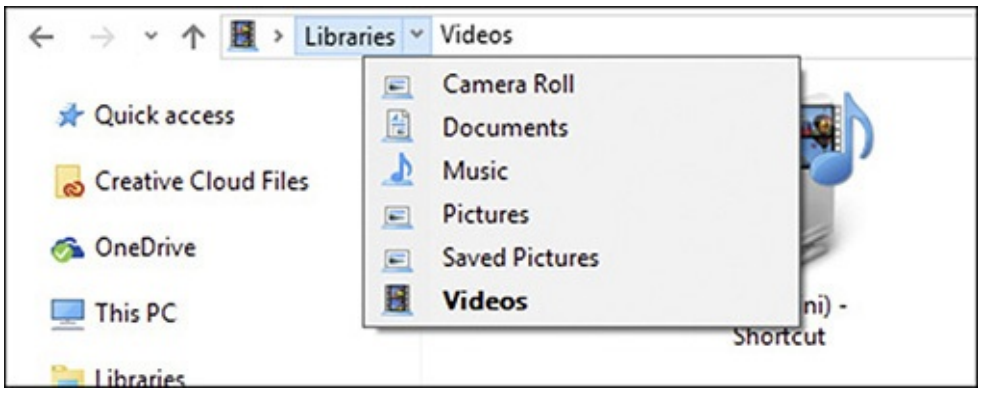


Figure 8-6 Subfolder menu in the Address bar



EXAM TIP Shortcuts, explained in Chapter 5, are pointers that refer to a file. They can appear not only on the desktop and Start menu but also in the file list for any folder.

File and Folder Properties

Each file and folder has a number of properties that describe it, such as its size, its type, and its creation date. A file's properties are sometimes referred to as its *metadata*, which literally means "data about the data." Let's look at attributes, file size, keywords, and program association.

Basic File Attributes

Attributes (sometimes called *flags*) are yes/no values for a file. There are four basic file attributes: read-only, system, hidden, and archive.

- **Read-only** *Read-only* marks a file as unchangeable. You can read the file, but if you modify the file, you need to save it under a different name. Read-only protects the original file from change.
- **System** A file marked *system* is hidden by default and protected from accidental deletion.
- **Hidden** A *hidden* file acts like its name would suggest, hiding from the default view in File Explorer.
- **Archive** A file with the *archive* attribute active indicates the file has

https://t.me/learningnets

changed since the last system backup. When a backup utility backs up a file, it turns this attribute off. When the file changes, the OS turns the attribute on, so the backup program will know that it needs to be backed up again next time it runs.

Advanced File Attributes

Most hard drives in Windows systems use a file system called *New Technology File System* (NTFS), Apple's *Hierarchical File System* (HFS) and its successor HFS+ are used for the macOS, and many Linux systems use the *Extended Filesystem version 4* (EXT4) file system. NTFS offers additional advanced attributes, such as indexing, compression, and encryption. FAT32 is an older Windows file system type that does not offer advanced attributes as NTFS does.

Indexed Windows (and some applications) can search file contents for something the user wants to find, but this can take a long time (especially on slow or large drives). Allowing a file's content to be indexed makes those searches go faster.

Other OSs such as Linux can use built-in commands such as *find*, which is for unindexed searching, or *locate*, which searches an indexed file system database.

Journaling Windows, Linux, and the macOS support a variety of journaled file systems. Journaling uses a transaction log for write activity to the file system. When the OS receives a notification to write something to disk, the OS opens a new journal transaction about what must be written *before* the data is actually written to disk.

In the event of disk corruption due to power outages, misbehaving software, and so on, the transaction journal can replay those entries that did not complete, which results in little to no data loss.

Compressed NTFS enables file compression so files take up less space on the volume. This compression is invisible to the user; the only thing you might notice is that the file takes slightly longer to open and to save. Compression can be enabled for individual files, though it is more often enabled for entire folders and thus affecting all files they contain.

The macOS can use HFS compression to maximize storage efficiency. The Linux *chattr* (change attribute) command is one method of encrypting files. There are plenty of OS and third-party compression tools out there for all OSs, including mobile device compression apps available through app stores.

https://t.me/learningnets

Encrypted In some Windows editions, NTFS supports file encryption through a feature called Encrypting File System (EFS). This encryption is invisible to the file's owner. When another user on the same local computer tries to access the file or folder, however, its access is protected by the encryption.



NOTE If encryption isn't available on your PC, you probably don't have a Windows edition that supports it. Encryption is available only on professional editions such as Windows 7 Professional, Enterprise, or Ultimate; Windows 8.1 Pro; or Windows 10 Pro.

Folder Attributes

Many file attributes can also be applied to folders. An attribute applied to a folder applies to all files within that folder, so assigning attributes at the folder level is a great time-saver.

File Size and Other Noneditable Properties

Some file properties simply describe the file. You can change them only by modifying the file. These include the file's size, when it was created, when it was last modified or accessed, and so on.

Some OSs have maximum file system and individual file size limitations. As an example, the maximum size of an NTFS volume is 16 exabytes (EB), but you won't find disks that large; this number is theoretic and based on mathematics, even if combining multiple large disks for a single volume.

An exabyte equals approximately 1,024 petabytes (PB). To give you an idea of how much space we're talking about, according to https://www.zmescience.com/science/how-big-data-can-get/#Exabyte, 5 EB is enough space to contain the text of all words ever spoken by human beings!

Keywords

Certain kinds of data files can have details assigned to them. Details can include tags (keywords), a subject, the authors' names, categories, and comments.

Viewing and Modifying Properties

To view (and optionally modify) properties via a file's Properties dialog box, right-click the file's name in File Explorer and choose Properties.

https://t.me/learningnets

On the General tab, shown in Figure 8-7, you can see many of the noneditable properties, such as the size and creation date/time. You can also mark or clear the Read-only and Hidden attribute check boxes.

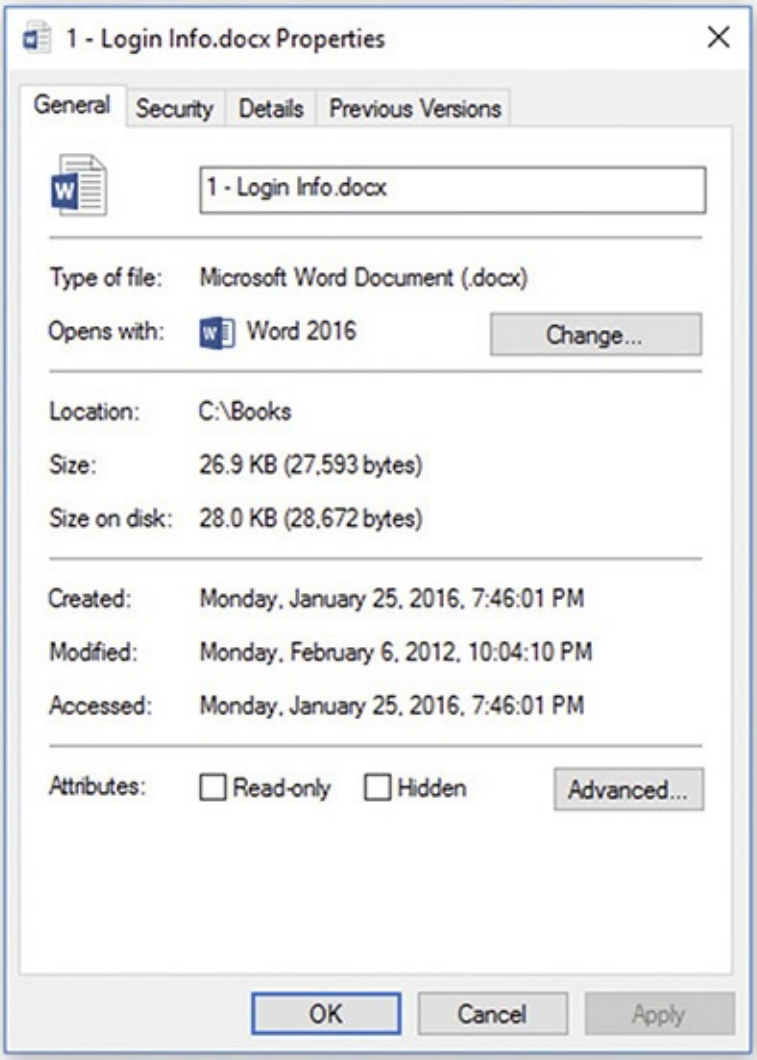


Figure 8-7 View a file's properties from its Properties dialog box.

To access other attributes, click the Advanced button to open the Advanced Attributes dialog box (shown in Figure 8-8). Here you can toggle the attributes that control whether the file is archived, indexed, compressed, and encrypted.

https://t.me/learningnets

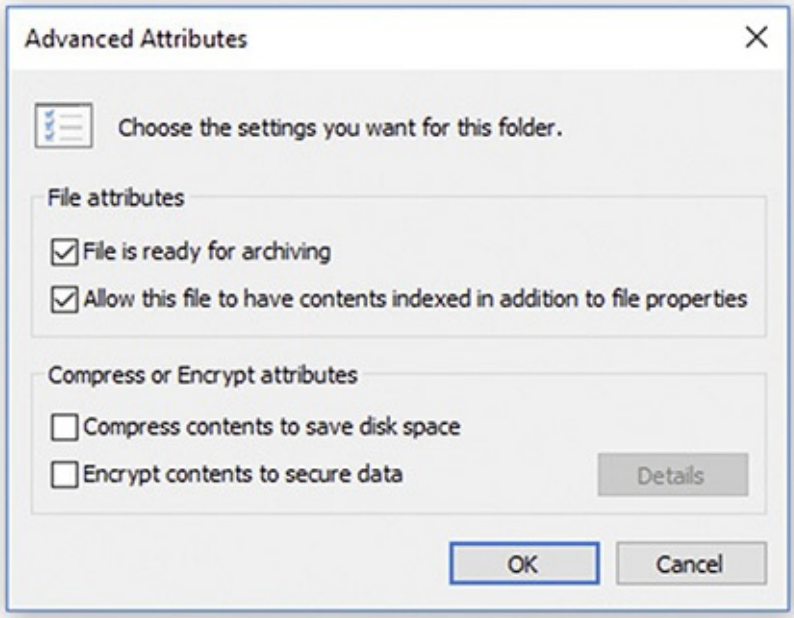


Figure 8-8 Use the Advanced Attributes dialog box to turn other attributes on/off.

To access other properties such as the title, subject, and tags, click the Details tab, shown in Figure 8-9. Click next to an item in the Description area to edit it. You can't edit the properties in the Origin section.

https://t.me/learningnets

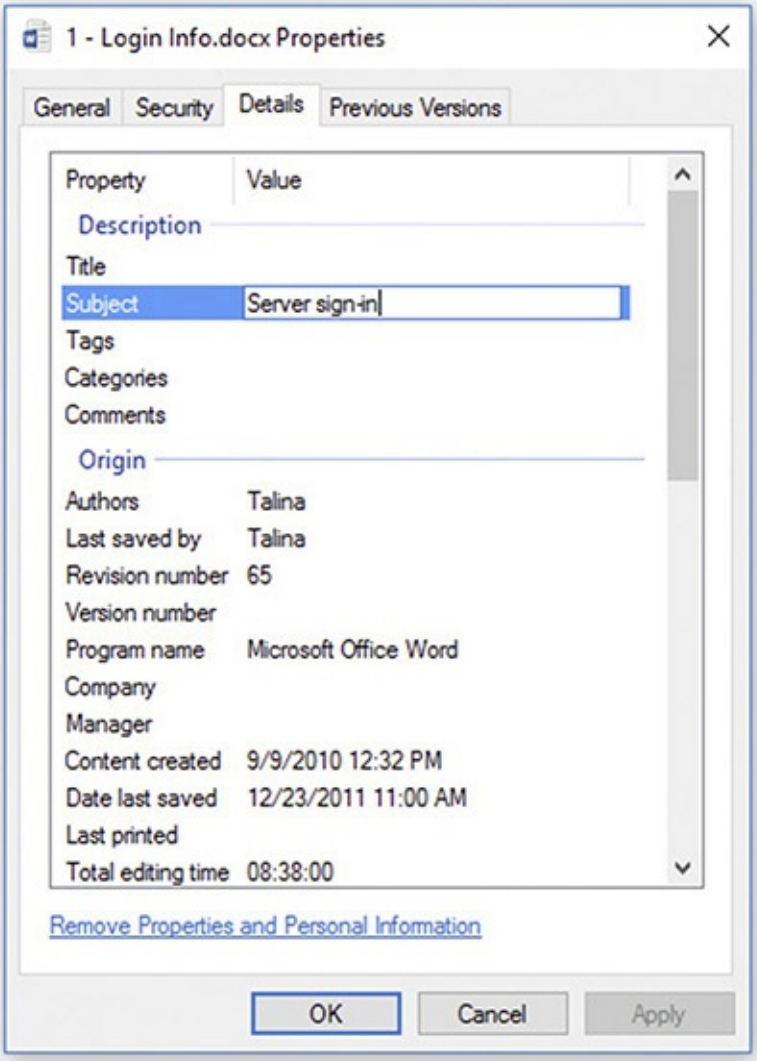


Figure 8-9 Set other properties on the Details tab.

File and Folder Size

As you saw in Figure 8-7, a file's size describes how much space it occupies on the volume. A folder technically has no size of its own; it is just a container. In practice, though, a folder's size is shown as the sum of the size of every file it holds. To see a folder's size, open its Properties box and look on the General tab. You'll also see a summary of what the folder contains. In Figure 8-10, for example, the folder contains 1,536 files and 560 subfolders.

https://t.me/learningnets

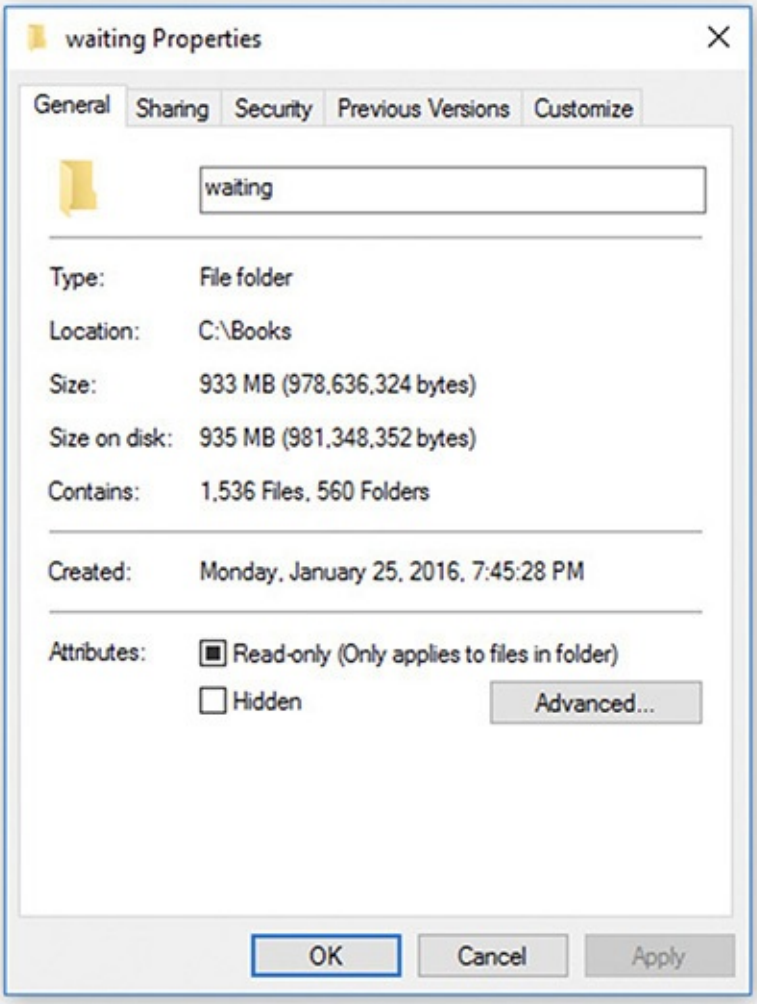


Figure 8-10 Viewing a folder's information

Manipulating Files and Folders

You will likely need to take some actions on the data files you create in various applications. For example, you might need to edit, rename, copy, move, or even delete a file. The following sections summarize how to perform the most common file manipulations in Windows.

Opening, Editing, and Saving Files

There are several ways to open a data file. Here are some of the easiest:

- **Open an application** that can work with data files of that type and then

https://t.me/learningnets

use the Open command in the application to select and open the desired file.

- **Double-click the data file** in File Explorer to open the file (in the default application).
- **Double-click a shortcut** to the data file. For example, you might have created a shortcut on the Windows desktop to a file that you use frequently.



TIP To create a shortcut on the desktop for a data file, right-drag the data file out of File Explorer and onto the desktop. (In other words, drag it using the right mouse button, rather than the left one.) When you release the mouse button, a menu appears. Select Create shortcuts here.

How does Windows know which application to open the data file in when you double-click a data file? It all depends on the file extension. A file's extension lets the OS know what kind of file it is. A .txt file is a text file, for example, and a .bmp file is a graphic file. Each data file extension has a default application assigned to it. This is called its *association*. When you double-click a data file, Windows opens it with the default application listed in its internal table of file associations.

If the application supports editing the file, you can make and save changes to it in the application. Microsoft Word can edit the text—for example, change the formatting or insert new content such as a graphic. If you don't know how to make a certain kind of edit, use the application's Help system to find out. Pressing the F1 key will open the Help system in most applications.

To save a file, use the Save command in the application. See the section "Saving Your Work" in Chapter 9 for details.

Moving and Copying Files and Folders

Moving and copying are similar activities, so we cover them as a pair. When you move a file, you remove it from one location and put it in another location. When you copy a file, you *don't* remove it from the first location; you just place a copy of it somewhere else.

To move or copy files (and folders) between locations, you have three

https://t.me/learningnets

methods to choose from: drag-and-drop, the Clipboard (cut/copy/paste), and the Move and Copy commands in File Explorer.

Selecting Multiple Files and Folders

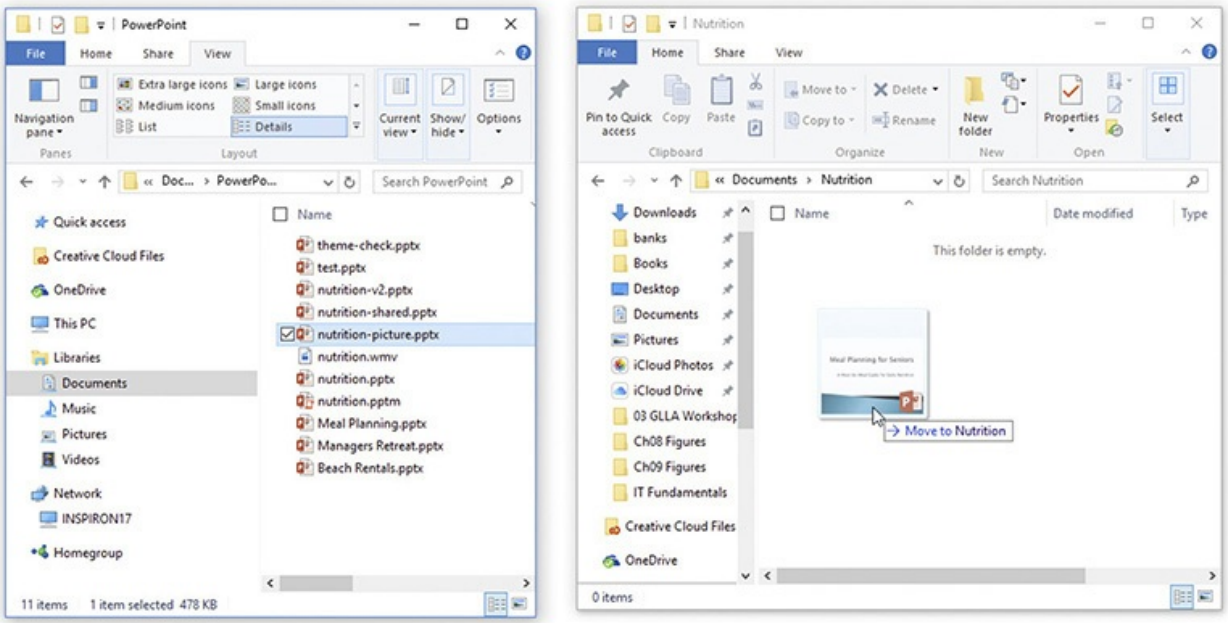
You will eventually want to move or copy multiple files and folders at a time. To select multiple files and folders, use these techniques:

- To select multiple *contiguous* items (located next to each other), click the first one, hold down SHIFT, and click the last one. All the items between the two files are selected. Alternatively, drag with the mouse to draw a selection box around the files you want to include.
- To select multiple *noncontiguous* items (not located next to each other), click the first one, hold down CTRL, and click each additional item that you want.

Drag-and-Drop

As the name implies, drag-and-drop means selecting the files and/or folders and then using the mouse to move them or copy them somewhere else.

You can open two separate File Explorer windows, navigate to a different location in each, and then drag between them. As you drag, a thumbnail of the file appears on the mouse pointer, along with a label that tells whether it will move (as in Figure 8-11) or copy them.



https://t.me/learningnets

Figure 8-11 Use drag-and-drop to move or copy.



TIP To open a second File Explorer window when one is already open, right-click the File Explorer window's button on the taskbar and choose File Explorer. You can also just drag and drop files onto one of the location shortcuts in the Navigation pane without opening another File Explorer.

How do you specify that you want a move versus a copy? It's a bit tricky. When you drag and drop between locations on the *same* volume, Windows moves the files by default. If you want to copy instead, hold down the CTRL key as you drag. When you drag and drop between locations in *different* volumes, Windows copies by default; if you want to move instead, hold down the SHIFT key. If you aren't sure whether the locations are on the same volume, you can still hold down CTRL to copy or SHIFT to move. You can also just right-drag, in which case a menu pops up when you release the mouse button asking what you want to do.



TIP Holding down ALT as you drag creates a shortcut.

Cut-and-Paste

The Cut, Copy, and Paste commands use the Clipboard, which is a temporary holding area in memory. When you select a file (or a group of files or folders) and issue the Cut command, the selected items are removed from their current location and placed on the Clipboard. If you issue the Copy command, in contrast, a copy is placed on the Clipboard, and the original stays in place.



EXAM TIP Make sure you understand the relationship between the Clipboard

https://t.me/learningnets

and the Cut, Copy, and Paste commands.

The Clipboard can hold the contents of only one Cut or Copy operation at a time. (A Cut or Copy operation can be performed on a multifile/multifolder selection, though, so it's not like you have to move or copy files individually.) When you choose Cut or Copy again, whatever was previously on the Clipboard is replaced with the new content.



NOTE If you use the Clipboard feature in Microsoft Office applications, an enhanced Clipboard is available that can hold up to 24 selections at once.

File Explorer supports two methods of accessing Clipboard commands.

- **Shortcut keys** CTRL-C for copy, CTRL-X to cut, CTRL-V to paste.
- **Shortcut menu** Right-click the selection and click Cut, Copy, or Paste. Figure 8-12 shows the shortcut menu for a group of selected files. The Paste command doesn't appear in Figure 8-12 because there is currently nothing to paste. (Nothing has yet been cut or copied.)

https://t.me/learningnets

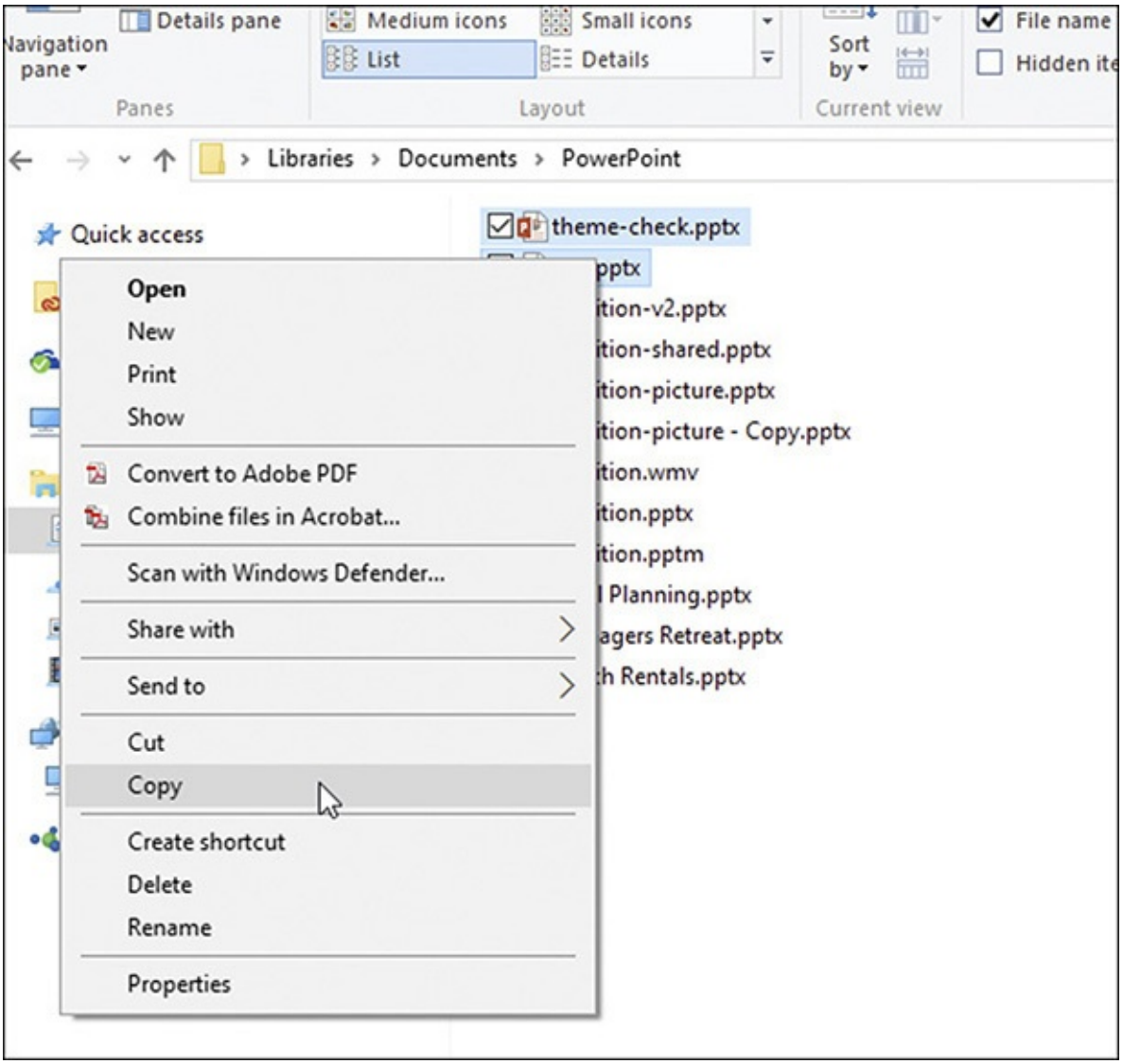


Figure 8-12 Right-click for the shortcut menu and then choose Cut, Copy, or Paste.

Move to and Copy to Commands

Here's one more method for moving and copying. In File Explorer, the Home tab of the Ribbon contains Move to and Copy to buttons. Select the desired items and then click one of these buttons; a menu of recently accessed locations will appear. Select a location from the menu to complete the operation. If you don't see the location you want, click Choose Location from the bottom of the menu.

Renaming Files and Folders

https://t.me/learningnets

To rename a file or folder in File Explorer (you can't rename more than one at a time), use one of these methods:

- Right-click the item, click Rename, type the new name, and press ENTER.
- Select the item, press F2, type the new name, and press ENTER.
- Click the item and then click it again to move the insertion point into the name. Edit the name and press ENTER.
- Select the item, click Rename on the Home tab of the Ribbon, type a new name, and press ENTER.



CAUTION File extensions are not displayed for known file types by default in File Explorer. You can toggle their display on/off from the View tab, with the File name extensions check box. When file extensions are displayed, you can change a file's extension when you rename it. Be careful: Windows relies on the file extension to know what kind of file it is and which app should open it.

Deleting and Undeleting Files and Folders

Deleting unneeded files and folders keeps your file system orderly and frees up disk space. However, deleting a file or folder doesn't automatically remove it from your hard drive. By default, the Delete command sends the files or folders to a special folder called Recycle Bin. You can restore deleted items from the Recycle Bin to correct any deletion mistakes.



TIP The Recycle Bin works only for local hard drives; it doesn't retain deleted files from network shares, USB flash drives, or optical discs.

To delete files or folders (and send them to the Recycle Bin, if available for the volume you are working with), select them and then do one of the following:

- Press the DELETE key.

https://t.me/learningnets

- Right-click the selection and choose Delete.
- On the Home tab on the Ribbon, click Delete, or click the down arrow on the Delete button and click Recycle Bin.

To delete files or folders permanently (without sending them to the Recycle Bin), do one of the following:

- Press SHIFT-DELETE.
- On the Home tab, click the down arrow on the Delete button and click Permanently delete.

To undelete, open the Recycle Bin by double-clicking its icon on the desktop. All the deleted content appears there. Figure 8-13 shows some deleted content in the Recycle Bin. Select an item; then on the Manage tab, click Restore the Selected Items. You can also right-click an item and choose Restore.

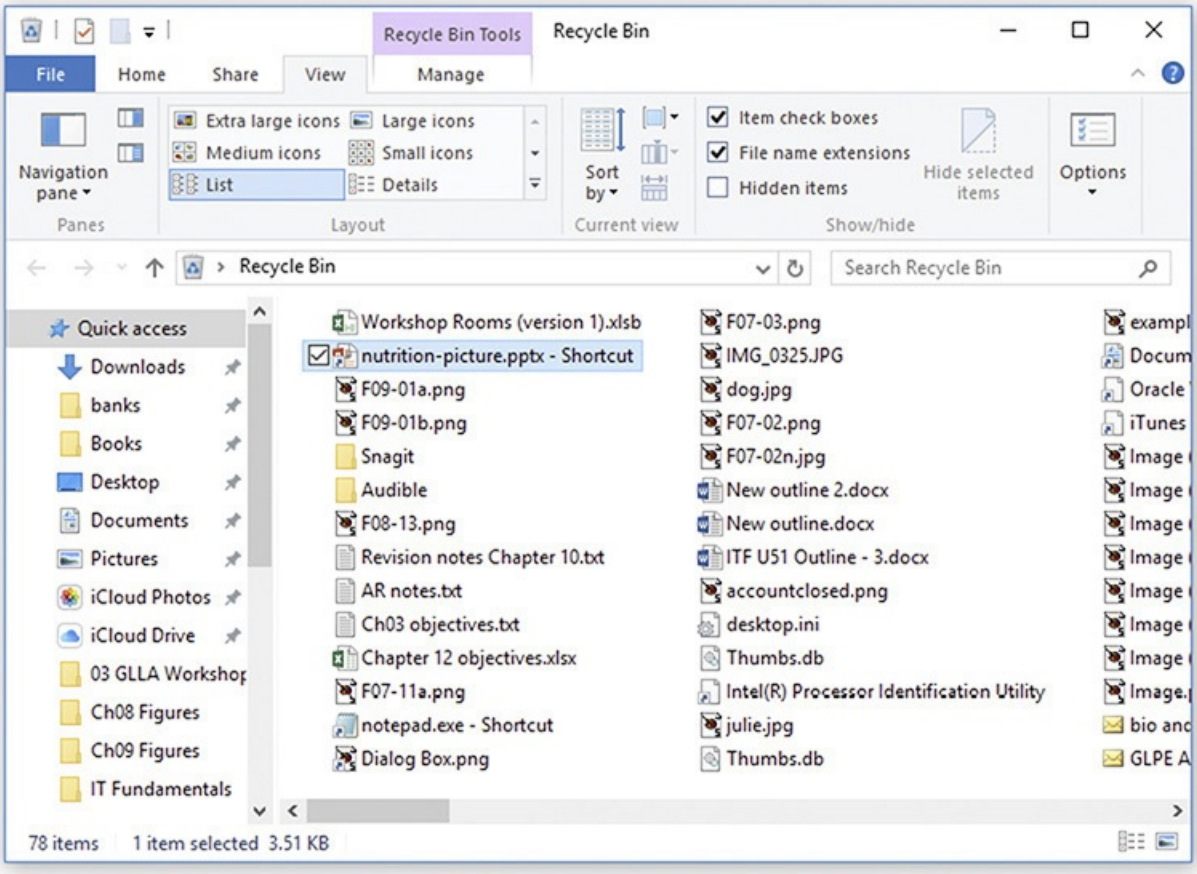


Figure 8-13 You can restore deleted files from the Recycle Bin.

https://t.me/learningnets

To permanently delete an item, delete it from the Recycle Bin. (Select it and press the DELETE key.) To empty the entire Recycle Bin at once, click Manage | Empty Recycle Bin.



TIP To empty the Recycle Bin without opening the Recycle Bin window, right-click the Recycle Bin icon on the desktop and choose Empty Recycle Bin.

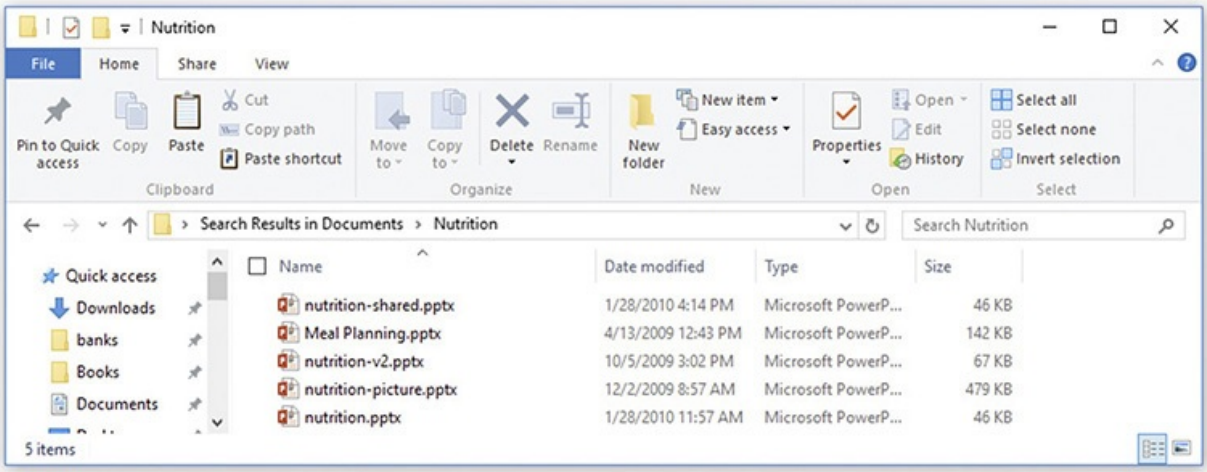
Searching, Sorting, and Displaying Files

As you accumulate files on your computer, it's easy to forget where you stored a certain file or what you named it. There are several ways of displaying file listings that can make it easier to find what you need, such as searching, sorting, and changing the display view.

Searching for Specific Files

For a quick search, use the Search box in the upper-right corner of the File Explorer window. Just type what you know about the file, either the name or the content, and press ENTER. Results appear in the Files pane.

For a more advanced search, click the magnifying glass icon in the Search pane to open the Search tab in the Ribbon, as shown in Figure 8-14. Then use the options that appear to refine the search criteria as desired. You can limit the search to a certain file type, for example, or to a size or date modified.



https://t.me/learningnets

Figure 8-14 Use the Search tab on the Ribbon in File Explorer to specify search criteria.

Changing the View

On the View tab in File Explorer you can select a view from the Layout group, shown in Figure 8-15. Different views work for different situations.

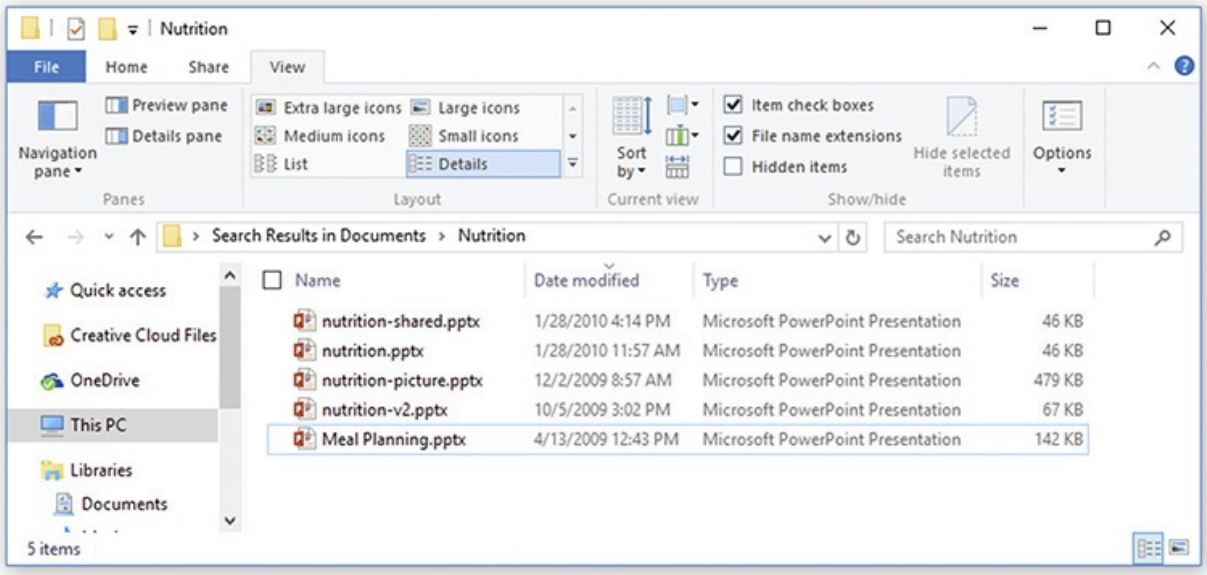


Figure 8-15 Details view

- The Small icons and List views show files in a compact way that helps when working with many files at once.
- The Details view (see Figure 8-15) shows multiple columns of data about the files, such as Size, Type, and Date Modified, making it ideal for browsing files by size, date, name, and so on.
- The Extra large icons, Large icons, and Medium icons views show a preview of the file if possible, which is great for finding images and documents by look instead of name (see Figure 8-16).

https://t.me/learningnets

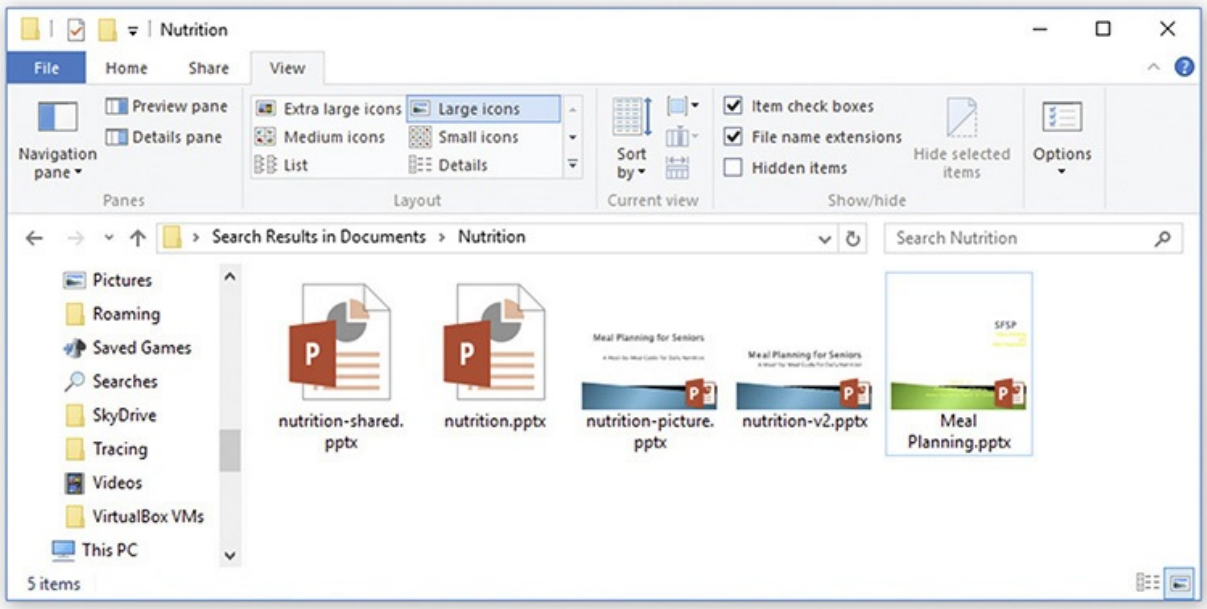


Figure 8-16 Large icons view

Also on the View tab are additional controls that affect the way you see the file listing, including these:

- **Navigation pane** Clicking this button opens a menu containing three options:
  - **Expand to open folder** Expands the folder tree to show the path to the folder displayed in the Files pane
  - **Show all folders** Shows additional shortcuts in the Navigation pane for locations such as the Control Panel, Recycle Bin, and folders on the desktop
  - **Show libraries** Shows shortcuts to the Libraries folders in the Navigation pane



NOTE Libraries, introduced in Windows 7, are virtual locations that combine the contents from multiple locations in a single window, as if all the files and folders were in one location. This way, you can use many folders on more than one volume to organize your pictures, videos, or music but still have a single place to browse all your pictures at once.

https://t.me/learningnets

- **Preview pane** This button toggles the Preview pane on/off to the right of the Files pane. This pane shows a preview of the selected file if the file is a supported data file.
- **Details pane** This button toggles the Details pane on/off. This pane shows information about the selected file. You can't have the Preview and Details panes open at the same time.

Sorting a File Listing

A file listing can be sorted in either ascending or descending order by Name, Type, Date Modified, or Size. Only one sort can be in effect at a time.

One easy way to sort a listing is to right-click an empty area of the Files pane, click Sort, and then click the desired sort type. Right-click again and choose Ascending or Descending if needed. See Figure 8-17.

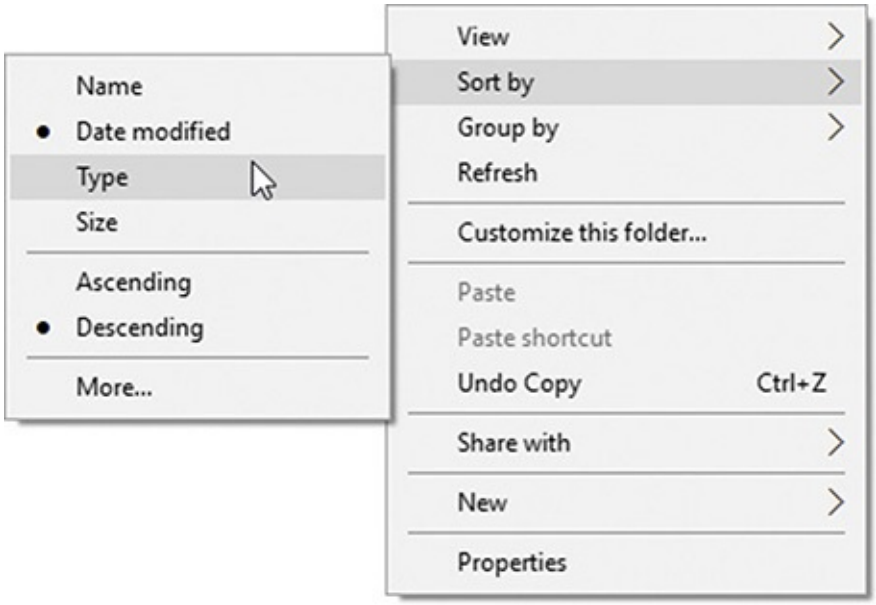


Figure 8-17 You can sort using the right-click menu.

In Details view, you can click a column heading to sort by that column. Click the same column again to switch between ascending and descending order.

You can also change sorting from the View tab (shown in Figures 8-15 and 8-16), in the Current View group. Click the Sort by button and choose the desired sort property. There are more properties available to sort by on this menu than on the right-click menu.

https://t.me/learningnets

Protecting Files

In this final section of the chapter, we'll look at some ways you can protect your files from snooping by other people who use your computer and how you can back up your files as an insurance policy against hard drive failures.

File and Folder Permissions

Your files are your own private business…until someone else who uses your computer starts snooping around. Protect your privacy by setting restrictions on who may view or edit certain folders on the local hard drives. These are called *local permissions*. The word *local* differentiates these permissions from *sharing*, which occurs across networks.

On a computer that multiple people share, you can set up a separate user account for each person. You can then restrict access to certain folders to only certain users (or only you). You can set permissions for individual files, but it is better to set permissions at the folder level. That way everything in the folder has the specified permissions, and you can set permissions for other files just by moving them into that folder.

To set a folder's permissions, right-click the folder in File Explorer, choose Properties, and then click the Security tab. On the Security tab, you can view permissions for specific users or groups of users. Some groups are built-in so that when you assign permissions to that group, everyone in that group also has those permissions. The Administrators group, for example, includes all user accounts with Administrator permissions. (The default is Standard permissions.)

To make a change, click the Edit button on the Security tab, opening the Permissions dialog box (see Figure 8-18). From here you can add users to the Group or user names list, and you can set Allow or Deny permissions for each file management activity for each group or user. Figure 8-18 shows that user Mike can view the selected folder but can't modify it.

https://t.me/learningnets

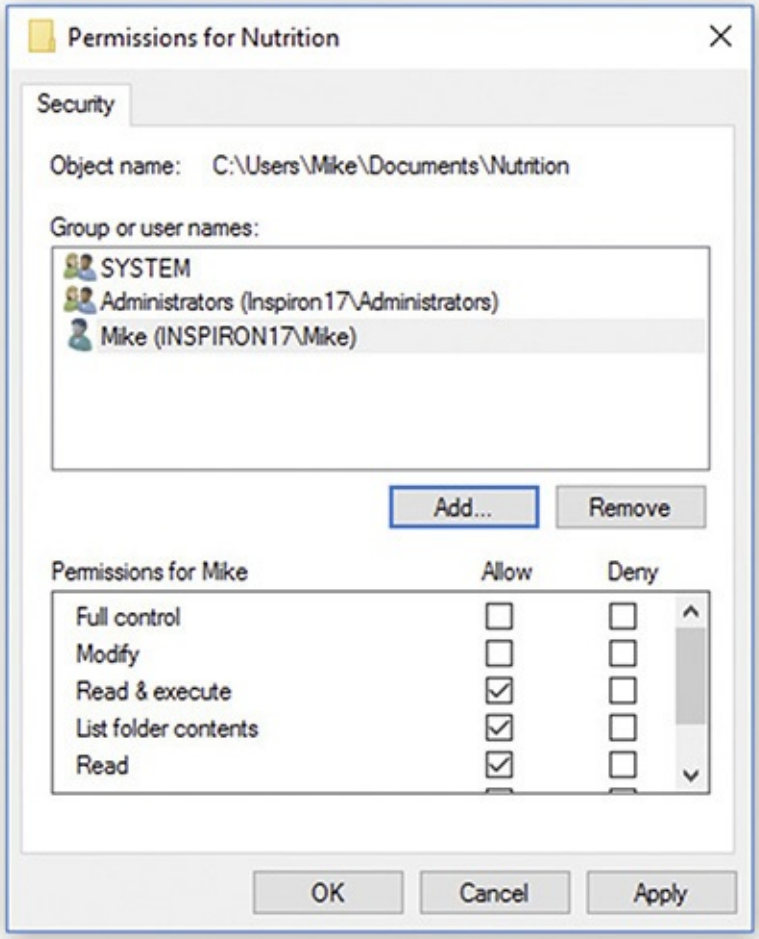


Figure 8-18 Modify folder permissions to control who can access the folder locally.



CAUTION Avoid using the Deny permission option. Yes, it works, but it's all too easy to create tough-to-troubleshoot problems if you start mixing Allow and Deny permissions for different groups. If a user is a member of multiple groups and one group is allowed and one group is denied, the effective permissions can become a confusing mess. A lack of Allow stops access, so just stick to allowing or not allowing.

Backing Up and Restoring Data

https://t.me/learningnets

On most computers, the stored data is more valuable than the computer itself. Let's say your hard drive dies and you suddenly lose access to everything it contains. Or, perhaps a child in your household decides to delete everything in your Documents folder to clear out space for the new game he wants to install. How bad would that be? Catastrophic? Panic-inducing just to think about? That's why backups are so important.

Backups can be performed automatically via a backup utility or manually by copying files to an external drive using the Copy command in File Explorer. Both methods have their advantages. Bear in mind that replacing OS and application files is easy even without backups, but the same is not true for data files.

Backup Software vs. Manually Copying Files

Most businesses have an automated backup system that backs up files from individual computers daily, usually in the middle of the night when network traffic is low. As a result, the average employee doesn't have to think about backups. Backups just happen.

Home and individual users, however, don't have access to an IT department and need to think about their own backup needs. A consumer-level backup utility is one option. Using a backup utility, since it is automated, takes less time, and you don't have to remember to do it. A backup utility also compresses the files as it backs them up, so the backups take up less drive space than the originals. However, the backups it creates aren't ready-to-use versions of the files; they're compressed into archive files. If you ever need to access the backed-up files, you must use the same backup utility to extract them.

Copying files manually to a volume results in ready-to-use backup copies, which is convenient if you need quick access to a backed-up file. You need to exercise discipline if you plan to go the manual route.

There are three main classes of backup applications. The first kind makes an image of the entire hard drive and then restores the disk image to new hardware in the event of a drive failure. This is sometimes called *imaging software*. Some popular imaging applications include StorageCraft ShadowProtect and Acronis True Image.

A second kind of backup application backs up individual files and folders that you specify. Microsoft Windows 7 comes with the Backup utility that does this kind of backup. Windows 8 and newer offer a third style of backup called File History that uses an additional storage drive to back up personal documents. Apple includes Time Machine with macOS, which takes snapshots of user

https://t.me/learningnets

documents.

Data Replication

You can use data replication to place an up-to-date copy of data in other geographical regions near users who need those files or for backup purposes. You can do this if your company has file servers in various locations around the world, although these days we can configure replication to other geographical regions through public cloud providers such as Microsoft Azure or Amazon Web Services (AWS).

With synchronous replication, an application does not receive notification that data has been written until *all* replicas have committed the data to disk. This normally requires a high-speed network. With asynchronous replication, after the primary, or first, replica has written the data, an application then receives notification that data has been written to disk; this can be used over slow network links.

Online Storage as Backup Media

If you use a cloud storage service like OneDrive or online storage provided by your employer, you might want to back up your important files to the cloud. This can be a simple, cost-effective way to keep your files safe because it doesn't involve any special utilities. In Windows, each user has a OneDrive folder in his or her user folders; a shortcut to it appears in the Navigation pane in File Explorer. When you place files in that folder, they are saved locally on your hard drive, but they are also uploaded to the OneDrive cloud, and any changes you make to the local copies are mirrored automatically in the online versions. Other cloud-based file storage systems can be configured to work similarly.

If you depend on a cloud provider for the storage of your backups, think redundancy. You should have two Internet connections, ideally through different providers between your on-premises network and the cloud, and you should make sure you have enough bandwidth to restore data quickly from the cloud to your on-premises network in the event of a disaster.

Backup Scheduling and Frequency

Whether you use a backup program or make backup copies manually, you should have a schedule in place to make sure you have recent backups available at all times. A backup utility will have a scheduling component that you can set up to perform a backup at specified intervals. If you're making your own backup copies, you'll need to create a reminder for yourself, perhaps in a calendar

https://t.me/learningnets

program.

Most data security experts recommend performing a weekly or monthly backup of the full set of your important data files as a starting point and then saving incremental daily changes.

Backup Storage Media

For maximum safety (in terms of your data surviving catastrophic what-ifs), you should back up to a different physical location than where your computer resides. If your home or office burns to the ground or gets swept away by a hurricane or earthquake, at least one copy of your data should ideally be far from danger.

There are several methods, listed here:

- You can back up to an off-site cloud-based location via the Internet.
- If your company has multiple locations, you could use the company's network to send your backup files to a network drive located in a different building, city, or even continent.
- You could also make backups to an external locally attached storage device (such as an external hard drive, USB thumb drive, or optical disc) and then physically carry (or ship) it somewhere else (take it home, for example, or leave it in a safe-deposit box).

If your data is not so important that you need to go to all that trouble, a lower level of protection would be to duplicate the data outside of your computer. Send it via LAN to network-attached storage (NAS), for example, or back up to an external drive. *Network-attached storage* connects to your network independently of any particular computer, such as a file server or a *NAS appliance* (a specialized network-enabled external drive that multiple users can share).



EXAM TIP Objective 6.7 lists cloud and local storage for backups. Make sure you understand the convenience and safety trade-offs for each of these storage locations.

https://t.me/learningnets

Backup Verification and Testing

If you go to the trouble of setting up a backup schedule (and perhaps purchasing backup software), make sure it works. Don't wait until disaster strikes and you need to restore your files before you test the process!

The first time you use a new backup method, verify the backups. Test them by going through the restoration process, and make sure the files are completely and accurately restored to their original locations. After you have verified that the process works, spot-check it regularly. The more critical the data, the more often you should check.

Chapter Review

In this chapter, you learned about folders and paths and how to navigate them using an OS file management utility. You worked mostly with File Explorer in Windows but learned that the equivalent utilities are Finder in macOS and Files in (Ubuntu) Linux.

You learned how to view and change file and folder properties using the Properties box in File Explorer and about the four basic attributes: read-only, system, hidden, and archive. You saw that file properties include size, dates created and modified, and keywords.

You learned how to manipulate files and folders in Microsoft Windows, including how to open, edit, save, move, copy, rename, and delete. You also learned how to search, sort, and display file listings, as well as how to protect your important files with local permissions and backups.

Questions

1. Which of these is a correctly written file path?
   - **A.** C:>Books/Mike\birthdays.txt
   - **B.** C:/Books/Mike/birthdays.txt
   - **C.** C:\Books\Mike\birthdays.txt
   - **D.** C:\\Books\Mike\birthdays.txt
2. What is a root directory?
   - **A.** The top-level storage location on a volume
   - **B.** The folder containing the system files
   - **C.** The folder containing the boot files

https://t.me/learningnets

D. The folder containing the signed-in user's personal files

3. What is the file management tool in macOS?
   A. File Explorer
   B. Dock
   C. Launcher
   D. Finder
4. Which of these is an on/off flag for a file?
   A. Size
   B. Archive
   C. Date modified
   D. Date created
5. Which file property makes a search faster for content within files?
   A. Archive
   B. Indexed
   C. Compressed
   D. Encrypted
6. What action opens a data file for editing in the application associated with its extension?
   A. Double-click
   B. Right-click
   C. CTRL-click
   B. SHIFT-click
7. How do you select multiple noncontiguous files in a file listing?
   A. CTRL-click
   B. SHIFT-click
   B. Double-click
   C. Right-click
8. CTRL-V is a keyboard shortcut in Windows for what activity?
   A. Copy
   B. Paste
   C. Cut

https://t.me/learningnets

D. Delete

9. In File Explorer, from which tab can you select a different view?
   A. View
   B. Share
   C. Details
   D. Home
10. Which utility in macOS backs up user files automatically?
   A. Backup
   B. File Explorer
   C. File History
   D. Time Machine

Answers

1. **C**. A correctly written path begins with the drive letter, a colon, and one backslash, and separates locations with backslashes. The other options don't follow this pattern.
2. **A**. The root directory is the top-level location on a volume. The other options don't describe the top-level location.
3. **D**. Finder is the macOS file management utility. File Explorer is the Windows file management utility. Dock and Launcher are components of macOS and Linux, respectively, but not involving file management.
4. **B**. Archive is an on/off flag (attribute). The others all have specific values.
5. **B**. Indexed allows a file's content to be indexed, speeding up searches. Archive indicates whether a file has changed since it has been backed up. Compressed and Encrypted are NTFS-specific properties that control how the file is stored.
6. **A**. Double-click a data file to open it. Right-click it to see a shortcut menu. CTRL-click and SHIFT-click select multiple files in a file listing.
7. **A**. CTRL-click each item to select them. SHIFT-click selects multiple contiguous files. Double-click opens a file. Right-click displays a shortcut menu.
8. **B**. CTRL-V is for Paste. CTRL-C is for copy. CTRL-X is for cut. DELETE is for deletion.

https://t.me/learningnets

9. **A**. Change the view on the View tab. The Share and Home tabs do not contain view commands. Details is not a tab; it is a pane that you access from the View tab.
10. **D**. macOS uses Time Machine to back up user files automatically.

https://t.me/learningnets

CHAPTER 9

Using and Managing Application Software

In this chapter, you will learn how to

- Run applications
- Install and uninstall applications
- Identify common applications and their uses
- Describe application licensing and distribution

This chapter tells the story of applications, starting with a primer on how to run them in several different operating systems. Second, we'll look at the process used in each operating system (OS) to install applications. The next section looks at the types of applications available today and reviews some common file types. The chapter finishes with licensing issues. We've got a lot of ground to cover, so let's get started!

Running an Application

As you learned in Chapter 5, the operating system handles the computer's basic operation and housekeeping. In contrast, an *application* enables you to do something with the computer. You can produce something of value, such as calculate a budget, touch up a photo, or play music. For convenience and flexibility, each OS has multiple ways of running an application. The procedure for running an application depends on the OS you use.

Many modern applications use a multitiered model. Traditionally, single-tier applications (also called *monolithic* applications) contained all of the application software logic running on a single computer. These days, many applications have a front-end or user interface (UI) tier, such as a web site that runs on a web server. Client devices connect to the front-end tier using a web browser. The UI tier running on the web server might then communicate with a middle-tier

https://t.me/learningnets

software component running on a different server, which in turn might read and write data to a back-end tier hosting database servers. This type of model is also called an *n-tier* application model.

N-tiered applications provide numerous benefits:

- Developers can make code changes to one tier while not affecting another tier.
- Updates can be applied modularly to specific tiers.
- Security controls can be applied separately to each tier.
- To maximize application performance and availability, different tiers can be load-balanced. Load balancing takes incoming application requests and distributes the least busy server in a group of servers hosting the application.
- IT administrators can back up tiers separately from one another.



NOTE The term *app* is often used as shorthand for application, especially the small applications that run on mobile devices. Some people use the terms *application* and *program* synonymously, but that's not really accurate. Whereas *program* refers to any software, *application* means a program that isn't involved in running or maintaining the computer itself.

Running an Application in Windows

The process of running an application in Windows varies somewhat depending on the Windows version, so let's look each version individually.



TIP You can also customize your desktop and taskbar with shortcuts to applications you access regularly.

In Windows 10, click the Start button to open the menu (see Figure 9-1). If there's a shortcut for the desired application in the Most used list along the left side or pinned to the Start menu as a tile on the right side, click that shortcut and

https://t.me/learningnets

you’re done.

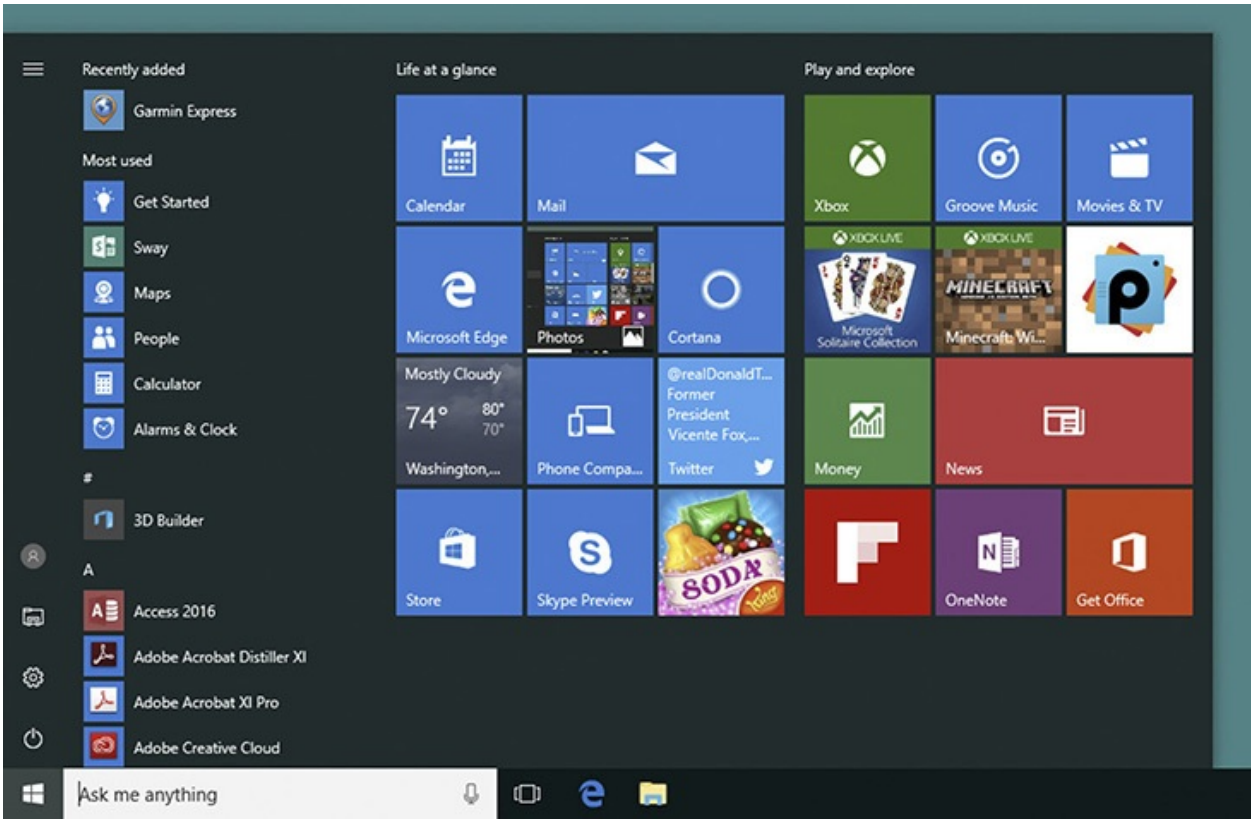


Figure 9-1 Open the Start menu to access shortcuts to the installed applications.

If you don’t see the application you want, you have a couple of options. You can scroll down to see a complete alphabetized list of available applications and then click the desired application’s shortcut from there. Alternatively, you can begin typing the name of the desired app and then select it from the search results, as in Figure 9-2.

https://t.me/learningnets

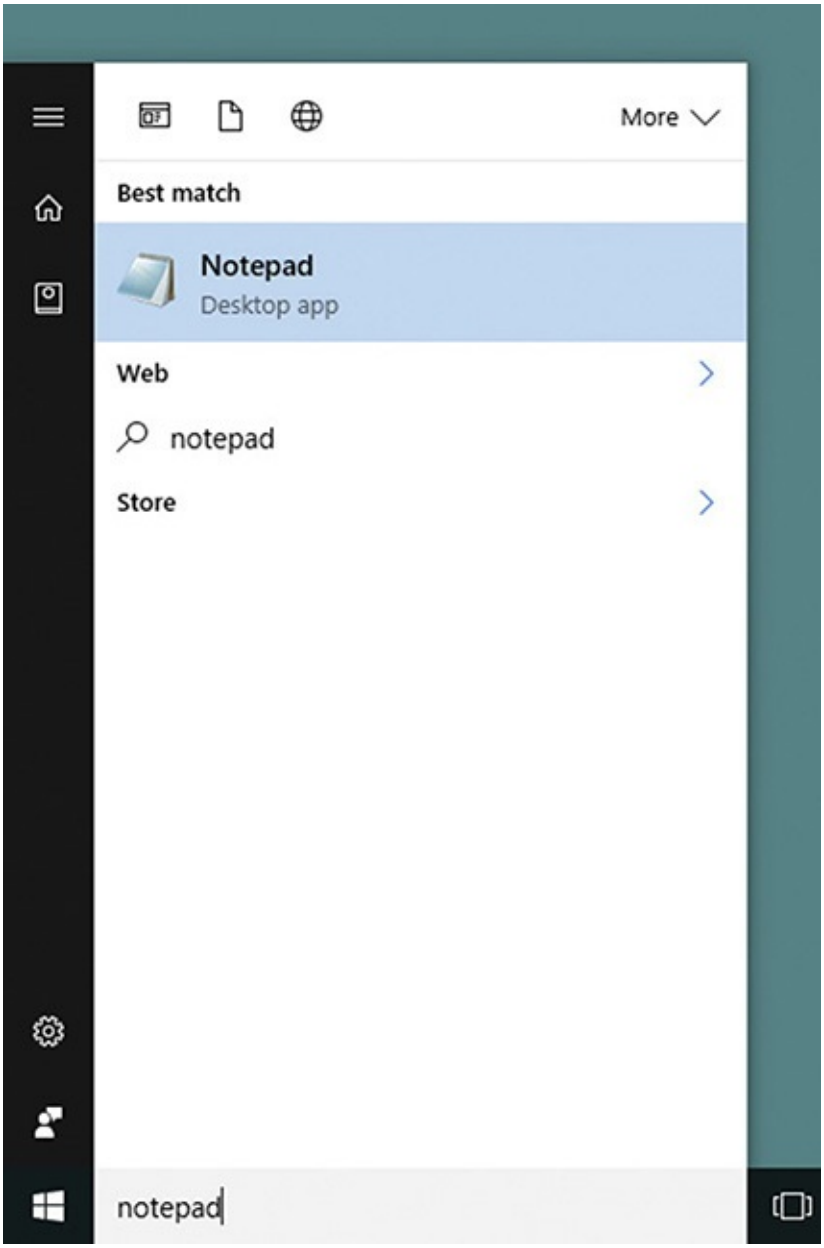


Figure 9-2 Begin typing an app's name and then select it from the search results.

When you click the Start button in Windows 8.1, you get the Start screen rather than the Start menu. You can click a shortcut tile on the Start screen to start an application, or you can click the down arrow at the bottom of the Start screen to display the Apps list. It's the same alphabetical list as before, but (as Figure 9-3 shows) it occupies the entire screen. Like in Windows 10, you can also start typing the name of the application you want to run and then choose it from the search results.

https://t.me/learningnets

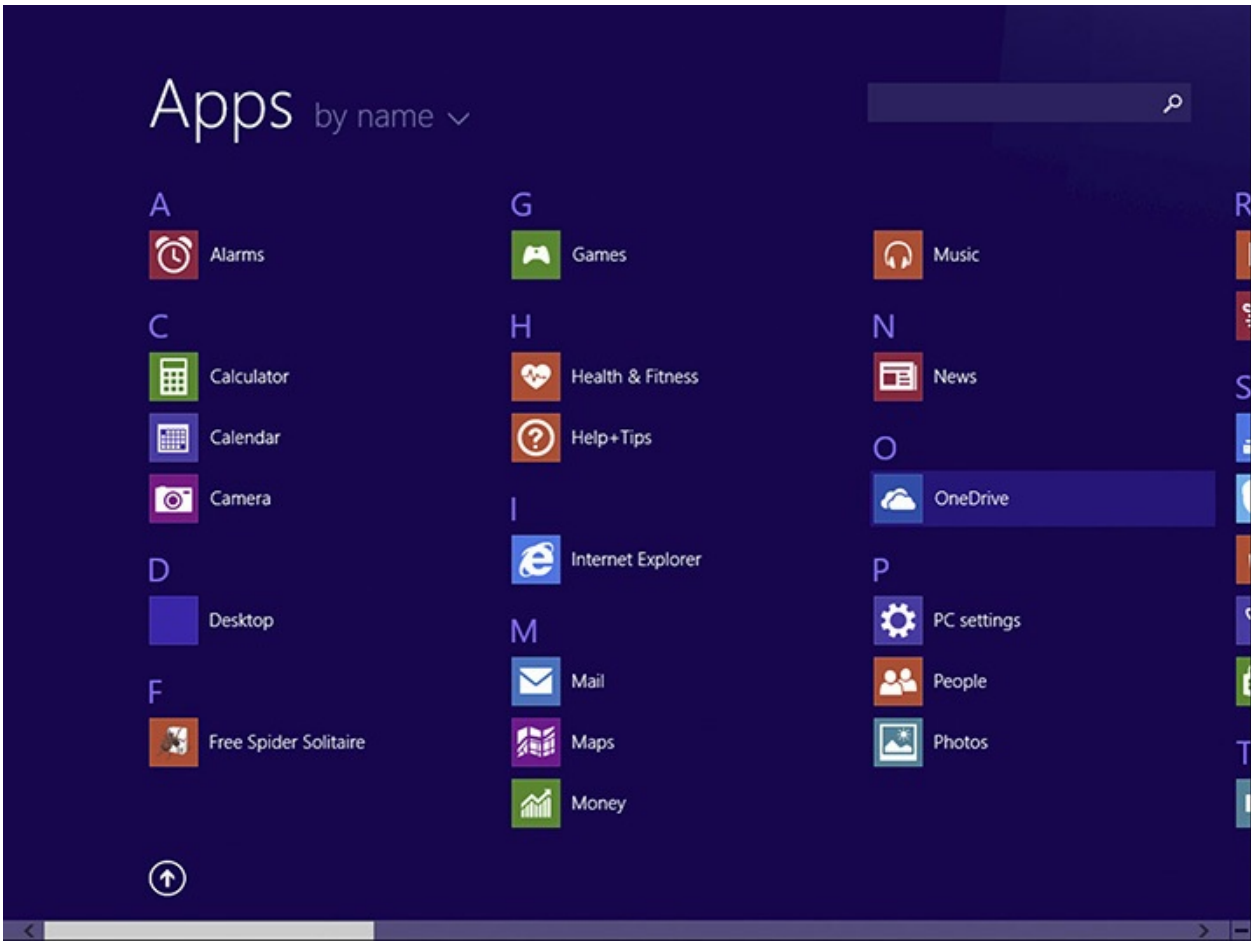


Figure 9-3 The Apps list in Windows 8.1



EXAM TIP The missing Start button in Windows 8 doesn't feature in the CompTIA IT Fundamentals exam. Assume every version of Windows has a Start button.

In Windows 7, the process is similar to Windows 10. Click the Start button to open the Start menu. If you don't see the app you want, click All Programs to open an alphabetical list of programs, or click in the Search box near the bottom of the Start menu and type the first few letters of the desired app's name.

Running an Application in macOS

https://t.me/learningnets

In macOS, the Dock at the bottom of the screen contains shortcuts to frequently used applications, similar to the taskbar and Start menu/screen in Windows. Click an application to run it (Figure 9-4).



Figure 9-4 Click icons in the Dock to run the associated program.

If the app you want doesn't appear on the Dock, click the Launchpad button on the Dock to open the Launchpad window, which contains icons for all the installed applications. Click the desired icon from there to start the application.



NOTE You can also run applications by searching for them with the macOS search tool, Spotlight, and clicking them or pressing enter.

Running an Application in Linux

In any version of Linux, you can use the Terminal (the command prompt) to run command-line applications. The command-line environment is used more for utilities and file management than for applications that directly serve the average user, though, so you will more often run applications within Linux's graphical user interface (GUI). As in Chapter 5, we'll look at the default GUI in Ubuntu Linux, Unity.

If a shortcut for the desired application appears on the Launcher bar along the left side of the screen, click it to start the application (Figure 9-5). If not, you can do the following:

https://t.me/learningnets



Figure 9-5 Click an icon on the Launcher bar to run an associated program.

- Click the Dash button (the topmost icon on the Launcher) and then click the Applications button at the bottom of the Dash pane (Figure 9-6).

https://t.me/learningnets

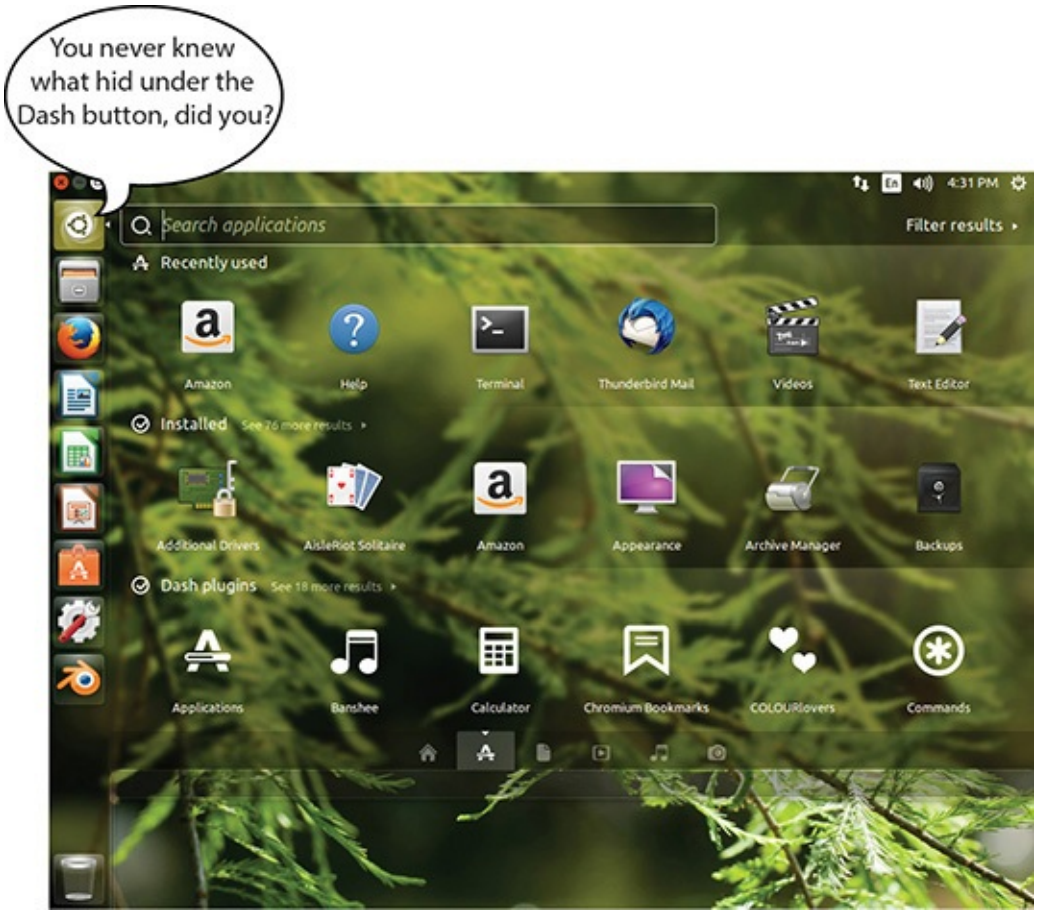


Figure 9-6 In Dash, click the Applications button to find more programs.

- Click the Dash button, begin typing the application name, and then click its name in the search results.

Running an Application in Chrome OS

To run an application in Chrome OS, right-click one of the apps on the shelf (Figure 9-7) or click the Launcher button (bottom left) to display all the available apps. Click the one you want to open (Figure 9-8).

https://t.me/learningnets

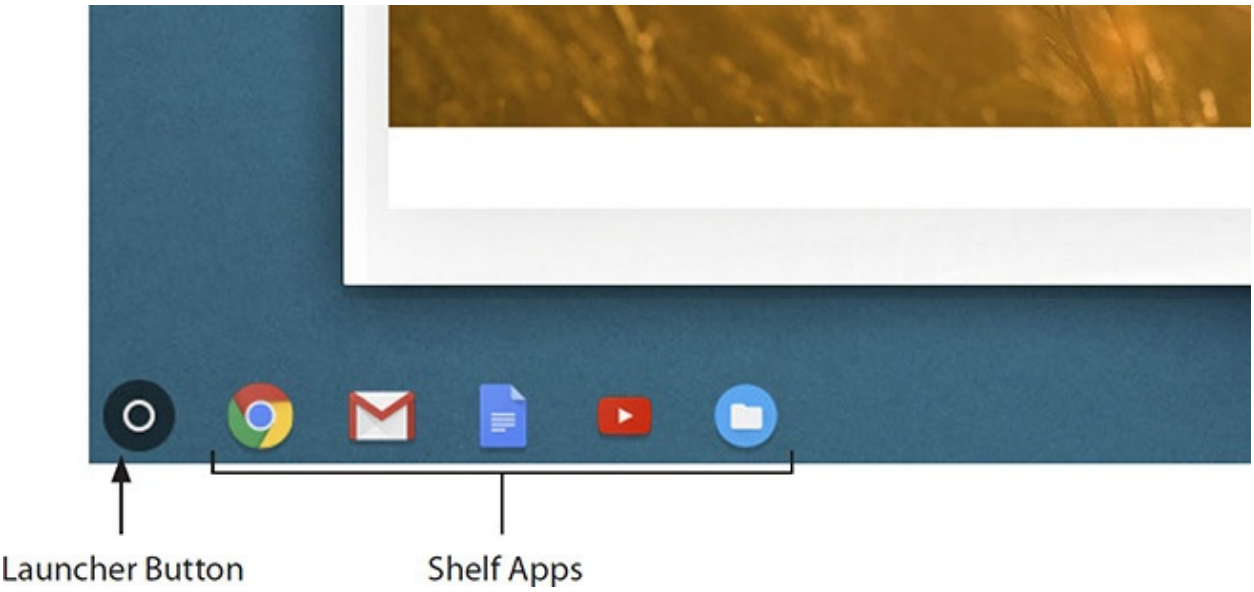


Figure 9-7 The shelf has commonly accessed apps.

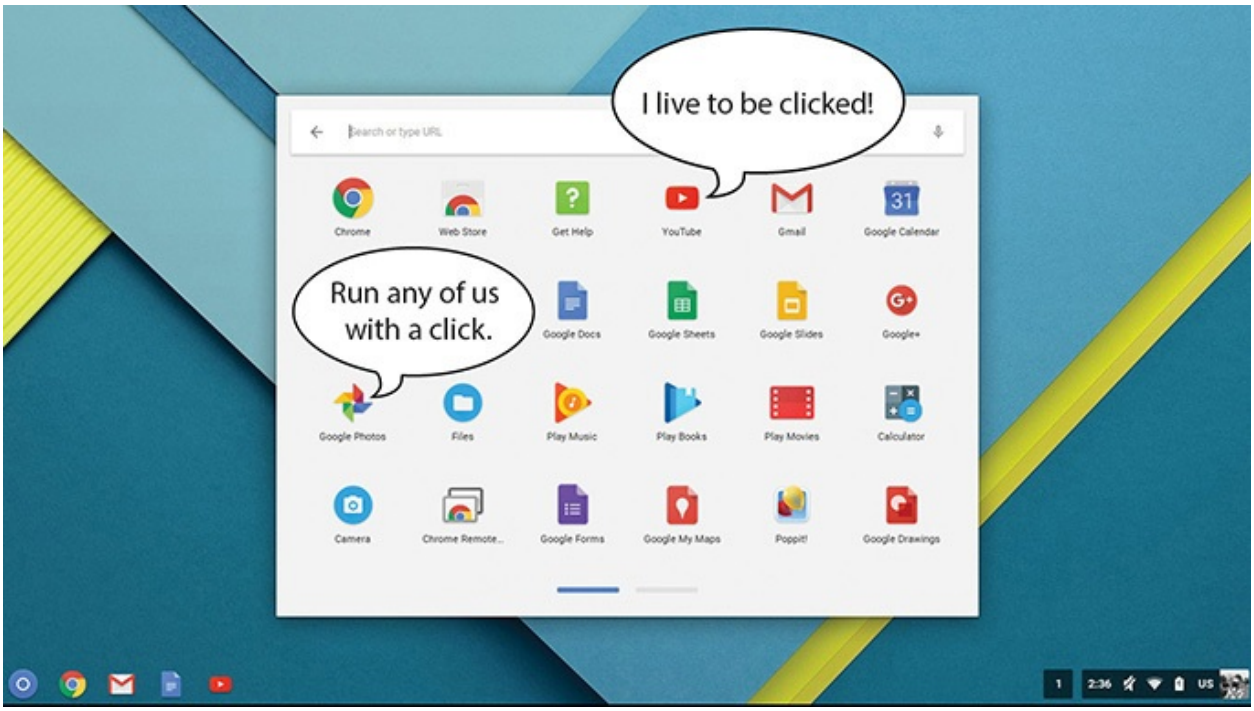


Figure 9-8 Open the Launcher bar and then click All programs to see everything you can currently do on the Chrome OS device.

Running an Application on a Smartphone

Smartphone operating systems such as Android and Apple iOS are similar when

https://t.me/learningnets

it comes to running an app. You can simply tap the app icon to launch the app on your device. Depending on the app, you might be required to provide user credentials to log in, you might be asked to grant permission to the app, or it might just open up immediately.

Some apps will stop running if the focus is switched to another app or if the phone is locked. An example of this is the YouTube app, which stops playing if it does not have the focus or if the phone is locked.

Switching Between Applications

Each of the desktop operating systems covered in the CompTIA IT Fundamentals exam can run multiple applications at once, but only one *active application* has focus at a time; any text you type or keyboard shortcuts you press will apply to this active application. Other applications can continue to operate in the background, and their displays might update, but you must switch to the app before you can interact with it.

There are many different ways to switch to an application:

- Click the desired application's button in the taskbar (Windows), Dock (macOS), Launcher (Unity Linux), or shelf (Chrome OS).
- If any portion of the application window is visible, click it.
- In Windows, press alt-esc. Each time you do so, a different application becomes active.
- Hold down the alt key (Windows, Linux, Chrome OS) or command key (macOS) and tap the tab key. Each time you press and release tab, a different application becomes active. Release the alt or command key when the desired application is active.
- Chrome OS has a couple of quirks that make it different from the other desktop environments. First, many applications run as tabs in the Chrome web browser. Press ctrl-tab or alt-tab to go to the next or previous tab. Second, dedicated Chrome machines, like a Chromebook portable, have a switcher key that brings up active programs. Click the program you want to bring into focus.
- Smartphone operating system techniques vary. You might switch between running apps using an app switcher button at the bottom of your screen (Android), or you might press a specific area of the screen and then swipe to the right to display an app switcher tool (iPhone).

https://t.me/learningnets

Saving Your Work

Many programs enable you to create data files and save them for later use. Microsoft Word enables you to create and save documents that you can later reopen, edit, save, and print. Saving works the same way across all operating systems and, for the most part, is standard across most applications too.

In any application, look for a Save or Save As command. If the data file has not previously been saved, these commands are identical—they both open the Save As dialog box, from which you can specify a filename, location, and type. Many individuals and companies prefer saving files in the cloud. This means running an application on your local computing device but saving resulting data files in cloud storage hosted by a cloud providers such as Microsoft OneDrive, Google Drive, or Amazon Web Services S3 storage, to name just a few.

Figure 9-9 shows an example of saving a file. If the file has been previously saved, the Save command resaves it with the same settings, without opening a dialog box.

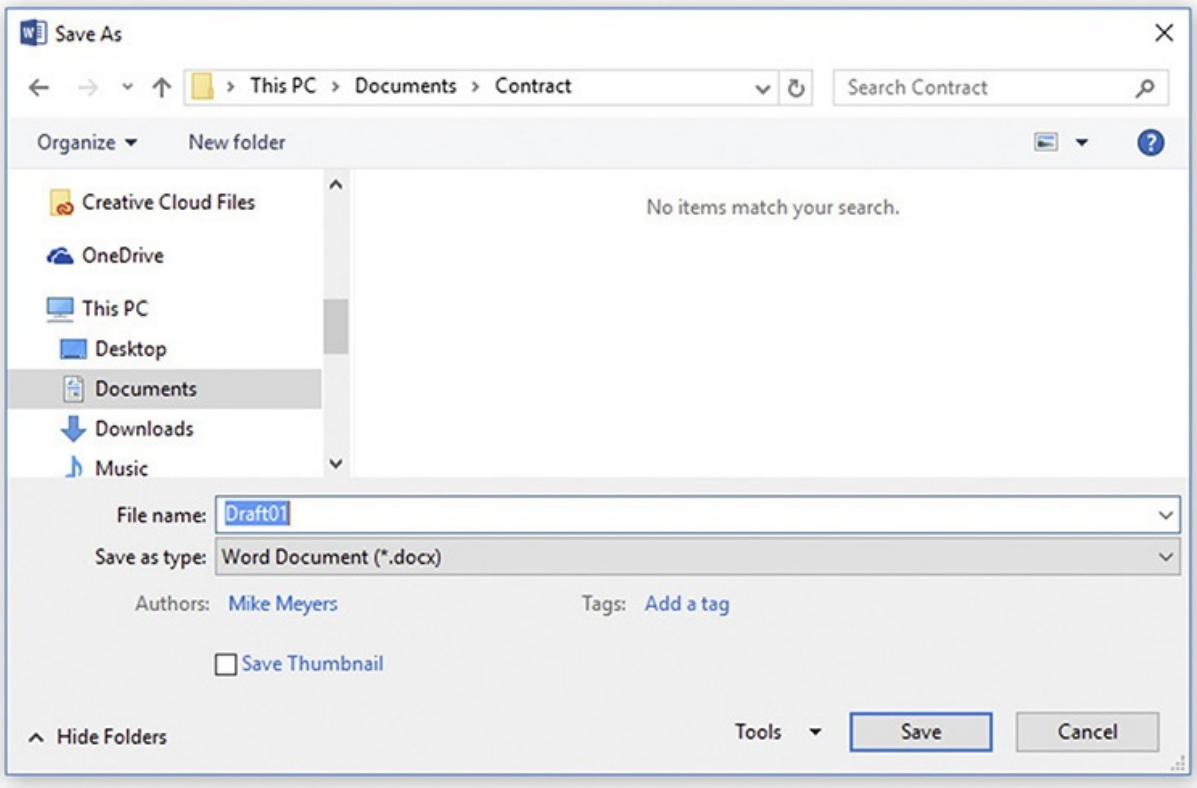


Figure 9-9 A Save As dialog box enables you to save your work.

https://t.me/learningnets

Exiting an Application

To close an application, use its Exit command or Quit command. Look for that command on the File menu (in most Windows and Linux applications) or on the menu named after the application (in macOS applications).

Depending on the OS and application, you might be able to exit by closing the application's window. In Windows, Linux (Unity), and Chrome OS, closing an application's window exits the application. In macOS, however, closing the application's window does not exit the application in many cases. (It depends on the application.) The application might still be open in the background. If the application has an icon on the Dock, a black dot under the icon indicates it is still open.



EXAM TIP For troubleshooting misbehaving or unresponsive applications, check out Chapter 13.

Installing, Updating, and Removing Applications

Next, let's take a look at the procedures for installing, updating, and removing applications. It's different in each OS (and among some versions/editions of the same OS, of course), but they are all similar.

Common to all is understanding the software that best fits the computing need and then reading installation instructions. A clear understanding of software licensing and use agreements is also important. For cloud-based apps, a *service level agreement* (SLA) lists cloud software usage and expected uptime and performance details.

Installing Applications

You'll probably want to install some additional applications to add capabilities to the computing device. You can buy applications in retail stores, buy and download applications online, or get applications from an app store associated with your OS. Some corporate networks also allow the installation of software over the company network. In some cases, the software runs only when it detects a connection to the corporate network either locally or through a remote *virtual private network* (VPN) connection when users are out of the office.

https://t.me/learningnets

When you get them from an app store, they'll typically install automatically. If not, you'll run a setup program (often called an *installer*) that prepares your system to run the application. The following sections explain the various installation methods.



NOTE Installer files can have any name the developers want to give them. Installers you download may be named after the application and may also include its version number. These installers are often named Setup, especially if the application comes on removable media such as an optical disc.

Installing a Desktop Application in Windows

Windows desktop applications typically have an installer. To install an application from removable media such as CD or DVD, insert the media and wait a moment to see whether the system either prompts you to run the installer or runs it automatically. If it does neither, browse the file system for the disc, locate the installer (its extension is usually .exe or .msi), and double-click it to get the ball rolling.

Many original equipment manufacturers (OEMs) that supply software for specific types of hardware, such as for Acer laptops, will provide their software for download on their web site as a compressed file or an ISO file. Third-party software vendors often also provide their software in the same way.

ISO files are CD or DVD images stored as a single file. On a Windows 10 computer, you can double-click the ISO to either open it in a decompression program such as 7-Zip or have it automatically mount as a drive letter, which also lets you view the file system contained within the ISO. The double-click behavior depends on your Windows file association settings. You can right-click an ISO file in Windows 10, choose Properties, and click the Change button next to Opens With. Then you can choose Windows Explorer for ISO automounting.



EXAM TIP This section and the next list common installer file extensions you'll encounter on Windows and macOS. If you aren't already familiar with file formats and extensions, circle back to confirm you understand these sections

https://t.me/learningnets

after you have learned about formats and extensions later in the chapter.

An installer you download may technically be a compressed archive file (with a format such as ZIP, 7z, RAR, and so on), in which case you'll have to double-click it once to unpack the files to a folder on your system. The setup utility might run automatically after that; if not, navigate to the folder the installer unpacked to and double-click it.



NOTE A *compressed archive file* is a single file that, much like a folder, can contain and compress many files. Compression "packs" data more efficiently so that it uses less space until you "unpack" it later.

Compressed archive files make it easy to bundle up related files (such as an application) and transfer them efficiently. Your OS can pack and unpack the most common compressed archive formats, but you may need a separate application to work with less common formats.

In either case, you may see a User Account Control (UAC) security prompt when you double-click the installer. You'll learn more about this in Chapter 11, but the UAC prompt is your system's way of confirming you (and not some malware) initiated the request. In this case, click Yes to continue—but don't get in the habit of clicking through unexpected UAC prompts unless you understand what caused them and know they are safe.

From here, follow the prompts to install the application. During the setup process, you may be asked to specify a location for the files, as in Figure 9-10 (the default location is usually best), and you might have the choice of installing optional features or doing a custom installation.

https://t.me/learningnets

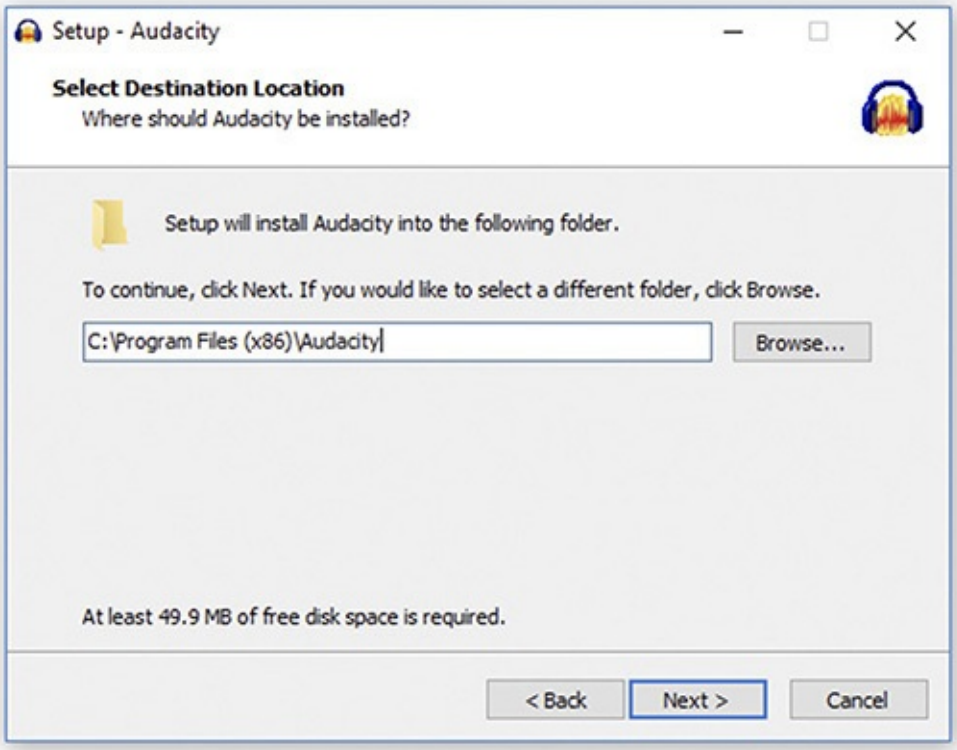


Figure 9-10 Work through the prompts to install a desktop application.



CAUTION It's often fine to pick the default or express installation, but it's safer to pick the Custom option to make sure the installer doesn't add extra software you don't want; you'll learn more about these risks in Chapter 11. If you don't understand specific custom options, stick with the default.

Installing a Desktop Application in macOS

To install an application from a disc, first insert the disc in the computer. A setup utility might run automatically. If it doesn't, browse the disc using Finder. Locate a file named Setup (or similar) and double-click it to start the setup process.

To install downloaded software on a Mac, double-click the file you downloaded. If an error message appears that the application can't be opened because it wasn't downloaded from the Mac App Store, right-click the downloaded file and click Open. Mac installation files come in several different

https://t.me/learningnets

formats: ZIP, PKG, or DMG. If it's a .zip file, double-clicking it unpacks the .zip file into its own folder, and within that folder you will find a .pkg or .dmg file. Double-click it. A .pkg file will install the application for you automatically from that point; a .dmg file may require you to manually drag the app into the Applications folder (using Finder). See Figure 9-11. You can delete the downloaded file when you're done.



Figure 9-11 Manually installing an app in macOS

Installing an App from an Online Store

All four desktop operating systems have a dedicated online app store so you can download and install programs. The store app enables you to browse applications, make a selection, and click Install. Figure 9-12 shows an app being selected in the Windows Store, for example. It's a free app, so you would click Free to begin the download. The rest of the setup process is completely automated—no choices to make.

https://t.me/learningnets

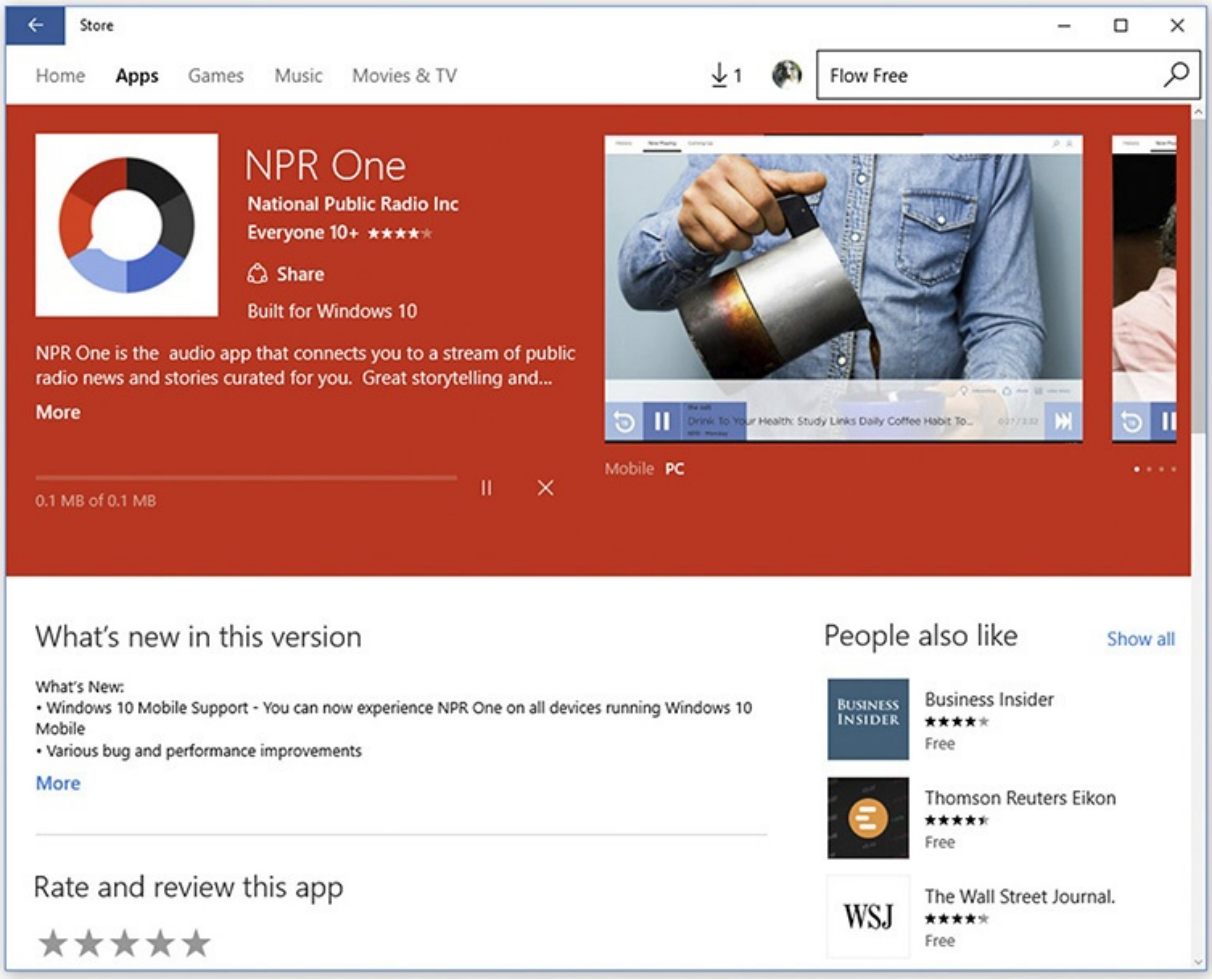


Figure 9-12 Installing a free application from the Windows Store



NOTE Be suspicious of free apps. In the best-case scenario, the app does what it says but installs ads or other software. In the worst-case scenario, the free app is, or contains, malware that might steal personal information from your device, encrypt your data files and demand a ransom for decryption, or monitor your device usage. Installing an app sometimes asks for specific permissions that the app will use. Be selective in allowing app privileges to items such as contact lists, GPS location, e-mail messages, and so on.

Using Web-Based Applications

You use web-based applications directly through a browser or other tool when

https://t.me/learningnets

you connect to the Internet. You do not need to install web-based applications, which are also called *cloud-based* applications. Companies provide these applications as a *service* to users, which is why web-based applications are described as *software as a service* (SaaS). Some SaaS is "free" to the user (this often means the developer makes money by showing you ads or collecting data about you), but most paid SaaS requires a monthly or yearly subscription.



NOTE Some desktop applications (including Microsoft Office 365) are licensed as SaaS but downloaded as desktop applications. You pay your first month's "rent" on the application, and then you can download its installer. You can use the application anytime, not just when online. Subscription-based software you can use offline may require you to go online once in a while to confirm your subscription is current.

Updating Applications

Like operating systems, applications can be updated to fix problems and add features. An update designed to fix problems is sometimes called a *patch*.

The process for downloading application updates varies depending on the application and the OS. Under Windows, Microsoft Office application updates are automatically installed along with Windows updates by default, for example.

Other applications run a small utility in the background that periodically checks a web site for updates and informs you of (or even installs) updates. You can often modify the scheduling and frequency of these update checks.



TIP Multiple applications running their own background utility to watch for updates can collectively use enough memory to make system performance suffer. If your system is running slowly, investigate whether you can disable some applications' automatic update features.

Still other applications have a manual Check for updates command, such as the one in the Help menu in Figure 9-13.

https://t.me/learningnets

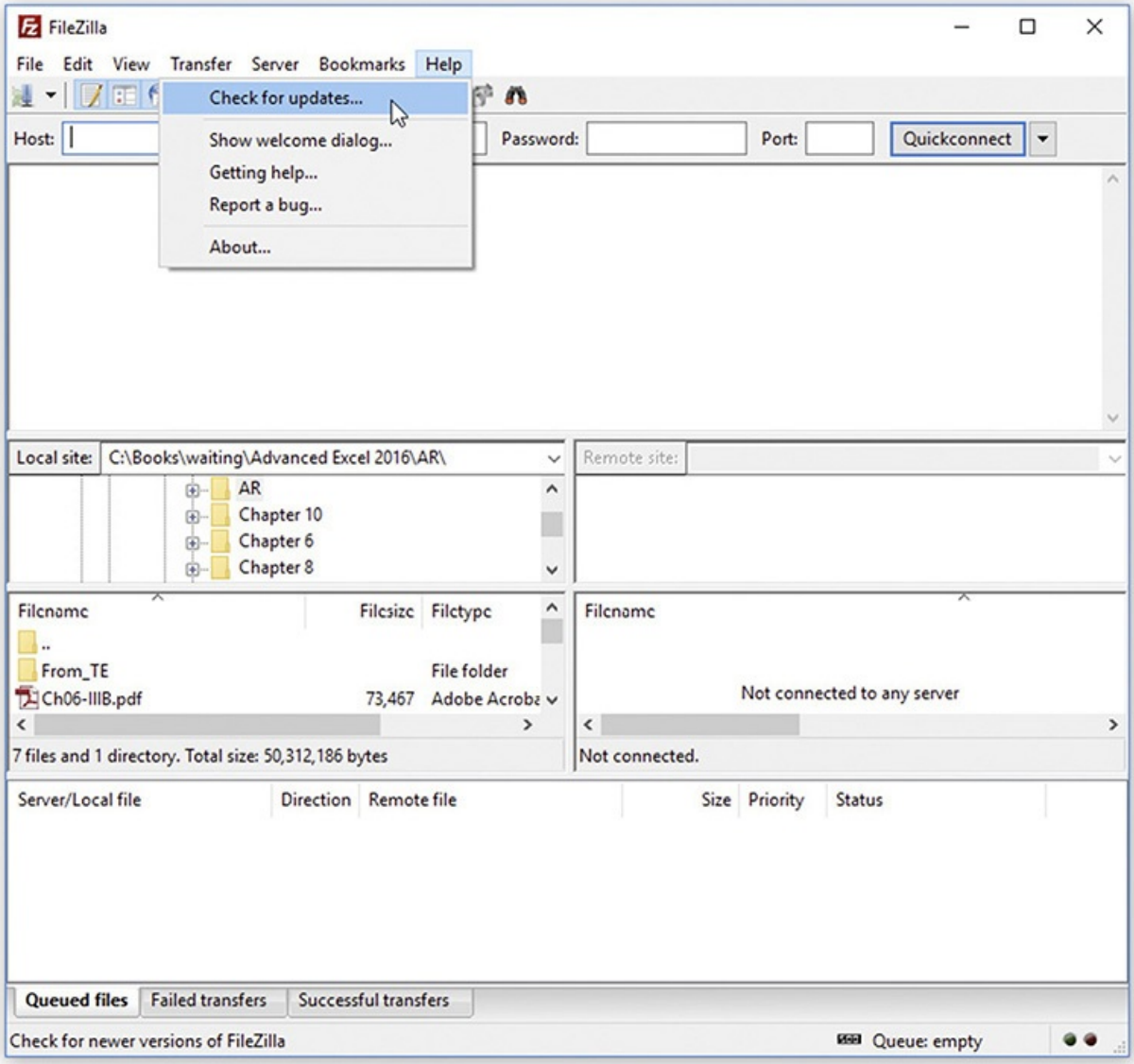


Figure 9-13 FileZilla's update command

All of these options compare the installed version number to the latest available number to make sure the new version truly is newer than the one you already have. You can also manually find an application's version number and check its web site to see whether there is a newer version.

- If there is a Help menu, open it and look for an About command. Figure 9-14 shows the result of such a command in FileZilla.

https://t.me/learningnets

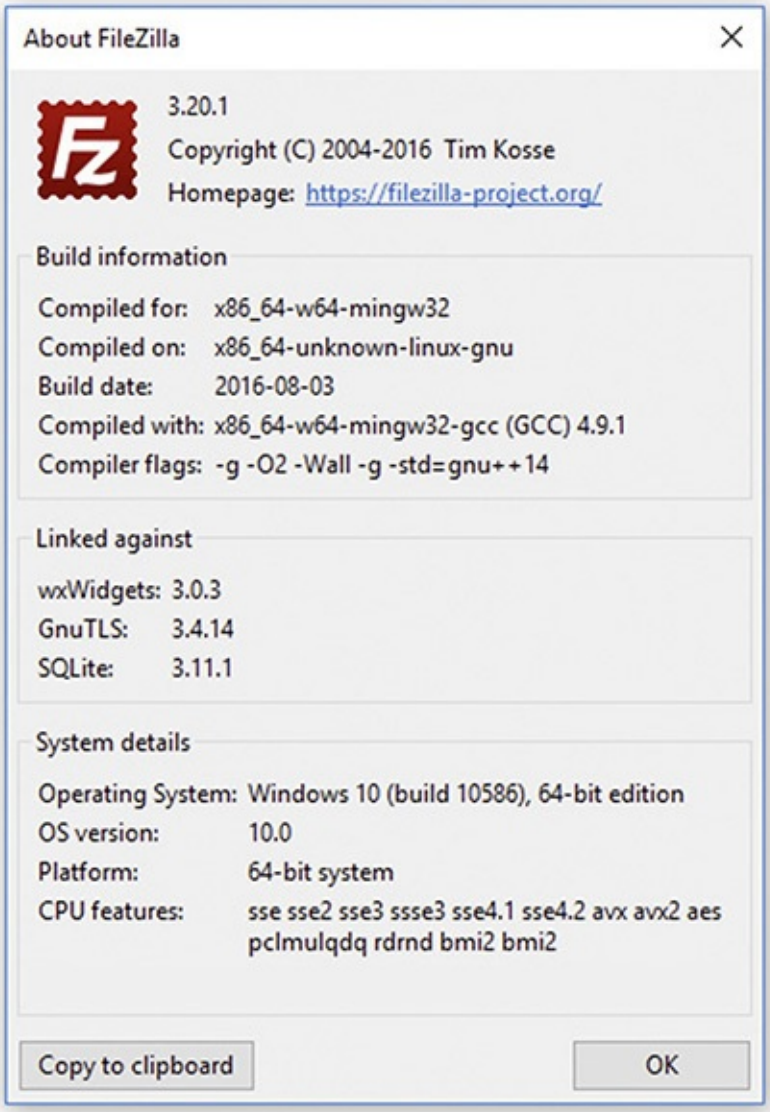


Figure 9-14 About FileZilla with version number at top

- In Microsoft Office applications, click the File tab and click Account and then click the About button.

Armed with the application's version number, you can also research any compatibility issues. For example, if you are running an older version of Windows and an update is available for your favorite application, it's a good idea to check online for any known compatibility issues between the new version and your OS version.

https://t.me/learningnets

Removing Applications

In some operating systems and with some application types, uninstalling is kind of a big deal; you have to go through a step-by-step process. In other cases, it's just a few clicks. The following sections summarize the processes you should know.

Removing a Windows Desktop Application

Let's start with Windows desktop applications because they are generally the most complicated to uninstall. The uninstall process removes the application's files, modifies system files, and deletes the application's shortcuts.

To remove a Windows desktop application, open the Control Panel and click Programs | Uninstall a Program. A list of installed applications appears. Click the one you want to remove, click Uninstall (or Uninstall/Change), and then follow the prompts. The uninstall process is similar to the setup process and usually involves multiple steps. Figure 9-15 shows an example.

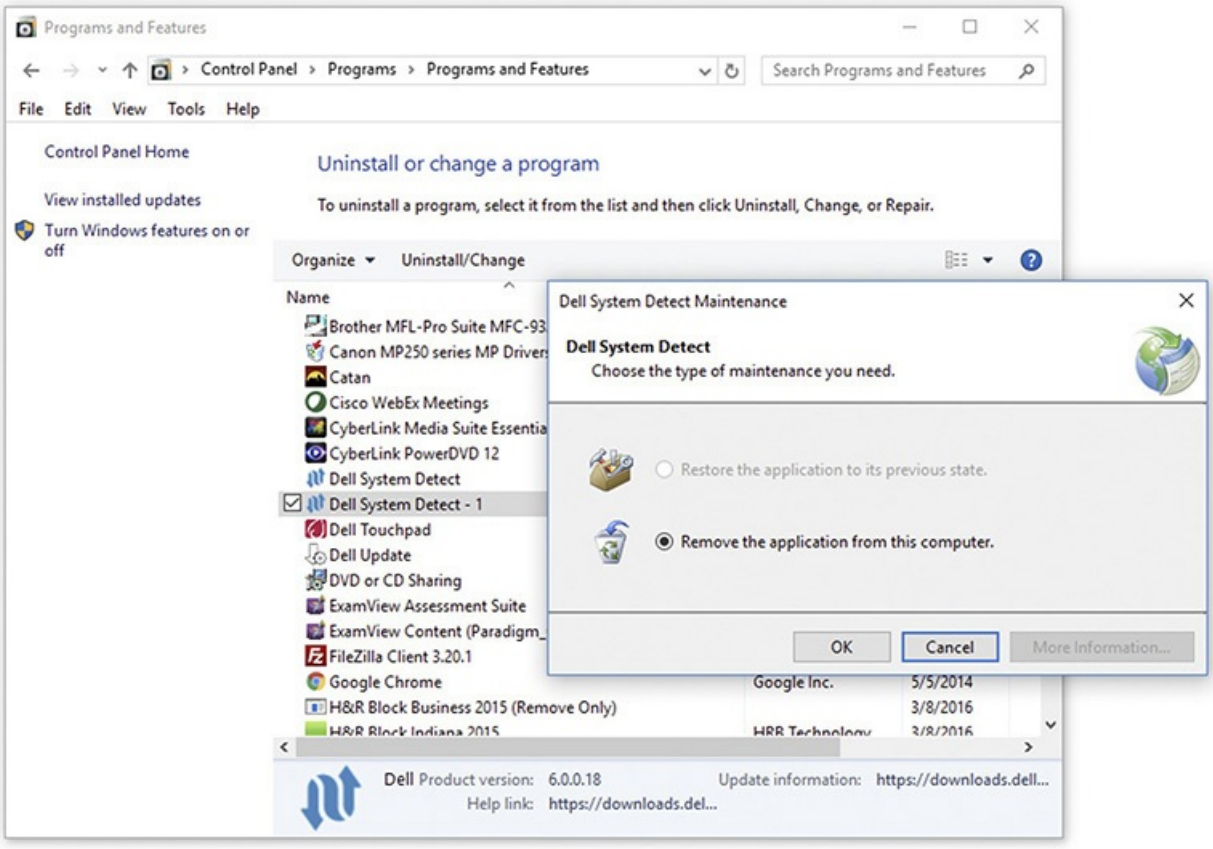


Figure 9-15 Click Uninstall or Uninstall/Change and then follow the prompts.

https://t.me/learningnets



NOTE The instructions here assume Control Panel is in the default Category view, which organizes utilities by category. If the drop-down menu in the upper-right corner doesn't say View By: Category, open the drop-down and choose Category.

Removing a Modern Windows App

To uninstall a Modern app (one you download from the Windows Store), first locate it on the Start screen or Start menu. You might have to bring up the full Apps list. Then right-click it and choose Uninstall, as in Figure 9-16.

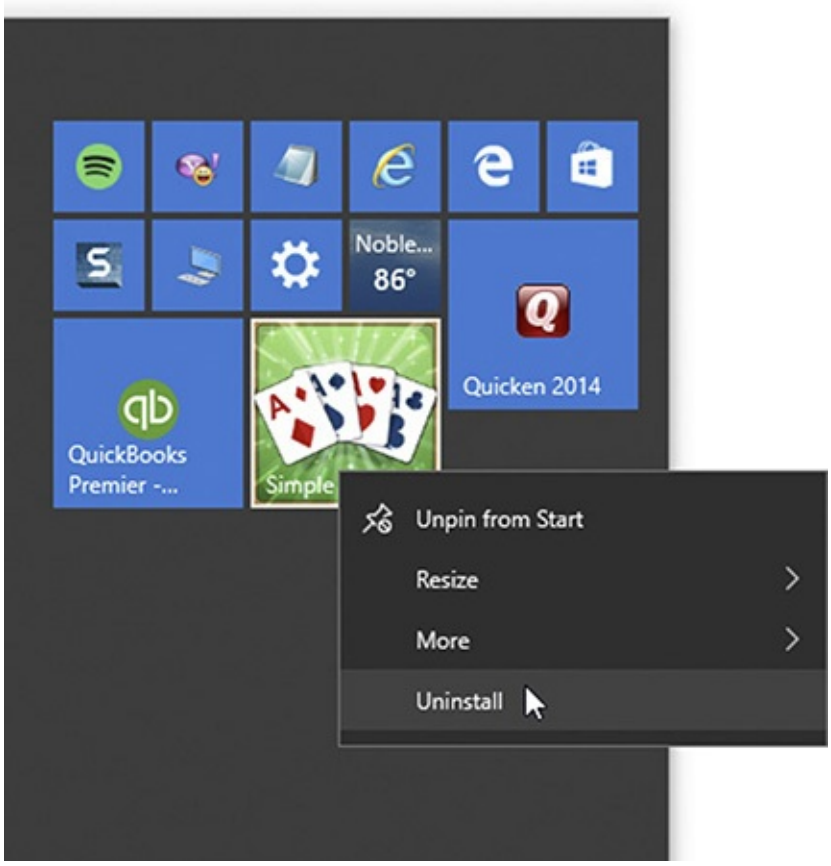


Figure 9-16 Uninstall a Modern app by right-clicking it and choosing Uninstall.

Removing a macOS Application

On a computer running macOS, drag the application from the Applications folder to the Trash located on the Dock. Then choose Finder | Empty Trash and

https://t.me/learningnets

it’s gone.

Removing an App in Ubuntu Linux

In Ubuntu’s Unity GUI, click the Ubuntu Software Center icon on the Launcher bar. Then on the toolbar at the top of the window, click Installed to see the installed applications. Expand the category for the app you want to remove so you can find it and then click it and click Remove. Figure 9-17 shows an example.

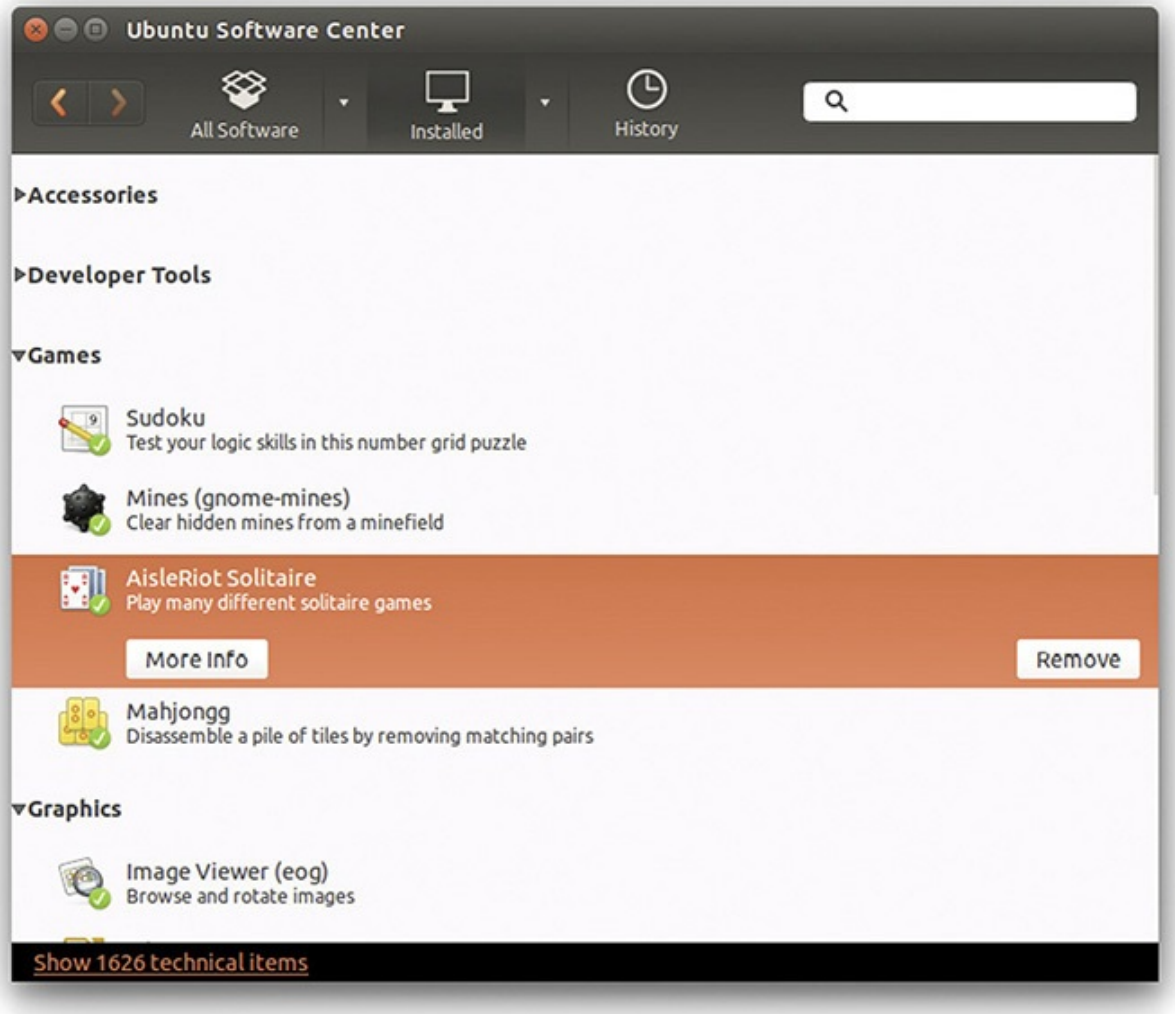


Figure 9-17 Uninstall applications in Ubuntu Linux via the Ubuntu Software Center.

https://t.me/learningnets



TIP You can also remove a Linux application from the command line. For example, with Ubuntu Linux, you could use the *sudo apt-get remove* command prefix followed by the name of the software package to be removed. The *sudo* command prefix runs the command that follows it with elevated privileges; this is enabled on many, but not all, Linux systems.

Removing an App in Chrome OS

To remove an app in Chrome OS, open Launcher and select All Apps. Right-click the app you want to uninstall and select Uninstall. Click Remove and the app goes away. If you have a single-button touchpad, hold the ALT key down and single click to access the uninstallation option.

Common Applications and Their Uses

This section is a whirlwind tour of the various application types and platforms you may encounter. The objectives list for the CompTIA IT Fundamentals exam has more than two dozen application types and three dozen file extensions, but you're not expected to know how to use everything. That would go well beyond the scope of the certification. You should read this section to get a sense of all the types of applications used in modern computing.



EXAM TIP You will get questions on the CompTIA IT Fundamentals exam that ask about which file extensions go with which type of software. A good study tool for memorizing the extensions here is to make a handwritten, two-column chart that matches extension to file type. Writing it out helps the memorization process.

Platforms

As you learned in Chapter 1, a *platform* is the hardware on which an OS (and its applications) runs such as mobile, workstation (also called *desktop*), and web-

https://t.me/learningnets

based, so let's look at each.

Desktop in this context does not mean a desktop PC necessarily but software that runs on a desktop OS such as Windows or macOS. *Mobile* means software that is designed to run on a mobile OS such as Android or iOS. Web-based means software that is accessed through a web browser. *Web-based*, or *cloud-based*, software (such as Office Online at www.office.com) is usually available only when you connect to the Internet and use the app's web site.

Types

In the context of the CompTIA IT Fundamentals objectives, an application's type refers to its overall purpose. What is it designed to help you do? Does it help you with business documents? Does it help you collaborate? The following sections provide a look at the types listed in the exam objectives. It's not a comprehensive list of every type of software that exists, but it's a good start for understanding what's available. Bear in mind that some software can fall into multiple categories despite not being listed that way in the following tables.



EXAM TIP Objective 3.3 lists three main types: Productivity, Collaboration, and Business software.

Productivity Software

This rather large class of software includes programs designed to help you do productive tasks associated with making a living, such as writing documents, managing personal information, giving presentations, storing data, and sending e-mail. Table 9-1 lists the types of productivity application the objectives specifically mention and explains each.

https://t.me/learningnets

Application Type	Purpose	Examples
Word processing	Create business and personal documents such as letters, reports, memos, and manuscripts	Microsoft Word (Windows, macOS) Pages (macOS) LibreOffice Writer (Linux) Google Docs (Chrome OS)
Spreadsheet software	Create worksheets that perform calculations on financial and statistical data	Microsoft Excel (Windows, macOS) Numbers (macOS) LibreOffice Calc (Linux) Google Sheets (Chrome OS)
PDF viewers/ creator	View and create formatted pages for printing or distribution on any platform	Adobe Acrobat (reads and creates) Adobe Reader (only reads)
Presentation software	Create graphical slides to support presentations	Microsoft PowerPoint (Windows, macOS) Keynote (macOS) LibreOffice Impress (Linux) Google Slides (Chrome OS)
Desktop publishing software	Combine text and graphics into page layouts such as magazine pages and brochures	Microsoft Publisher (Windows) Quark Xpress (macOS, Windows)
Personal information manager	Manage contacts, calendars, tasks, notes, and reminders; may also send, receive, and manage e-mail	Microsoft Outlook (Windows) Evolution (Linux)
Remote desktop software	Access the desktop of one computer from another	Windows Remote Desktop
Visual diagramming software	Create blueprints and 3D renderings of buildings and products, create and edit drawings and other artwork, edit photos	AutoCAD Adobe Photoshop Adobe Illustrator
Web browser	Connect to web services on local networks as well as the Internet; used for research and entertainment (YouTube, NetFlix) as well as for the use of web-based application usage such as G Suite (formerly Google Apps) or Microsoft Office 365	Microsoft Internet Explorer Microsoft Edge Google Chrome Apple Safari

Table 9-1 Productivity Software Types

Collaboration Software

Collaboration software helps people communicate and work with one another, and it helps computers share information. Although this collaboration can be

https://t.me/learningnets

personal in nature, it's more often for business. Table 9-2 lists the collaboration software types you should know for the exam.

Application Type	Purpose	Examples
Online workspace	Provide an online environment for running cloud-based services and applications	Office Online (applications) Microsoft SharePoint (complete environment including file libraries and messaging) Google Docs
Document storage/sharing	Provide private or sharable file storage via cloud-based services	Microsoft OneDrive Google Drive
Screen-sharing software	Enable a remote user to see and take control of another user's screen while the original user and others watch	Windows Remote Assistance Can also be built into video-conferencing software
Video-conferencing software	Place and receive video calls among two or more locations; may also include screen, file, and application sharing	Citrix GoToMeeting
Instant messaging software	Enable two or more people to communicate in real-time using text; may also include video-conferencing capability	Yahoo! Messenger AOL Instant Messenger
E-mail software	Sends and receives e-mail messages	Microsoft Outlook (Windows, macOS) Mail (Windows) Evolution (Linux) Gmail (Chrome OS)

Table 9-2 Collaboration Software Types

Business Software

This type of software refers to applications that are related to business-specific process and the tracking of projects and financial information. Table 9-3 provides further detail.

https://t.me/learningnets

Application Type	Purpose	Examples
Database	Store and manage structured data, such as lists of contacts, products, or transactions.	Microsoft Access (Windows) Microsoft SQL Server FileMaker (macOS, Windows) MySQL Oracle Database
Financial	Track and manage financial information; many different types exist, from personal finance applications to software that runs large accounting departments.	Quicken TurboTax Peachtree Accounting QuickBooks
Project management	Create and track project details such as milestones, schedules, deadlines, and budgets. Team members can update their progress for specific project tasks.	Microsoft Project LiquidPlanner Wrike
Business-specific	Also called *line-of-business* (LoB) apps, these can be purchased or custom developed. Specific industries such as medical and manufacturing use software specifically tailored for those types of businesses.	AdvancedMD (patient health records, telemedicine) WorkWise ERP (manufacturing process management)

Table 9-3 Business Software Types

Utility Software

Utility software is arguably not in the Productivity category because it doesn't do anything directly for the human using the computer. Instead, utilities help keep the computer running smoothly and help manage and distribute files. You should know the utility software types listed in Table 9-4.

https://t.me/learningnets

Application Type	Purpose	Examples
Anti-malware	Scan a system for malicious software (malware) including viruses, worms, and exploits. See Chapter 12 for more about this kind of software.	Norton Internet Security Symantec Endpoint Protection McAfee VirusScan Malwarebytes Windows Defender
Software firewalls	Prevent hackers from gaining access to a computer remotely via network or Internet.	Windows Firewall Norton Firewall
Diagnostic/ maintenance software	Check hard disks for errors and optimize their performance. Chapter 13 covers several kinds of diagnostic software.	Check Disk/Error Checking Optimize Drives (Windows)
Compression software	Combine and compress multiple files into a single archive file that can be more easily distributed. See the "Compression Formats" section later in this chapter.	WinZip Compression features built into some operating systems

Table 9-4 Utility Software Types

Specialized Software

In this category are applications designed to appeal to a specific segment of the population. This can include software for people in professions such as computer-aided design 229(CAD), medicine, science, and finance, as well as games and entertainment applications designed for people of a certain type or age. Table 9-5 reviews the types mentioned in the exam objectives.

Application Type	Purpose	Examples
Scientific	One type provides reference information and tools for scientific professionals; another type manages the process of doing scientific research.	LabVIEW Mathematica MATLAB Origin
Gaming	Entertain (and potentially educate) the user; may run on separate PCs independently or on a network. May be desktop, mobile, or web-based.	*The Sims* *World of Warcraft* *Candy Crush*
Entertainment (nongames)	Entertain a specific audience, such as playing music or movies or providing digital copies of magazines to read.	Texture Spotify iTunes Windows Media Player

https://t.me/learningnets

Table 9-5 Specialized Software Types

Common File Types

Each application has a default format for its data files, also called its *file type*. On Windows systems, a file's type is specified by its extension, which is a code (usually three characters but not always) that follows the filename, separated by a period, like this: myfile.txt. In other operating systems, the file type is determined by the OS looking inside the file for that information, so a file's extension, if it has one, is not a reliable way to determine a file's actual type. Still, it's a good starting point.

Executables

Files that run programs are known as *executables*. An executable can be part of the OS itself, an application, or an installation package. Table 9-6 lists some common executable formats you should be familiar with for the exam.

Extension	File Type
.app	A Mac application bundle. In macOS it looks like an application executable, but the *bundle* is actually a folder containing the application's files. Windows users just see the bundle as a folder.
.bat	A batch file (or *script*) is a list of commands to be executed in sequential order.
.exe or .com	A Windows application. An .exe file may have multiple helper files that work with it; a .com file is normally a stand-alone application.
.msi	An installer package file format used in Windows.

Table 9-6 Executable File Extensions on the CompTIA IT Fundamentals Exam

Compression Formats

Groups of files can be compressed and combined into a single *compressed archive* file, which makes the group of files easier to distribute and transport (Figure 9-18). For example, suppose you have to send ten picture files to someone. You could attach all ten files separately to an e-mail, but it would be better to create a single compressed archive that holds them.

https://t.me/learningnets

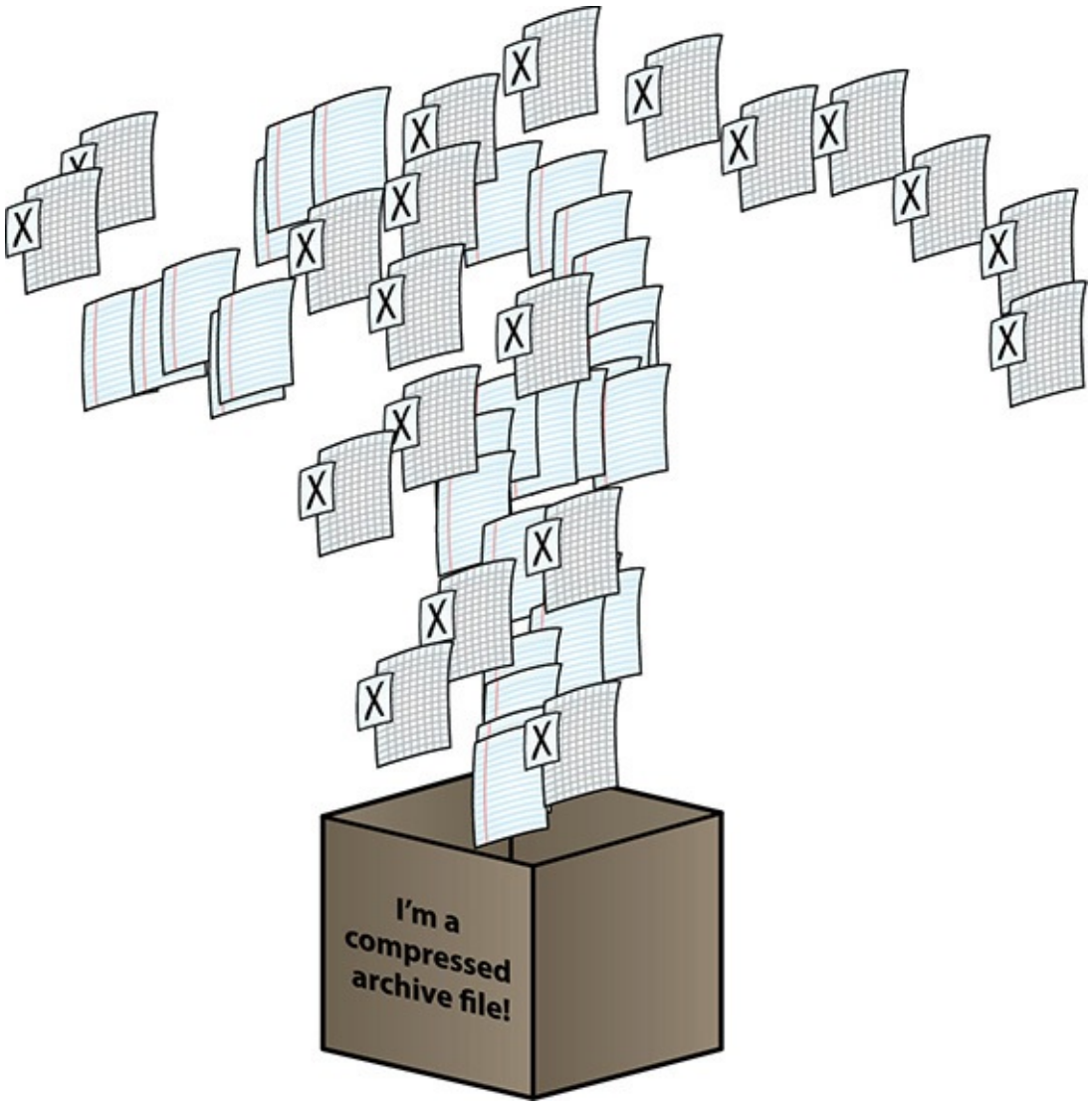


Figure 9-18 Creating a compressed archive file

To create a compressed zip archive file out of a group of files in File Explorer, select the files and then right-click the selection, point to Send To, and click Compressed (zipped) folder. Type a name for the compressed archive file (the default is the name of the first file in the selection) and press Enter. Now you can take this .zip file and e-mail, move, copy, or do anything else with it that you can do with a regular file. It will open in File Explorer as if it were a folder if you double-click it. File Explorer will give you the option to extract all of the files, but you can also just select and move or copy specific files out of the .zip file.

You may encounter many other compressed archive formats, but in Windows, .zip (the default) dominates. Some of these formats may require you to use a

https://t.me/learningnets

third-party utility to create and manage their archive files. Table 9-7 lists the compressed archive formats you should know.

Format	Purpose
7-ZIP or 7z	7ZIP is the default format for the file compression utility 7-Zip archiver. 7z is an updated version of the file format, offering better compression and security.
DMG	The format of a macOS disc image; similar to ISO but for Mac.
GZIP or GZ	The default format for the gzip utility. The G stands for GNU. GNU is a Linux variant.
ISO	The format of a file that represents an optical disc image; use a DVD-burning application to burn an ISO file to removable media such as a blank CD, DVD, or USB flash drive.
JAR	A compression format for Java classes and data. You may encounter this when you work with Java applications.
RAR	The default format of the WinRAR file archive program
TAR	The Linux and UNIX standard archive format. It's an acronym that stands for *tape archive*.
ZIP	A popular compression format for Windows computers. Originally developed for a command-line application called PKZIP, it is now most closely associated with WinZip.

Table 9-7 Compression Formats

Audio and Video Formats

Collectively, files containing audio (such as voice recordings, music, or audio books) and video (movies, music videos, presentations, TV shows, and so on) are often referred to as *media clips*. You'll need to download some media clips before you can play them, but your device can play *streaming media* as the clips transfer from sites and services such as SoundCloud, YouTube, Spotify, and Netflix. There are many different formats for audio and video recordings, each with its own set of benefits and drawbacks.

No media player supports all formats, so it's important to find one that supports the formats of the clips you want to play. The playback software must have a *codec* installed for each format it supports. Codec is short for "compressor-decompressor," and it refers to the encoding of the clips. Playback software uses the codec to decode clips on the fly. Windows Media Player in some versions and editions of Windows, for example, lacks the codec needed to play most DVD movies; you must purchase a codec as an add-on to the application.

https://t.me/learningnets



CAUTION *Compression* can refer to condensed files like the compressed archive files discussed here. It can also refer to the encoding of a media file.

Some clips are *compressed*, meaning they use a special type of encoding that makes the file take up less disk space. You'll find two types of this kind of compression with media files: lossless and lossy.

Lossless compression creates a file that retains the quality of the original file. Media producers use this kind of compression when file size doesn't really matter but quality does.

Lossy compression deletes some of data from the file to make the final file size smaller. That funny cat video on YouTube uses a lossy compression, but it looks good enough on a computer monitor. You would only see the fact that it's missing data if you made the image huge.

Almost all video files are *containers* for data encoded in any of several different formats. Codecs are for the inner content, not the container file type. To play back the clip, the player must have a codec for the formats used inside the file.

Most video files are container files for both visual and audio data, each decoded by a different codec during playback. The playback software needs to know how to talk to the container file and have the correct codecs for the internal data.

Here's where you can run into trouble. A container file gets a file extension, such as .mov. There's no rule that says that data inside a .mov container has to use one type of encoding. You can have two .mov container files with wildly different internal encoding. Even if playback software can talk to .mov files, it needs the codecs for all the internal data as well. With a missing codec, you might hear sound but get no video when playing a media clip.

An audio or video container file may have special features or properties. Some formats support *digital rights management* (DRM), for example, a kind of copy protection that prevents copyrighted clips from being freely shared. (The music and film industries call this a feature, but most of us call it a nuisance!)



https://t.me/learningnets

EXAM TIP The list of acronyms for the CompTIA IT Fundamentals exam includes MP3 and MP4. All of these share a common source: Moving Pictures Experts Group (MPEG). MPEG is a standards organization that has defined several popular audio and video formats.

Table 9-8 lists the audio and video formats you should know.

https://t.me/learningnets

Type	Format	Purpose
Audio	AAC	Advanced Audio Coding (AAC) was designed to replace MP3. It has better sound quality than MP3 at similar compression levels and file sizes.
Audio	FLAC	Free Lossless Audio Codec (FLAC) is similar to MP3, but the lossless compression yields a little higher quality.
Audio	M4A	This format is used for music downloads from iTunes that have no copy protection on them. M4A is a container file, and the content inside the container is usually coded as AAC.
Audio	MP3	This is a common general format for music files. It's popular because it uses a high level of lossy compression (so files are small), it lacks copy protection (so files can be freely shared), and almost all music player applications support it. The extension is short for Moving Picture Experts Group Layer 3 Audio.
Audio	WAV	The raw data inside is usually uncompressed CD-quality sound. The files are large, so this format is not usually used for long clips. This is the default container format for the Sound Recorder application in Windows.
Audio	MID/MIDI	This format is not in the exam objectives, but it is in the exam acronyms list. A Musical Instrument Digital Interface (MIDI) file is a text file that takes advantage of the sound-processing hardware to enable the computing device to produce sound. Programmers use these small files to tell the sound card which notes to play; how long, how loud, and on which instruments to play them; and so forth. Think of a MIDI file as a piece of electronic sheet music, with the instruments built into your sound card.
Video	AVI	Audio Video Interleave (AVI) is a Microsoft-created container format for audio and video. It's a common format for short, homemade videos you might find online.
Video	FLV	Flash Video (FLV) is a container file format designed to distribute video online using Adobe Flash Player as the playback application, usually within a web page.
Video	MP4	This format uses MPEG-4 raw video data and usually AAC or MP3 audio data. The extension is short for Moving Picture Experts Group Layer 4.
Video	MPG/MPEG	The MPG format is a container that can hold either MPEG-1 or MPEG-2 raw video data, plus accompanying audio data. It is an older format but still in use. The extension is an acronym for Moving Picture Experts Group.
Video	WMV	Windows Media Video (WMV) is used in some Microsoft programs that deal with user-created videos, such as Windows Movie Maker.

Table 9-8 Audio and Video Formats

Image Formats

https://t.me/learningnets

Files that store still images, like photos, are called *image formats*. There are two kinds of image files: raster and vector. A *raster format* is used for photos and digital paintings. It contains color information for each individual dot (pixel) in the entire image. Another name for this kind of image is bitmap (because it is literally a map of bits). Raster image files tend to be rather large, even when compression is applied. (As with audio and video, compression can be lossless or lossy.) The main drawback to the raster format is that the image loses quality when it is resized (particularly when resized larger than the original). Raster images are created and edited in programs like Microsoft Paint and Adobe Photoshop.

A *vector format* is used for line drawings. It uses math formulas to describe each line and curve in the image, like the geometry formulas you might have plotted in high school. Vector drawings are not photorealistic, but they take up a lot less space, and they don't lose quality when resized. Vector format is great for technical drawings and flow charts. You create vector drawings when you use the drawing tools in Microsoft Office applications, for example, or when you use an application like Microsoft Visio or Adobe Illustrator.



EXAM TIP No vector formats appear in the CompTIA IT Fundamentals objectives, but graphic artists and illustrators often work in vector formats that are easy to re-scale as needed and export in a raster format.

Raster formats have their own unique mix of file size, compression, and quality, and each has its fans in certain industries. For example, the GIF format has a somewhat unusual extra capability: it can store several versions (frames) of the graphic inside a single file and cycle among them automatically, so it's popular on web page advertisements that cycle through several ads. Table 9-9 describes the image formats you need to know.

https://t.me/learningnets

Format	Purpose
BMP	Short for bitmap, the BMP format is one of the oldest raster formats used in personal computing. In the early days of Windows, BMP was the only format that Microsoft's application Paint supported. BMP is widely supported in many graphics applications for backward compatibility but no longer widely used because there are other formats that are more appealing in terms of file size and quality.
GIF	Graphics File Interchange (GIF) is an uncompressed format. It supports only 256 colors, so it's not a great choice for photos, but it is popular for web page ads because it can store and cycle through several graphics in a single file.
JPG/JPEG	Joint Photographic Experts Group (JPG or JPEG) is a lossy image compression format that sacrifices some image quality but has a small file size. It's commonly used on the Web and in on-screen graphics, where you can't detect the reduced image quality.
PNG	Portable Network Graphic (PNG) is the successor to GIF. It uses lossless compression and supports 16.7 million colors, a big improvement from GIF's 256 colors. It is one of the most popular formats used on web pages and in game graphics.
TIF/TIFF	Tagged Image File Format (TFF or TIFF) uses lossless compression and is considered a high-quality format but with a rather large file size. Some digital cameras capture images in this format, and photos in publications that will be printed on paper often use this format because of the high quality.

Table 9-9 Image Formats

Documents

Our final category of file type to consider is *documents*. It includes not only various types of text-heavy files but also spreadsheets, presentations, and page layouts—all types of data files that you would create in business-oriented applications. Table 9-10 summarizes the document file types you should know.

https://t.me/learningnets

Format	Purpose
TXT	A plain-text file, with no formatting. This is the default format for the Notepad app in Windows, as well as most other text editors.
RTF	Rich Text Format (RTF) is a widely accepted generic word processing format. Nearly all word processing applications can read and write this format. It includes all the basic text formatting options, including fonts, attributes, paragraph indentation, margins, bullets and numbering, and headers/footers.
DOC/DOCX	The DOCX format is the current format for Microsoft Word documents and is also used by many other word processing applications for compatibility with Word. The DOC format is an earlier version, used in Word 2003 and earlier and still supported.
XLS/XLSX	Microsoft Excel, the spreadsheet application, uses XLSX as its default format. The XLS format is an earlier version, used in Excel 2003 and earlier and still supported.
PPT/PPTX	Microsoft PowerPoint, the presentation application, uses PPTX as its default format. The PPT format is an earlier version, used in PowerPoint 2003 and earlier and still supported.
PDF	Portable Document Format (PDF) is the default format for Adobe Acrobat and Adobe Reader. This format is designed to make document formatting consistent when distributing documents across platforms. No matter what computer or device you open up a PDF file on, the file looks the same, without any variation in fonts or spacing. You can save to PDF in most Microsoft Office applications; you can also set up a PDF print driver that outputs print jobs to PDF files, useful in applications that do not save to PDF.

Table 9-10 Document Formats

Software Licensing

Companies distribute software in several ways. When you purchase a computer, it comes with the operating system and some other basic *bundled* (pre-installed) applications from the original equipment manufacturer such as a text editor, a media player, and a web browser.

Some software is sold in neat little boxes that include an optical disc or USB flash drive containing the application installer so that you can install software locally. Most folks use the Internet these days to get software; this includes both programs you download and web apps (software as a service) that you access with a browser.

All software is subject to licensing and copyright regulations, so you usually have to agree to an *end-user license agreement* (EULA) before using a program or service. The terms vary depending on the type of software, but they're most common when you install, update, or open a downloaded program, and when you register, log in to, or access a web app. Agreeing to the EULA creates a

https://t.me/learningnets

contract between the software company and the user (you). This contract specifies terms such as how many computers you can install it on and limits the vendor's liability should something disastrous occur as a result of installing the software.

A lot of (often overlapping) terms apply to how software developers sell, distribute, and license their products. Let's look at some of the most common here.

- Software that you can download at no cost—like Adobe Reader or Google Chrome—is called *freeware*. Some freeware includes advertising.
- A related term, *freemium*, applies when the developers offer the basic version for free, but you have to make an in-application purchase or subscribe to get some features.
- Many paid programs and web, or cloud, apps have a *trial* version. The trial version is usually limited in either time or functionality. If you pay, you unlock the missing features or get permanent access.
- *Commercial* software must be purchased. You pay for it, and then you get access to it. In some contexts, it indicates that software can be used for commercial purposes.
- *Closed source* software applies when the software developers keep the source code and other information about how the software works private.
- *Open source* software means the software's source code is freely available for anyone to copy, modify, and create new versions of the application. Examples of open source software are Linux and OpenOffice.



EXAM TIP The CompTIA IT Fundamentals objectives include comparing open source versus proprietary software as if they are clearly different, but the reality is messy. For the exam, know the following:

- Developers charge money for proprietary software, keep the source code private, and prohibit you from selling or giving away copies of their software.
- You are free to use, modify, and redistribute open source software.

https://t.me/learningnets



EXAM TIP Beyond the exam, know there are *many* software licenses that vary in what they permit and require you to do. They may, for example, require commercial users to pay for a commercial-use license, prohibit commercial uses entirely, require you to publish any modifications you make, and more. In short, always consult the license.

- *Public domain* software isn't owned by anyone. When the original developer releases any claim on it, anyone can do what they want with it. Public domain software is usually (but not always) open source.
- *Proprietary* software is the opposite of public domain. A proprietary application clearly belongs to a company or individual who retains the rights to it, even if they are currently giving it away for free or making its source code available. In practice, proprietary software is usually closed source.

Single and Multi-use Licenses

If you buy software for personal use, you will probably get a *single-user license* that permits you to install the application on a single device or perhaps on a small fixed number of devices.

Schools and organizations can save money by purchasing a *multiple-user license* (also called a *volume license concurrent license*, or *site license*); they can distribute the same software to several users or groups in their network. The organization pays the appropriate licensing and maintenance fees and ensures its users stay within legal bounds.

Multiple-user licensing comes in two main varieties. A *per-seat license* grants permission to install the application on a certain number of computers and has no specifications about how many people can use those computers. A *per-user license* grants permission to a certain number of users, who can use the software on multiple computers.

Product Keys and Activation

When installing an application, you might be prompted for a *product key* or *serial number*, which is a unique string of letters and numbers that identifies your

https://t.me/learningnets

copy of the application. Product keys are common as theft deterrents for high-priced software to prevent people from sharing their copy of the application with others. If you buy the application via download, you will receive an e-mail message containing the product key. Print it, and also keep a digital copy of it. If you buy the application in a retail box, the product key may be on a sticker or card inside or on a sticker on the disc sleeve, USB flash drive, box, or manual.

A product key, by itself, is not an effective theft deterrent, because people can just as easily provide their product key to others along with the setup files. Therefore, after the application setup has completed, you might be prompted to *activate* the software online. Activation locks that particular copy of the application (as indicated by the product key) to a particular computer so it can't be installed on any other computers. Some products that require activation give you a little leeway there, allowing installation on two or three computers before cutting you off.

How does activation work? The actual process is more complex than you probably want to know about, but essentially the setup program examines the computer's hardware components and generates a *hash* (a code created by performing some closely guarded math calculations). It then combines the hash with the product ID to create a unique value and assigns that value to that product key in a database. As a result, that same product key can be reused to install that same software on the same computer again because the hash code will match, but it can't be used on different hardware.



EXAM TIP Be prepared to apply the software-management best practices in this chapter to specific scenarios. These practices include installation and uninstallation, patching and updates, version identification and compatibility, and licensing.

Chapter Review

This chapter looked at how to run applications in Windows, macOS, Linux, and Chrome OS. In Windows the entry point for applications is the Start menu/screen, in macOS it is the Dock or the Launchpad application, and in Linux it is the Dash button or the Terminal window. In Chrome OS, you can click application links in the shelf or open Launcher.

https://t.me/learningnets

It also explains how to install and remove applications. In Windows, the process is different depending on whether it is a desktop application or a Modern app. You can remove desktop applications via the Control Panel; Modern apps are removed from the Start menu/screen. On a Mac, you drag the application from the Applications folder to the Trash. In Ubuntu Linux, you use the Ubuntu Software Center. A right-click and Uninstall in the Launcher gets you there in Chrome OS.

We reviewed common applications and their uses, and you learned about many different file extensions and what kind of applications they are associated with. Along the way, you learned about formats for compressed archives, multimedia clips, and productivity applications.

Finally, we examined software licensing, including freeware, public domain, open source, and proprietary licenses.

Questions

1. Where in Windows 8.1 can you browse installed applications?
   - **A.** Apps list
   - **B.** Dash pane
   - **C.** Dock
   - **D.** Windows Store
2. Where can you see what applications are installed in Ubuntu Linux?
   - **A.** Apps list
   - **B.** Dash pane
   - **C.** Dock
   - **D.** Windows Store
3. How do you install a Modern app in Windows 8.1 or 10?
   - **A.** From the Control Panel
   - **B.** From a downloaded executable file
   - **C.** From the Store app
   - **D.** From the Start menu/screen
4. What is the purpose of an application patch?
   - **A.** Adding new features

https://t.me/learningnets

B. Removing the application
C. Upgrading to a new version
D. Correcting a problem

5. What can you find out about an application by choosing Help | About?
A. Most recent data file used
B. Supported extensions
C. Application version number
D. Windows version

6. How can you remove a Windows desktop application?
A. From the Control Panel
B. From the Store app
C. From the Start menu/Start screen
D. From the Dock

7. Which of these is a graphic format?
A. PNG
B. PPTX
C. AVI
D. TAR

8. Which of these is a productivity application?
A. Microsoft Excel
B. *Candy Crush*
B. Windows Firewall
C. Spotify

9. Which of these is a collaboration application?
A. TurboTax
B. Microsoft Word
C. SharePoint
D. Symantec Endpoint Protection

10. Which of these is a compression format?
A. WAV
B. TXT

https://t.me/learningnets

C. XLS

D. RAR

Answers

1. **A**. In Windows 8.1, open the Start screen and then click the down arrow to view the Apps list, which shows all installed applications. The Dash pane is in Linux. The Dock is in macOS. The Windows Store is for acquiring new apps, not viewing existing ones.
2. **B**. The Dash pane shows installed applications in Linux. The Apps list is in Windows 8.1 and Windows 10. The Dock is in macOS. The Windows Store is not in Linux.
3. **C**. Modern apps come from the Store app. The Control Panel is not a common place to install software. A downloaded executable would be for a desktop app, not a Modern app. The Start menu/screen shows already installed apps.
4. **D**. A patch corrects a problem. New features and new versions are not provided in a patch. A patch does not remove the application.
5. **C**. Help | About will tell you the application's version number in many applications. It does not report the most recent data file, supported extensions, or Windows version.
6. **A**. Remove a desktop application from the Programs section of the Control Panel. The Store app installs applications; it doesn't remove them. The Start menu/Start screen could be used to remove a Modern app, not a desktop app. The Dock is used in macOS.
7. **A**. PNG is a graphic format, PPTX is a PowerPoint data file, AVI is a video file, and TAR is a compressed archive file.
8. **A**. Excel is a productivity application, used for spreadsheet creation. *Candy Crush* is a game. Windows Firewall is a utility. Spotify is a music player.
9. **C**. SharePoint is a collaboration application. TurboTax is a personal finance program. Microsoft Word is a productivity application (a word processor). Symantec Endpoint Protection is a utility.
10. **D**. RAR is a compression format, WAV is an audio format, TXT is a text file format, and XLS is a spreadsheet format.

https://t.me/learningnets

PART III

Networking, Security, and Maintenance

- **Chapter 10** Configuring Network and Internet Connectivity
- **Chapter 11** IT Security Threat Mitigation
- **Chapter 12** Computer Maintenance and Management
- **Chapter 13** IT Troubleshooting

https://t.me/learningnets

CHAPTER 10

Configuring Network and Internet Connectivity

In this chapter, you will learn how to

- Understand basic network terminology
- Choose, set up, and configure a small office/home office (SOHO) router
- Choose between wired, WiFi, cellular, and satellite connectivity
- Use a LAN to share files and printers

Few computers are islands unto themselves. To experience the full power of computers, you must connect them to other computers. Imagine you receive a new computer, but it's not on a network, so you can't share work documents, send e-mail, download music, or interact across the Internet with your friends. How boring would that be?

When you link computers to share files and communicate, you create a *network.* Network devices use addresses to transmit packets containing data among one another. Networks range in size from two computers connected together to the largest and most complex network of all—the Internet.

In this chapter, you will learn the basics of home networking. You'll learn how to choose and configure a router, share files and printers on a network, connect to the Internet, and share data online.

Understanding Network Basics

Networks come in many sizes and vary widely in the number of computers attached to them. Some people connect two computers in their house so that they can share files and play games together—the smallest network you can have. Some company networks connect thousands of employees in dozens of countries to get work done.

https://t.me/learningnets

LANs and WANs

Network folks put most networks into one of two categories: LANs and WANs.

A *local area network* (LAN) covers a small area, where all the computers connect via cables, wireless signals, or a combination of the two, through connecting boxes (Figure 10-1). LANs usually cover a single building or group of nearby buildings. Typical LANs include home and small office networks. A *wireless local area network* (WLAN) is a LAN that connects components wirelessly.

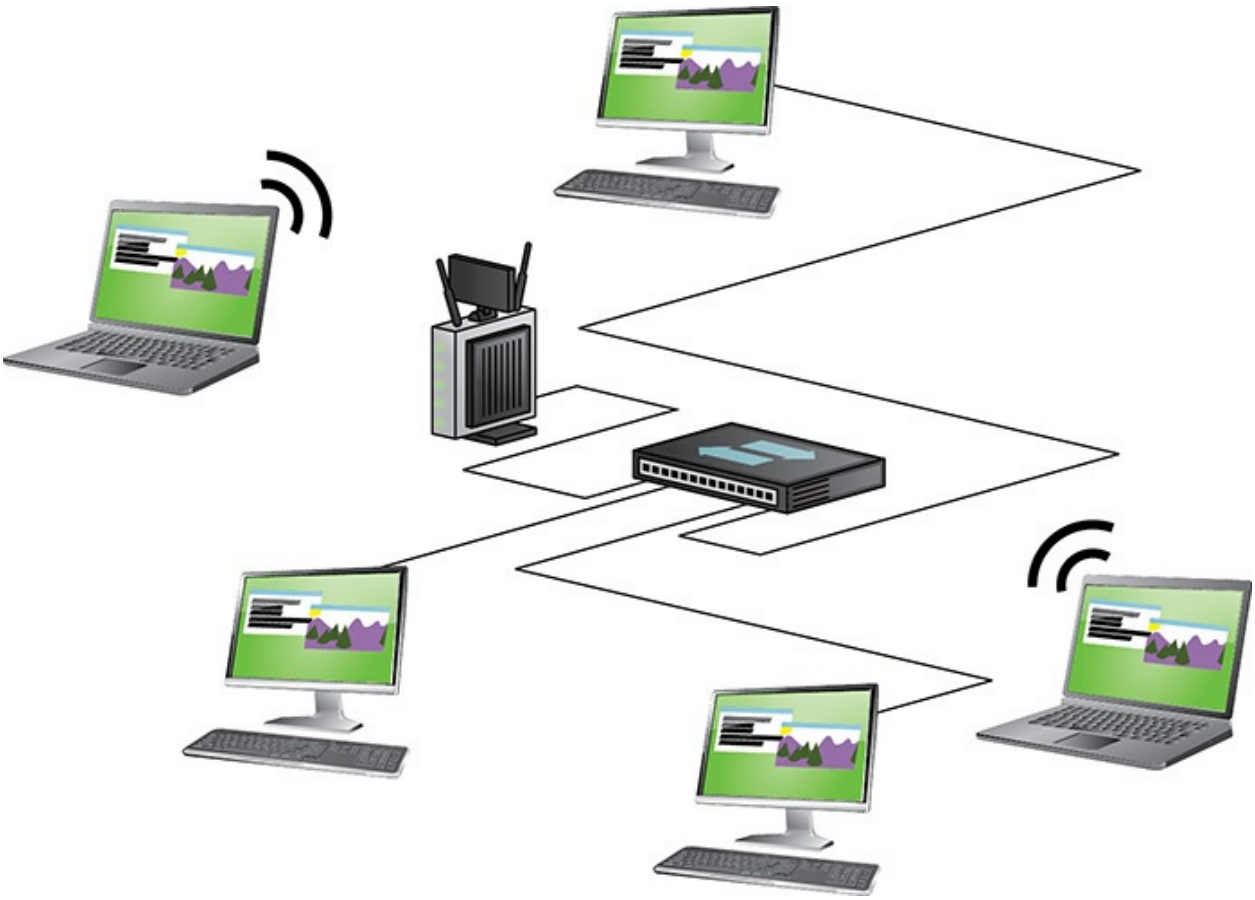


Figure 10-1 A local area network

A *wide area network* (WAN) covers a large area and can have a substantial number of computers (Figure 10-2). Usually, a WAN is composed of two or more LANs connected together. All the LANs in all of the schools in your district, for example, might link together to form a WAN. The largest WAN in existence, the *Internet*, is a worldwide network that connects millions of computers and networks.

https://t.me/learningnets

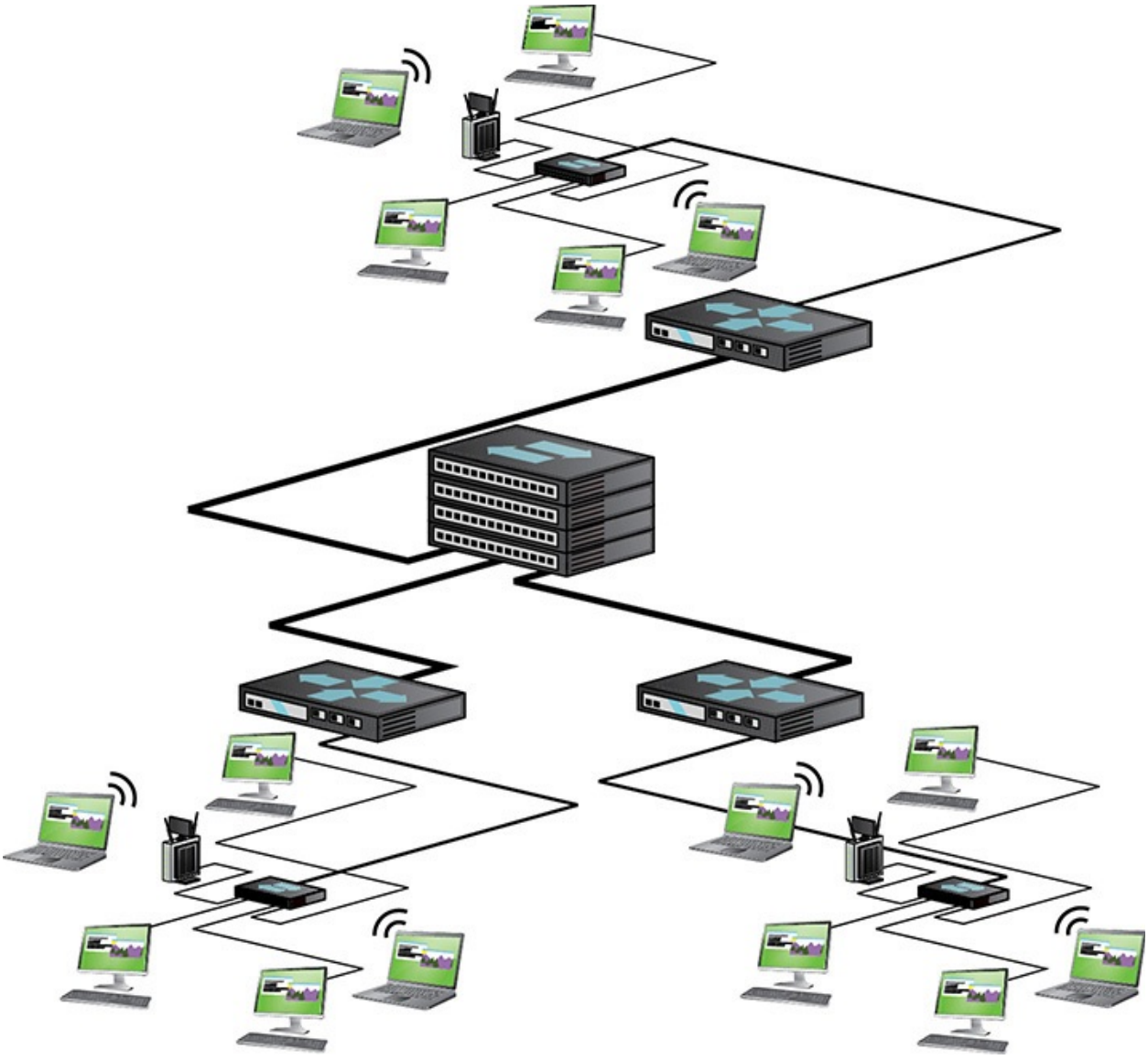


Figure 10-2 A wide area network

Clients and Servers

People use two kinds of computers on a network: clients and servers. In a nutshell, *servers* share things such as files, folders, and printers, and *clients* access those shared things (Figure 10-3). One of the most common client computers is a *workstation*, which is a PC or macOS box that handles general computing chores. Smartphones, depending on which apps are installed and how they are used, can also be considered workstations. Almost any personal computer can serve as either a client or a server. Microsoft and other developers also make server-specific operating systems, such as Windows Server.

https://t.me/learningnets



Figure 10-3 Client and server interaction

Computers running Windows, macOS, and the many varieties of Linux make up the vast majority of clients. You'll also find other client devices, though, such as game consoles, smartphones, tablets, and digital video recorders (DVRs). Servers manage network resources (such as printers, e-mail, and other stuff that makes a network valuable), provide central storage of files, and provide services for the users (such as having the print server tell the printer to print or having the e-mail server send your e-mail).

Networks are traditionally classified into *client-server* or *peer-to-peer,* depending on the role played by each computer in the network. In a client-server network, one or more computers act as servers while the remaining computers act as clients. An example of a client-server network is a corporate network at a large company, where IT professionals maintain multiple servers that provide the individual computers that the employees use (the client computers) with a variety of services.

On some home or small office networks, however, there may not be a separate server. Instead, every computer on the network acts as both a client and a server. Each computer mostly does its own client thing, functioning as a normal computer, and also shares resources with the other computers on the network. Such networks are called *peer-to-peer networks*. An example of a peer-to-peer network is a network in a residence that allows five computers and two smartphones to all share the same printer and Internet connection. A *SOHO network* is a small network operated in a home or a small business.



https://t.me/learningnets

NOTE An online peer-to-peer network temporarily connects multiple client computers for a specific purpose, such as sharing music or video files. When you participate in peer-to-peer file sharing online, you are part of an online peer-to-peer network. Because of copyright restrictions, much of the activity in online peer-to-peer file-sharing systems is illegal.

Switches and Routers

In a LAN, each computer connects to a central gathering point, either using a cable or wirelessly via radio frequency (RF) signals. Wired LAN computers connect to a *switch*; wireless LAN computers connect to a *wireless access point* (WAP). Many SOHO networks use a box that combines both connection options (see Figure 10-4). The switch or WAP keeps track of the computing devices on the network and makes sure network traffic gets to the proper computer.

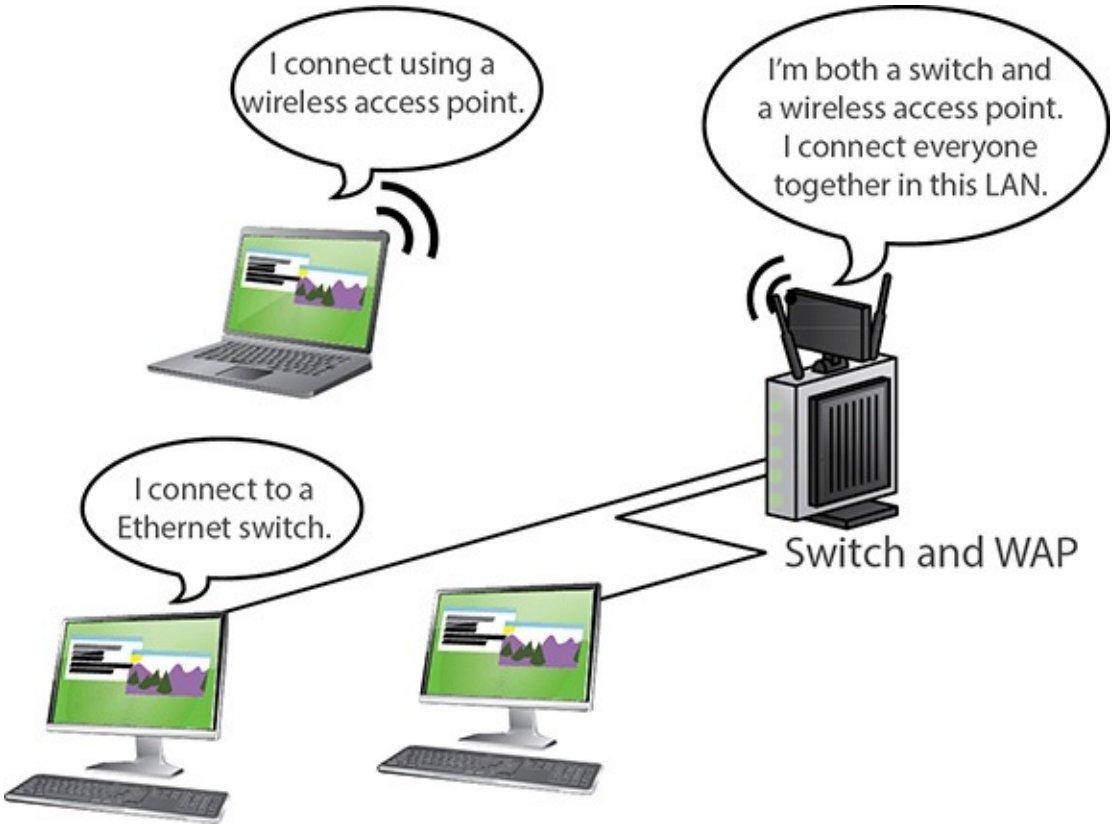


Figure 10-4 A SOHO LAN with both wired and wireless clients

A *router* connects two or more networks directly, depending on the number of router interfaces. Depending on their configuration, routers can indirectly send

https://t.me/learningnets

network traffic to other remote networks that could be located anywhere on the planet. Connecting a SOHO LAN to the Internet therefore requires a router. The router acts as a gateway between the LAN and the *Internet service provider* (ISP) that provides that essential Internet connection. Most SOHO networks use some kind of *broadband* connection, such as a cable modem, to make the high-speed connection between the router and the ISP. Figure 10-5 shows a simplified LAN connection to an ISP and then on to the Internet.

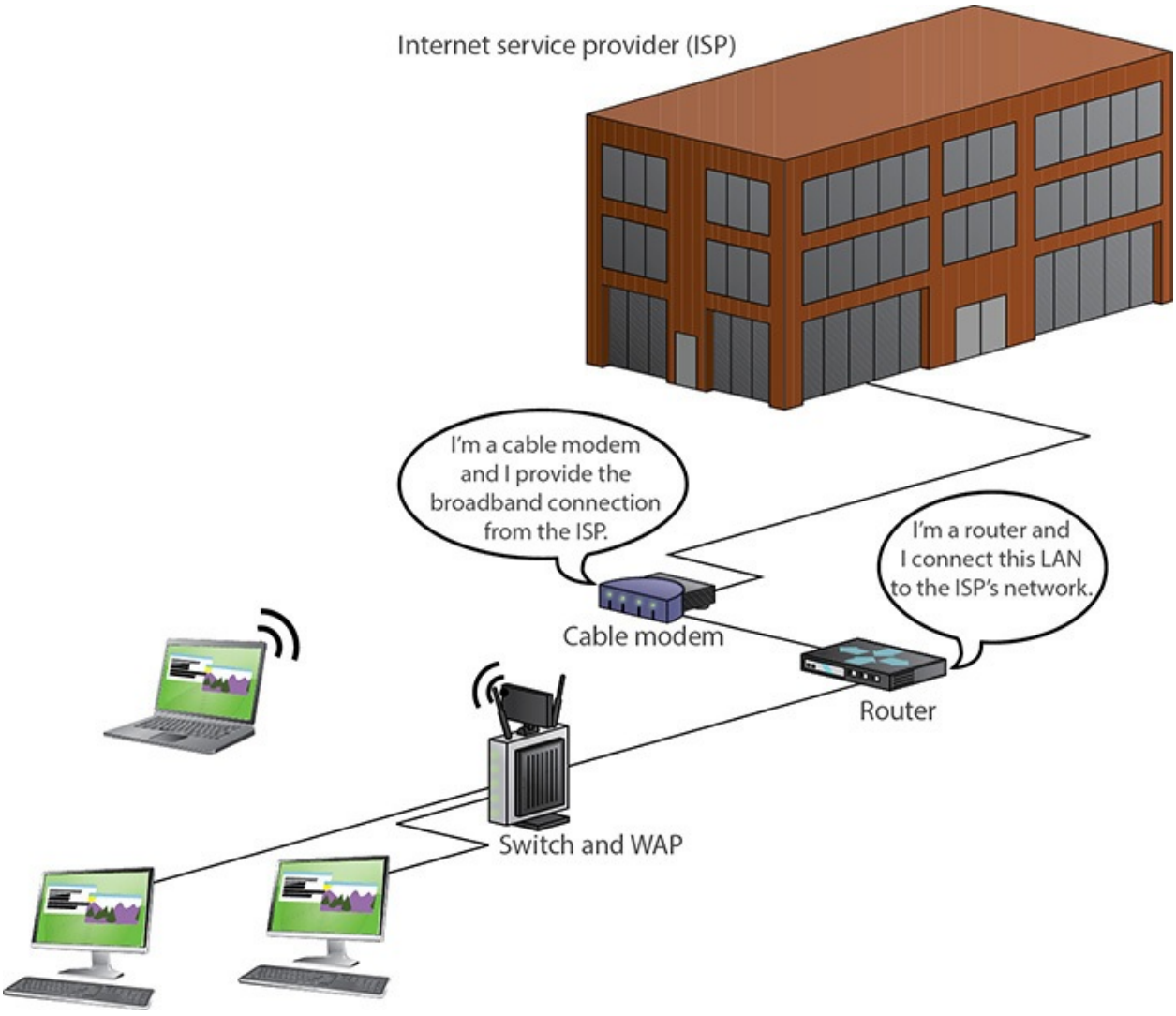


Figure 10-5 Adding a connection to an ISP

A typical SOHO LAN that connects to the Internet, therefore, has five types of devices. Here's the list:

https://t.me/learningnets

- Workstation or other computing device that people use to connect and do work.
- Switch that enables the wired connections among devices so that a LAN happens.
- WAP that enables the wireless connections among devices so that a LAN happens. Remember, the WAP can also be the wired network switch at the same time.
- Router that provides the connection between the LAN and another network, specifically the Internet service provider. This device can also be a WAP and switch all at the same time.
- Broadband box (cable or other) that provides the physical connection between the router and the ISP. This can also act as the router, WAP, and switch all at once.

At this point, the consumer labeling of devices can cause a little confusion. Most SOHO users have a *single* magic box that does it all—switch, WAP, router, and broadband connection rolled into one (Figure 10-6). Worse, most people call this magic box a *SOHO router* or *broadband router*. As a CompTIA IT Fundamentals student, you need to understand the functions that make the magic box work at each level. Switches and WAPs create LANs. Routers connect networks. Broadband devices provide the physical connection for the router to the ISP.

https://t.me/learningnets

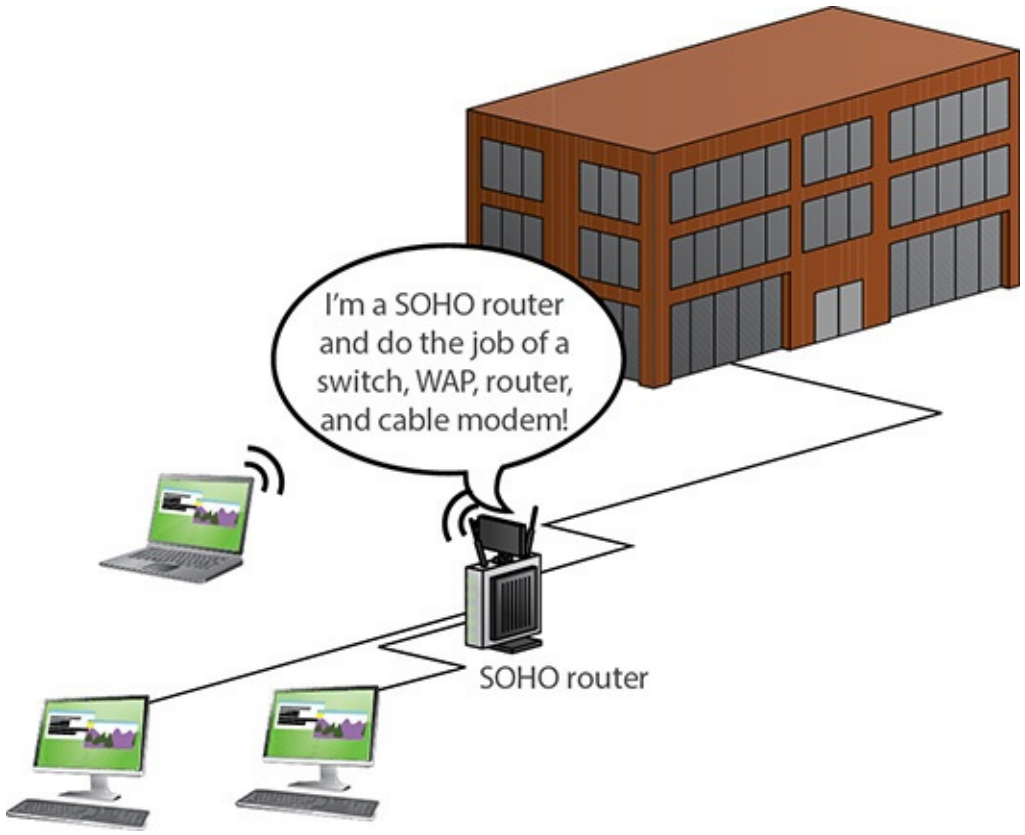


Figure 10-6 A switch, WAP, router, and broadband connection rolled into one magic box



EXAM TIP Connecting computers to a switch or WAP creates a LAN. Connecting two or more LANs with different network addresses requires a router.

Local Ad Hoc Networks and Direct Links

You can join a few computers in a direct connection without going through a connecting device such as a WAP. This is called an *ad hoc network*. An ad hoc network is typically wireless (WiFi). Although you could set up this type of network in Windows 7 and earlier, security risks led Microsoft to remove the option of setting up an ad hoc network in Windows 8 and newer. It is technically still possible to do in Windows 8 and newer, but it involves typing long strings

https://t.me/learningnets

of commands at a command prompt and is best left to computer professionals and technical enthusiasts.

A *direct link* connection (PC to PC) is a one-to-one connection between two computers via their Ethernet ports. It is technically a kind of ad hoc network (in that there is no central gathering point like a switch), although it's not usually called that. To create a direct link, you need a specially wired *crossover cable*.

Setting Up and Configuring a SOHO Router

Most SOHO routers work pretty well right out of the box, but you should check basic configuration options to ensure proper security. Security is important on a router to keep would-be hackers from spying on your computer usage and stealing your Internet bandwidth. Follow along with the upcoming sections to learn how to make your SOHO router work just the way you want it to work.



NOTE Many Internet service providers lease equipment to customers that is both a modem and a wireless router. The modem portion provides the Internet connection, and the router portion creates a small LAN and allows all the computers on the LAN to share the Internet connection. If you have one of these combo boxes, you might not have to go through most of the activities outlined in the upcoming sections. Just follow the advice of your ISP and you will likely be good to go.

Choosing an Appropriate Router

There are two main considerations when choosing a SOHO router. The first is whether it should support wireless connections. This isn't a difficult question—the answer is almost always *yes, it should*. Even if you don't have any wireless devices right now, you might have some in the future, or a guest in your home or office might have one. A typical wireless SOHO router also supports wired (cable) connections, usually at least four ports, so it's not an either-or proposition.

Second, you should determine which wireless standard the SOHO router supports. New wireless routers you buy today will almost all support the 802.11ac standard, which is the newest one, although the 802.11 WiFi standards are constantly evolving. If you pick up a secondhand wireless router or buy one

https://t.me/learningnets

on clearance, it might support an older standard, like 802.11n or 802.11g. Those are okay, but you won't achieve the same data speeds with the older models.

Setting Up a SOHO Router

Follow the instructions that come with the SOHO router to set it up physically. This usually involves plugging it into a wall outlet and placing it in a location reasonably near where the wireless devices will be. Some lights will flash on it, and after a minute or two it will be ready for use.



TIP In most cases, a SOHO router will work right out of the box with its default settings. You should still go through a configuration process to enhance its security.

Making a Wired Connection

To configure most SOHO routers, you will need either to connect a computer to it with an Ethernet cable or to connect using a web browser to the router's default IP address on its own default wireless network; check the router instructions to determine how to do this. For a wired connection, you must use a computer that has an Ethernet port (an RJ-45 port). There are USB-to-Ethernet adapters that may work in a pinch, but it's better and easier to use the Ethernet port.

Connect one end to the computer's Ethernet port and the other end to an Ethernet port on the back of the SOHO router. There should be several generic-looking Ethernet ports there and one special one (perhaps a different color or with a label like "Internet"). Use any of the generic-looking ports. See Figure 10-7.



https://t.me/learningnets

Figure 10-7 Connect a computer to any of the four Ethernet ports.

Checking for Basic Internet Connectivity

If you plan to use the SOHO router for Internet access, connect the Internet to the SOHO router. Do this by running an Ethernet cable from the broadband box (which is often called a *modem*) to the special port on the SOHO router. This may be labeled "Internet" or "Modem" or have some such wording. This port may be a different color than the others or be offset from the others. Make sure you connect to this special port and not one of the generic ones. This step isn't necessary if the broadband modem is also a SOHO router.

To verify your connection, try accessing any web site with a web browser. If you get Internet access, great! It'll make it possible for you to check for firmware updates, which you'll do later in this chapter. If not, don't sweat it for now. If you still don't have Internet connectivity after you complete the configuration process, check with your ISP to see what extra steps you might need to take.



EXAM TIP For Objective 2.8 of the CompTIA IT Fundamentals exam, make sure you know how to verify wireless Internet connectivity; open a web browser and try to display a web page.

Accessing the SOHO Router Configuration Utility

Read the documentation that came with the SOHO router to find out how to access its configuration interface with your browser. The process probably involves the following:

1. Connect a computer to the SOHO router with an Ethernet cable. Follow this step even with a computer that will connect to the SOHO router wirelessly in the future.
2. Look up the SOHO router's default IP address in the documentation. The *IP address* functions as the unique name for that device. It will probably start with 192 and be something like this: 192.168.1.1 (see Figure 10-8). If you don't have the documentation, find the documentation online to get

https://t.me/learningnets

this information.

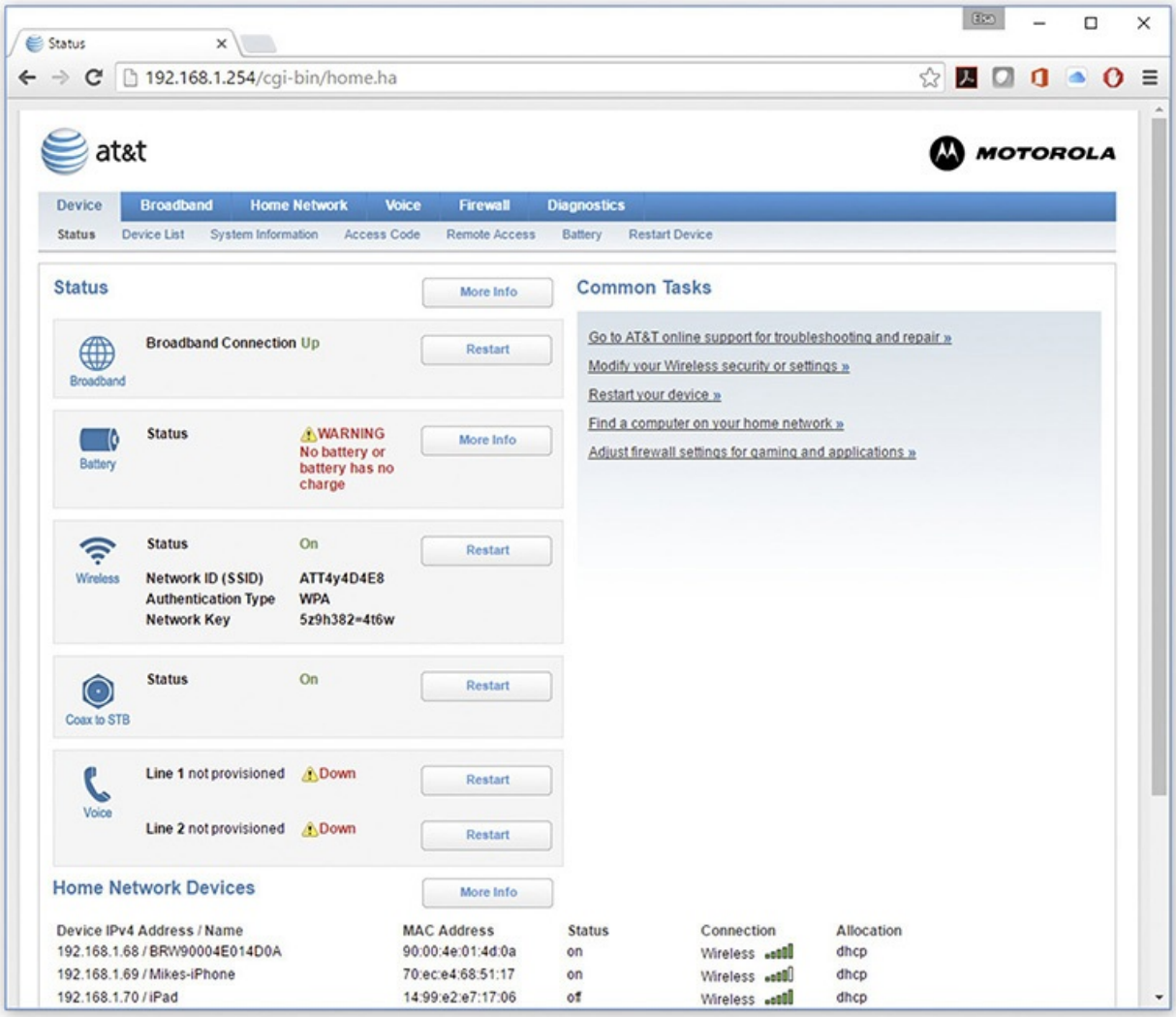


Figure 10-8 Configuration interface for a combination broadband modem/wireless router

3. Open a web browser, click into the address bar, type **http://** followed by the SOHO router's IP address, and press enter. The SOHO router interface should open as a web page.

The configuration interface will vary by SOHO router make and model. Figure 10-8, for example, shows the interface for a combination AT&T broadband modem and wireless router, while Figure 10-9 shows the interface for an older Belkin wireless SOHO router.

https://t.me/learningnets

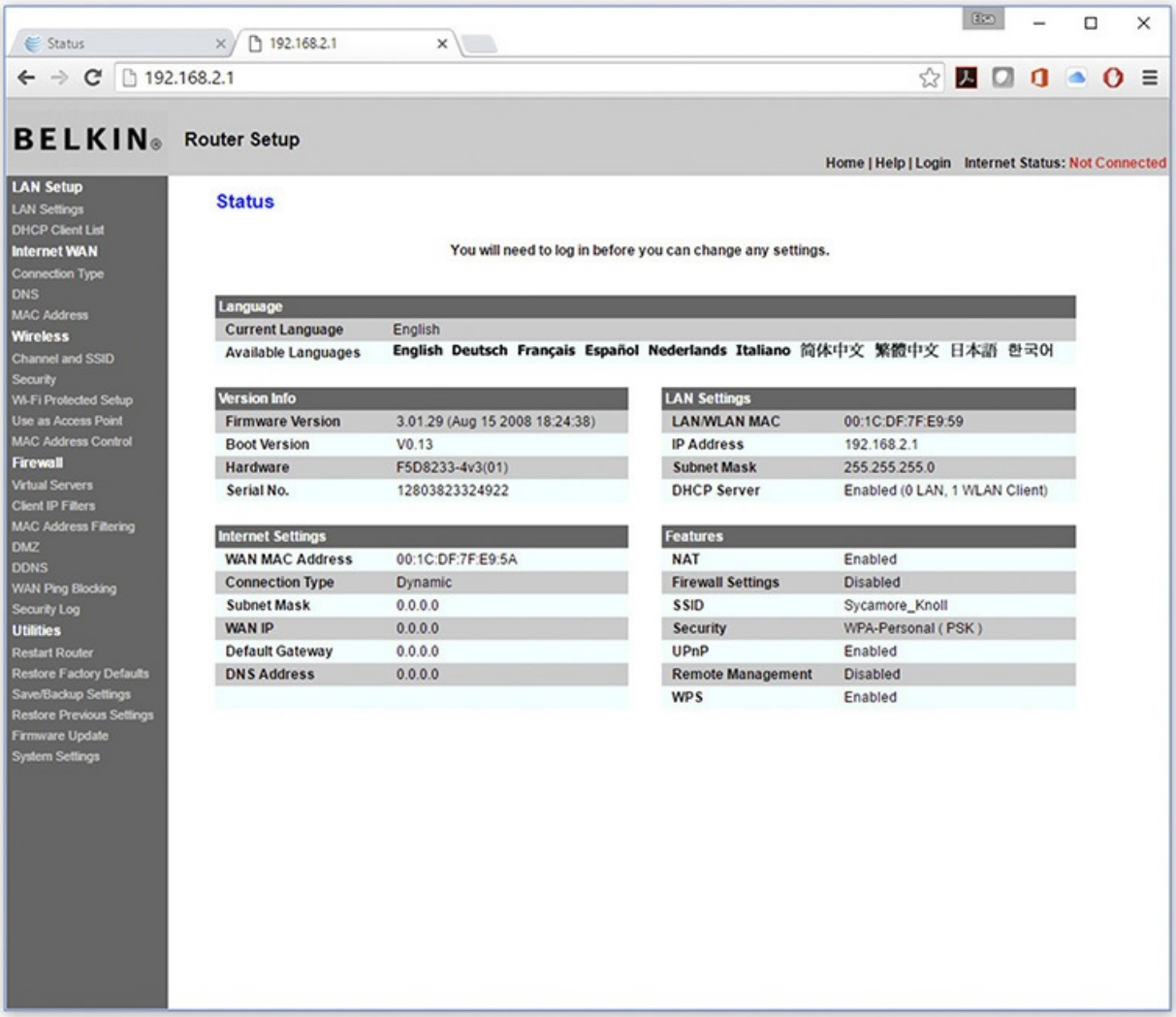


Figure 10-9 Configuration interface for a wireless router

Logging In and Changing the Password

Before you can change any settings, you will need to log in to the SOHO router. If it's a new SOHO router, look up the default user ID and password in the documentation if you are prompted for that information. If it's not new but you don't think anyone has changed the password yet, look up the router's documentation online to find out the default information. If it's already been changed, you'll need to know the current password to continue.

https://t.me/learningnets



TIP If you can't find the SOHO router's password anywhere and it's been changed, you'll need to do a hard reset of the router to reset the password to the default. Look at the router documentation online to find out how to do this, as the process varies.

The login screen in Figure 10-10 has a hint that the router's default password is blank. In other words, just click Submit without typing anything.

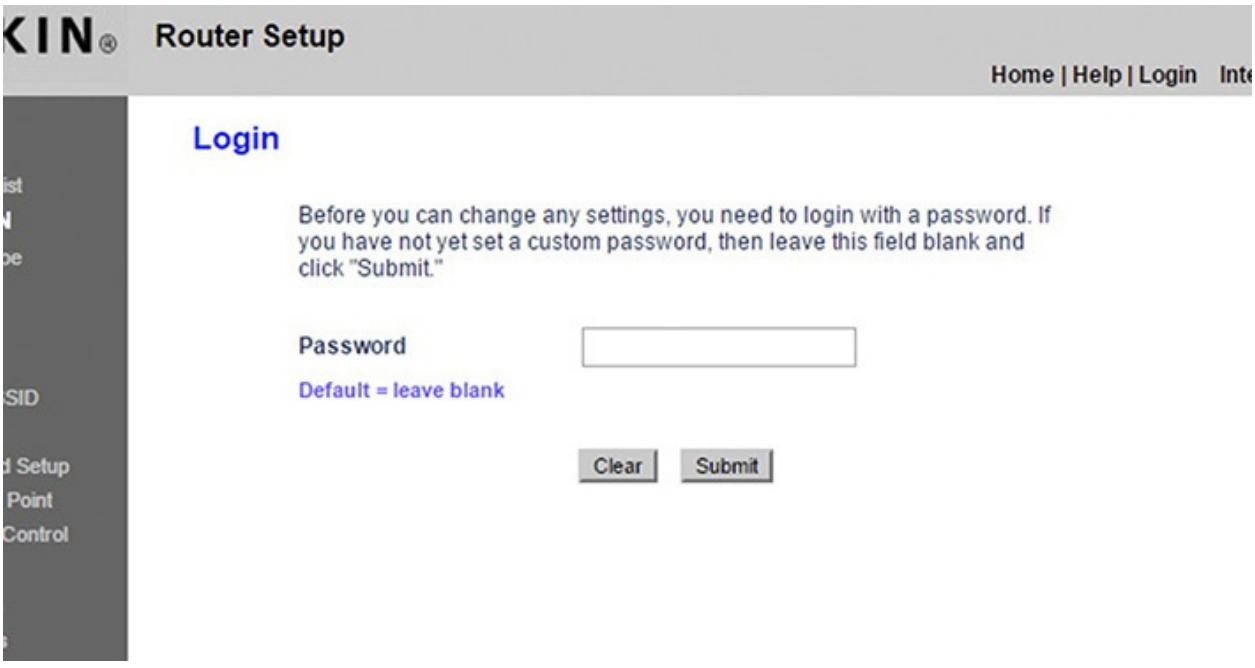


Figure 10-10 Login screen with a hint about the default password

A blank password does not provide good security, especially when the login screen provides a helpful hint. So, first change the password. The process depends on the interface. Check the router's documentation or look for a Help command in the configuration interface. This setting is called Administrator Password on the router in Figure 10-11; it's found in Utilities | System Settings. The Login Timeout setting determines how long your configuration session can be idle before you have to log in again.

https://t.me/learningnets

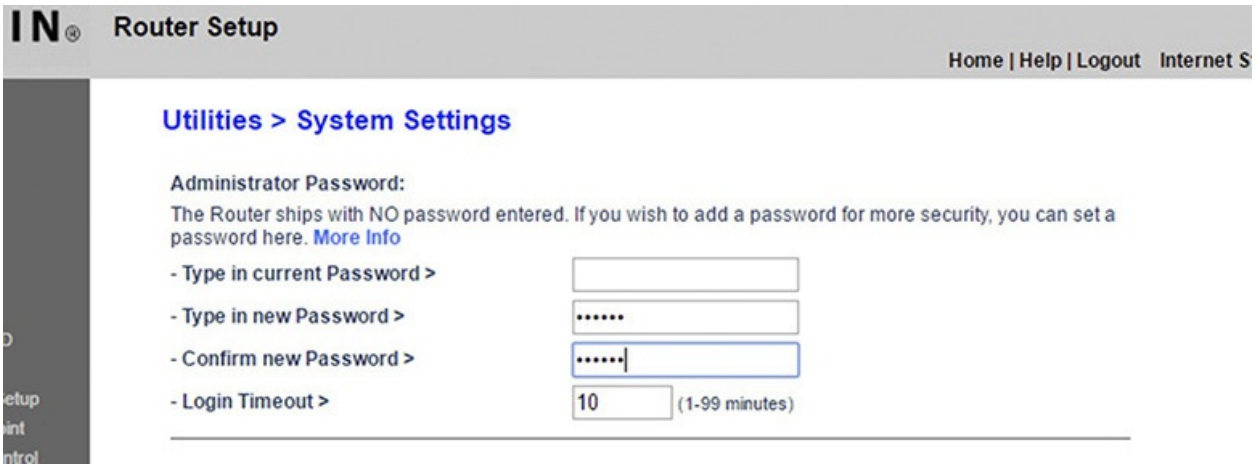


Figure 10-11 Change the password to prevent unauthorized access to the configuration utility.

Updating the SOHO Router Firmware

Before you get too far into SOHO router configuration, you should check for updates to the router's firmware. Firmware, as you may recall from earlier chapters, is programming stored on a chip inside the device to perform the device's basic functions. The configuration utility itself is stored in firmware, for example, as is the software that the SOHO router uses to start up and do its job.



NOTE You might have to postpone the firmware update if the SOHO router isn't connected to the Internet yet, but familiarize yourself with the button's location and come back to it when you can.

Look in the configuration program for a Firmware Update button or hyperlink. If an Internet connection is available, click Check Firmware and then follow the prompts to install an update if one is found. See Figure 10-12.

https://t.me/learningnets

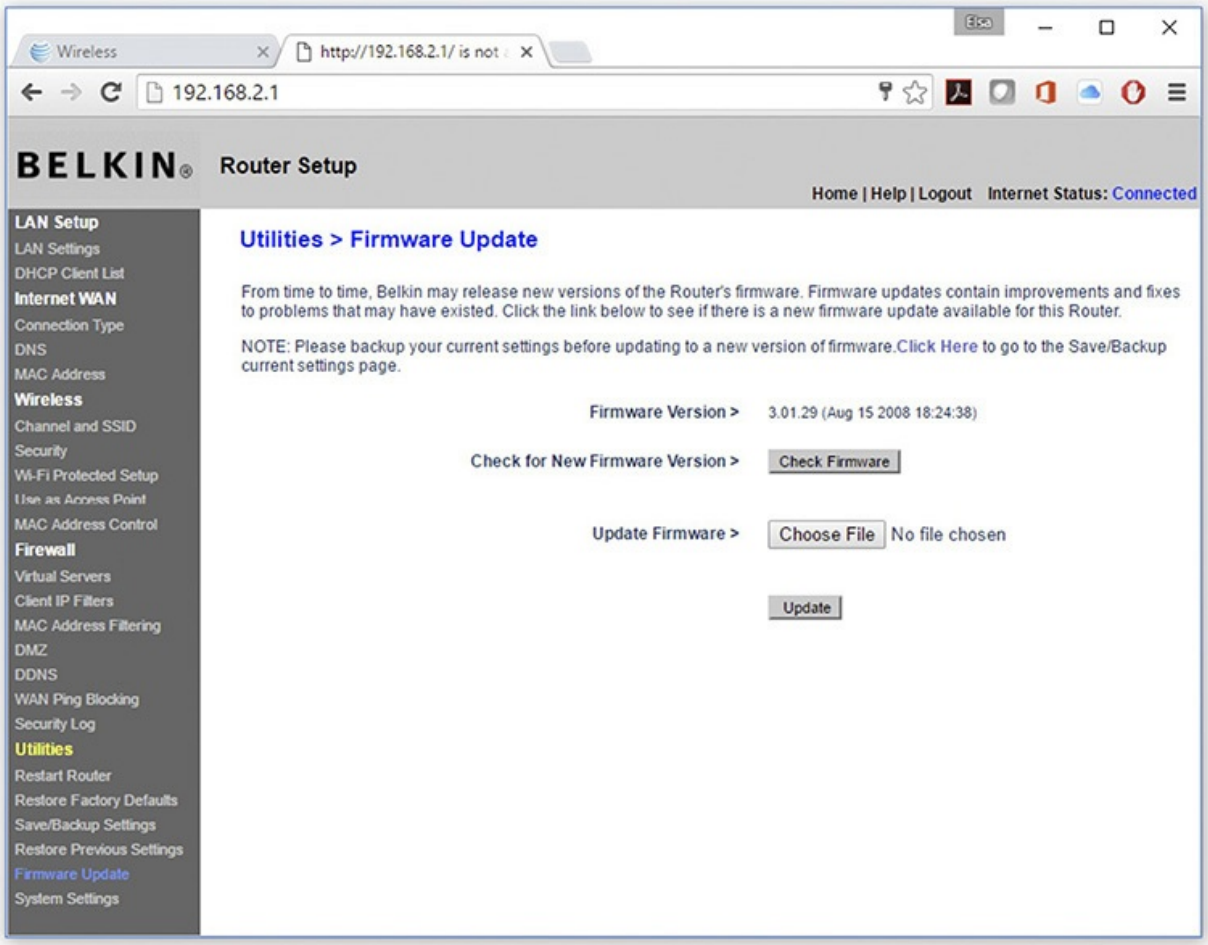


Figure 10-12 Update the firmware if an update is available.



EXAM TIP Because the procedure for updating firmware varies among SOHO routers, you don't need to know the specific steps; however, you should understand why router firmware should be updated and how to find the button or hyperlink to accomplish an update in the router's setup utility.

Changing the SSID

The *service set identifier* (SSID) is the name wireless users see when they browse available wireless networks. The SOHO router's default SSID might be the manufacturer's name, for example. You can change the SSID to something

https://t.me/learningnets

more memorable that will help you and your friends find the SOHO router easily even if there are multiple wireless routers in the vicinity (such as in an apartment building). However, if you change the SSID to, say, “Board Room A – Acme Bank,” the downside is that anybody in close proximity will see the SSID and know what it is—assuming you named it for what it really is, of course!

Depending on the name, changing the SSID can offer some basic security because it gives away less information about your router type, which makes it harder to determine default settings and any vulnerabilities it may have. Many default SSID names and administrator passwords, for example, are well-known and widely available online.



NOTE You can also configure most wireless routers to allow administrative access only through a wired connection rather than wirelessly. If you limit access to the physical router, this adds another layer of security to the wireless network.

To change the SSID, look for that setting in the configuration utility (in Figure 10-13 it is located under Wireless | Channel and SSID).

https://t.me/learningnets

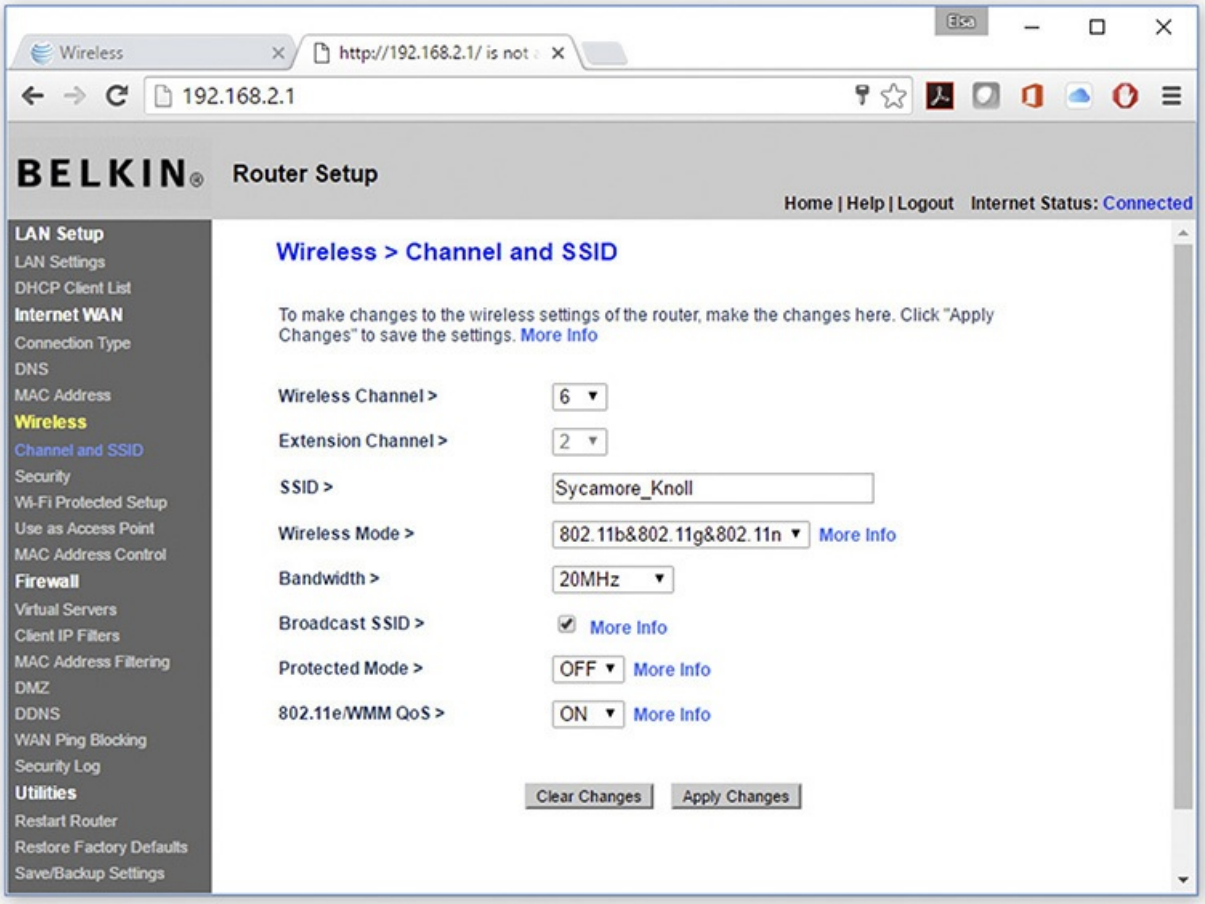


Figure 10-13 Change the SSID.

Setting Up Wireless Security

Wireless security refers to a system of authentication for the wireless clients that connect to the SOHO router. If a router's security is set to Open, that means it has no security. Anyone with a computer with WiFi can connect to the SOHO router and use the resources on the network. Unless you *want* to provide free Internet access to the public, having an open wireless SOHO router is a bad idea, especially if you share files on your network. It's an open invitation to hacking.

In the Security section of your SOHO router's configuration utility, you can select a security mode. You will see several options, such as WEP, WPA, and WPA2.

WEP

Wired Equivalent Privacy (WEP) encryption was meant to secure data

https://t.me/learningnets

transmitted wirelessly. WEP encryption uses 40-bit encryption (that is, a 40-digit coding system of ones and zeros) to scramble data. Many vendors also support 104-bit encryption.

WEP has some serious security flaws. Shortly after it was released, hackers demonstrated that WEP could be cracked in a matter of minutes using software readily available off the Internet. WEP is better than nothing, but it will not deter any serious hacker. The industry quickly came out with a replacement called WPA.

WPA and WPA2

Wireless Protected Access (WPA) encryption addressed the weaknesses of WEP, and it functions as a sort of security protocol upgrade for WEP-enabled devices. WPA offers security enhancements such as an encryption key integrity-checking feature and user authentication through the industry-standard *Extensible Authentication Protocol* (EAP). The use of EAP is a huge security improvement over WEP. Usernames and passwords are encrypted and therefore much more secure. WPA uses an encryption standard called *Temporal Key Integrity Protocol* (TKIP).

Wireless Protected Access 2 (WPA2), the most secure authentication method for a SOHO wireless network, offers additional benefits over WPA, making WPA2 the strongest available encryption today. WPA2 uses an improved encryption standard called *Advanced Encryption Standard* (AES). You don't need to know the technical details of the differences between TKIP and AES.

There might be some options available with WPA2, depending on your router. For example, one of the choices might be *WPA2 – Default Key*. The default key is a pre-assigned password for the router that is difficult to guess, usually a long random string of numbers, letters, and symbols. This is the default option on most modem/router combinations because it's extra-safe—there are no easy-to-guess passwords. The drawback is that every time a new user needs to access the router, you have to look up its password because there's no way anyone can remember it.

An alternative, WPA2-PSK (PSK stands for "preshared key"), uses a password (or key) you specify and share with people who need access. The drawback is that most people don't make this password strong enough. Use a combination of letters, numbers, and symbols that is easy to remember but difficult to guess. See the section "Authenticating Users" in Chapter 11 for more information about selecting strong passwords.

https://t.me/learningnets



NOTE The WPA3 wireless security standard was certified by the Wi-Fi Alliance in 2018. Expect to see more vendor support for this in the near future.

Setting Up Security

In the router's configuration utility, open the Security section and choose a security mode. You might also be prompted to choose an authentication type or encryption technique. In most cases, the best choice is WPA2-PSK with AES as the encryption technique, as in Figure 10-14.

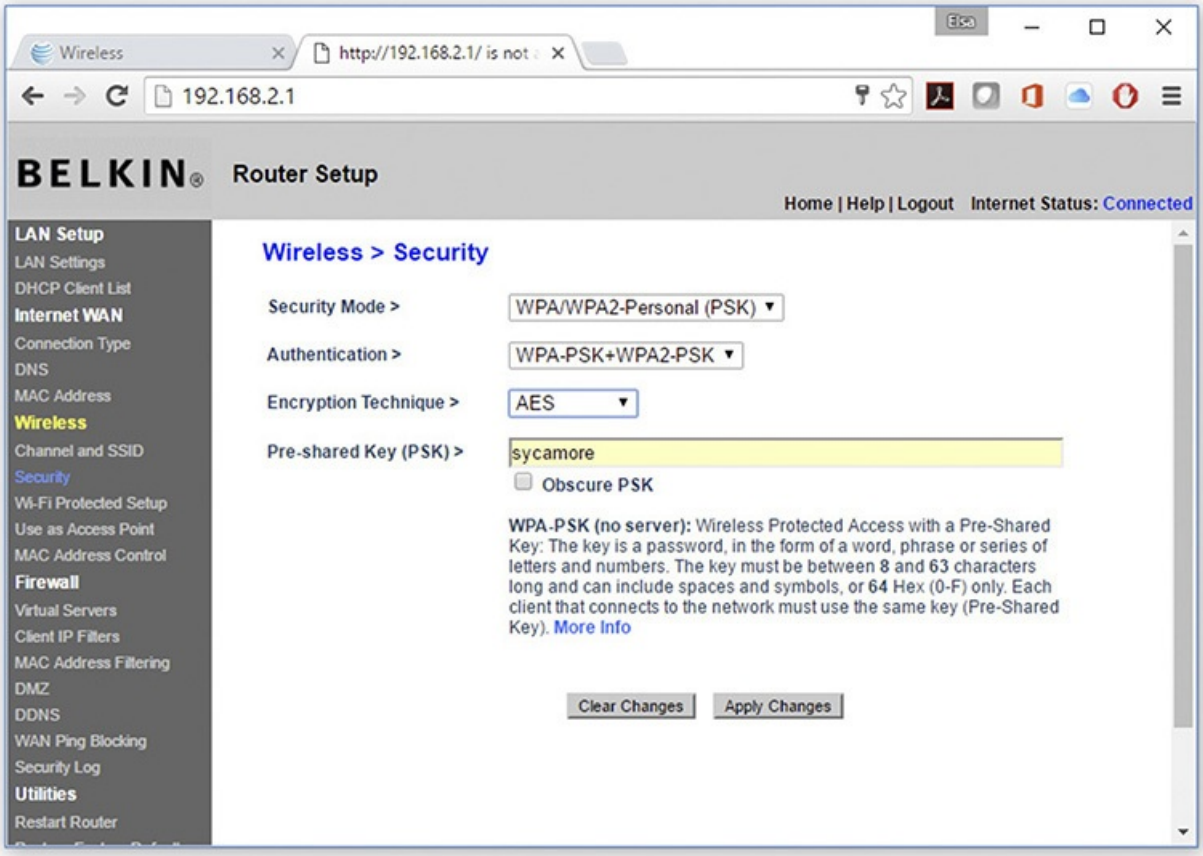


Figure 10-14 Choose a security mode and encryption technique.

WPS

The easiest way to set up a client to access a secured router is with *Wi-Fi Protected Setup* (WPS). There are a few different WPS methods; the method you

https://t.me/learningnets

use depends on the device's capabilities. With push-button configuration (PBC), you push a button on the router to place it in a special mode where it accepts new connections for a brief time. During those few minutes anyone can connect wireless devices to the router without knowing its password. The device and the router come to an understanding, and the device is approved for future use of the router. Not all routers support WPS, but many of the SOHO routers sold today do.

A second WPS method requires a device to enter a personal identification number (PIN) to join the network. The SOHO router might have a PIN sticker, or it may generate a different PIN each time. The third WPS method uses *near-field communication* (NFC), which is a very short-range wireless networking technology that allows devices to connect when they are within a few inches of each other. Chapter 9 discussed NFC.

You can enable or disable WPS. Find the WPS setting in the router's security properties and choose Enabled or Disabled.

When you finish configuring the router, close the browser window to exit the configuration utility.



EXAM TIP Make sure you know how encryption options rank from least to most secure (in order, WEP, WPA, WPA2) and how to differentiate them from WPS. In practice, use WPA2 if at all possible.

Connecting Wireless Clients

The last step in setting up a SOHO router offers the most benefit: enabling wireless clients to connect and become part of the LAN. You learned earlier in the chapter how to connect a wired client—run an Ethernet cable between the back of the router's switch ports and the Ethernet port on the computer. The setup for a wireless client, however, requires a few steps.



CAUTION Anyone with an Ethernet cable can walk right up to a SOHO

https://t.me/learningnets

router and connect a computer to your network; router security applies only to wireless connections. Therefore, you should lock up your router if it's in an environment you don't trust or can't control.

On a Windows desktop or laptop computer, you can view the available wireless networks by clicking the network icon in the notification area. Then click the desired SSID to connect to that router and click Connect. See Figure 10-15. If the router is open (insecure), you'll be connected automatically. If it has security enabled, the first time you connect to the router you'll be prompted to enter the password (or preshared key).

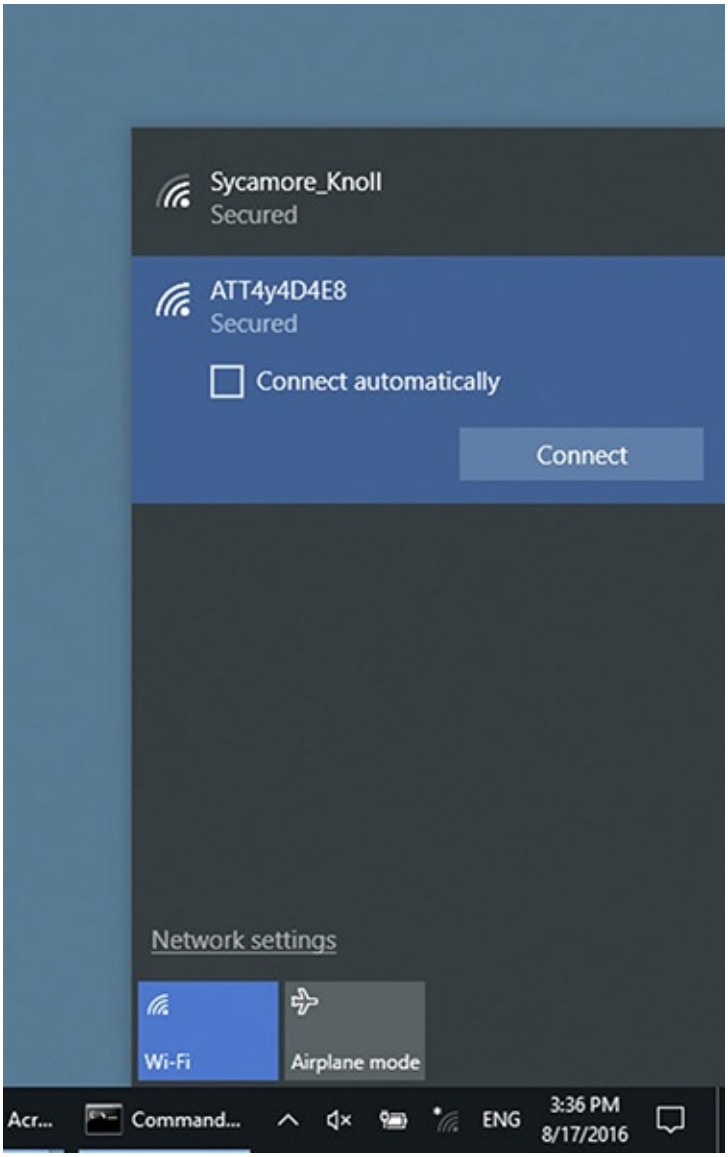


Figure 10-15 Select the desired wireless network to which to connect.

https://t.me/learningnets

Wired, Radio Frequency, Satellite, and Cellular: Making the Right Choice

You just learned how to set up a SOHO router, which can act as an on-ramp to the Internet if you connect a broadband modem to it (or if the broadband modem is built into it). You also learned that you can access that router via a wired connection or wirelessly. These two methods aren't equal. There are benefits and drawbacks to each.

Let's also throw a third and fourth option into the mix for Internet connectivity: *cellular* and *satellite*. You can connect to the Internet via smartphones or tablets that have cellular service, as an alternative to using a broadband Internet connection in your home or office. You can also buy a cellular modem that connects to a desktop or laptop computer to allow you to access the Internet via the same cellular data network that smartphones use.

Internet connectivity can also occur through satellites orbiting the Earth. In remote locations, during flights, or when at sea, indirect access to the Internet through satellites is common. The satellites connect to *network operation centers* (NOCs), which are terrestrial networks that satellites connect to on Earth. Satellite Internet connectivity providers will give customers a *committed information rate* (CIR); this is the guaranteed lowest speed that can be expected. Internet speeds through satellites vary depending on the provider and how much you're willing to pay. As long as you can compare network transmission rates between various wireless connection types, such as 5 Mbps versus 100 Mbps, you'll be able to determine the best fit for your needs and budget.

Let's examine each of these methods, focusing on costs and benefits, so you can make the right choice in a given situation. This section tackles these seven things to consider:

- Mobility
- Availability
- Bandwidth
- Latency
- Reliability
- Number of concurrent connections
- Security

https://t.me/learningnets



EXAM TIP For Objective 2.4 of the CompTIA IT Fundamentals exam, make sure you can identify the strengths and weaknesses of cellular, radio frequency, and satellite Internet service types.

Mobility

Mobility describes how far you can travel and still access network resources. Ranked in order from highest to lowest mobility are satellite, cellular, radio frequency as used by WiFi, and wired.

Satellite Internet connectivity makes sense when no other options are available or when comparing options. For example, if you ever go on a Disney ocean cruise, you'll find that local WiFi Internet access on the ship is provided using satellite connectivity.

When you're on the go in populated areas, cellular Internet gets the top score. Different cell phone networks have different technologies available in certain locations, such as 3G, 4G, or LTE, that can affect the speed at which you surf, but basic data service is available just about anywhere. You can be within several kilometers or miles of the nearest cell tower and still get good service.

Wireless LAN (WiFi) connections are in the middle mobility-wise; they can start to fade out at approximately 30 meters (100 feet) from the WAP, depending on the WAP's technology (with newer WAPs having better range in general).

When considering mobility, however, don't overlook the availability of public wireless access points (or *hot spots*) like at restaurants, coffee shops, and hotels. If a business offers free WiFi, you and your mobile device can connect to it, just like you do your wireless router at home.

In contrast, wired LAN connections to the Internet are only as mobile as the length of your cable, which, using copper-based network cables, normally maxes out at approximately 100 meters (328 feet). That's definitely not very mobile.

Availability

Availability refers to the probability that a system will be functional. In other words, when you want to use a service, can you depend on it? Wired network connections win this battle because they don't commonly have interference problems. Cellular networks do a little better than WiFi but can suffer from

https://t.me/learningnets

interference, as can satellite networks. Wireless network technology can be affected by environmental conditions such as heavy precipitation, lightning, or sand storms.

Throughput/Bandwidth

Throughput refers to the data transfer rate. How quickly does your e-mail download, and how long do you have to wait for a web page to load? *Bandwidth* relates to throughput in terms of getting data from point A to point B but refers more to the size of the connection. In practical networking terms, both result in the same order of technologies. Internet throughput is often cited in download speeds and upload speeds. Because of the nature of Internet usage, download speeds are often much higher than upload speeds.

The clear winner is wired LANs. Wired connections on modern SOHO networks run at somewhere between 1 and 10 gigabits per second (Gbps), depending on the hardware used. That is *much* faster than any other Internet connection technology discussed here runs, so a wired LAN connection is rarely going to be the cause of speed limitations when you surf the Web. Always remember that the slowest network between two connecting endpoints can slow down a normally fast-performing Internet connection. So, while transferring files on a wired LAN might be lightning fast, accessing a slow web site on the other side of the planet might still be painfully slow.



NOTE Many people equate bandwidth with speed, but it's more properly analogous to volume. Think about drinking through a wide straw versus a narrow one. The liquid might be moving at the same rate, but more of it arrives in your mouth per second with the wider straw; it has greater bandwidth.

In second place is a wireless LAN, or WiFi. Depending on the technology of the router and the network interface on the device, a wireless LAN can transfer data at between 11 Mbps (802.11g) and 1.3 Gbps (802.11ac). You'll recall that one gigabit equals 1,000 megabits. Again, these speeds apply to the local area network; connectivity to the Internet will likely be much slower than this. Many broadband Internet provider technologies like fiber, cable, and DSL offer connection speeds up to 1 Gbps. As long as you have reasonably current networking hardware, the wireless connection should not be a barrier to taking

https://t.me/learningnets

full advantage of your SOHO Internet connection speed.

Generally speaking, last in the race for throughput are satellite and cellular. As an example, satellite connections for rural customers can range from 25 Mbps up to 100 Mbps. Cellular 4G LTE networks can provide up to approximately 300 Mbps. The newer proposed 5G cellular network standard should provide speeds between 500 Mbps and 10 Gbps.

Connection Delay (Latency)

Latency refers to the *connection delay* between a request and the response to that request. You always want that delay minimized, so low latency is preferred over high latency. In networking terms, a wired connection will always respond the quickest. Electrical pulses on a copper wire move very fast indeed, although fiber optic transmits light pulses much more quickly.

WiFi networks come in second because the distances between the client and the WAP are short. Cellular connections need to travel to the cell tower and back, creating a slightly bigger delay. Satellite generally comes in as the "winner" having the greatest network latency.

Reliability

Reliability refers to the quality of the data received and the error-checking and correcting capabilities of the technology. Does the data match what was sent, or have errors been introduced? How frequently does data need to be sent again because the receiving computer detected errors?

Wired connections offer the highest reliability because so little typically can cause problems on a copper wire. WiFi and cellular seem to offer similar strengths and weaknesses in reliability. The shorter distances and lower chance of interference from things such as storms put WiFi marginally in second place and satellite in third place.

Number of Concurrent Connections

The phrase *number of concurrent connections* can have a couple of different meanings. In classic networking terms, connections refer to unique conversations between a client and a server, called a *session*. This gets complicated quickly because modern servers handle all sorts of connections, and a single client computer can have multiple sessions with a single server at the same time. Here's an example of this beyond the CompTIA IT Fundamentals

https://t.me/learningnets

definition. Open a complicated web site, like www.yahoo.com. Then open a command prompt, type **netstat**, and press ENTER. See all those TCP lines that say "ESTABLISHED"? Those are connections.

This classic definition of concurrent connections seems to fall well outside the scope of the exam. So, let's look at a more English-based definition of *concurrent connections* in terms of access to the Internet. Which type of Internet connection enables more simultaneous users to access the Internet?

Wired networks scale up easily, so they support the most users. Cellular towers can support hundreds of users. A wireless access point supports a small number of wireless clients, at which point it taps out.

Level of Security

When we talk about security in the context of the Internet (and we'll do so a lot more in Chapter 11), we mean the risks involved in, for example, sending bank account or credit card information online. Which type of service is most or least likely to be snooped or hacked?

Wired LAN wins the most secure ranking here. Because it's all about the cables, there's little opportunity for someone to hack into it without physically plugging a cable into your switch.

Cellular data travels miles to reach the cell tower, so there's a lot of ground between you and the tower and more places for hackers to intercept data, but not as much as communicating with satellites orbiting the Earth. Cellular networks all use proprietary technologies for connectivity, however, so it's less likely a hacker has access to the software needed to hack into any given cell phone network than the oh-so-standardized WiFi network type. More specifically, Apple and Google look closely at every app that goes on their phones before making that app available for download. And it's hard to install an app on a smartphone in secret.

Properly set up and configured WiFi networks, with a good password on the WAP and encryption enabled, offer a high level of security. Bad guys can capture the radio signals, however, and creative people work hard to break encryption standards. What drops WiFi to third place in the security game is that you can set up a network with woefully poor security. An open-access WiFi point network, like at a coffee shop, is fertile hacking ground, because anyone can join that network. Wi-Fi hotspots often use a captive portal (web page) that users must interact with, such as agreeing to terms of use, before being granted Internet access. Short version: don't do your banking at a public WiFi hotspot.

https://t.me/learningnets

Using a LAN to Share Files and Printers

So, you've got a LAN up and running in your home or small business, and everyone is happily using your shared Internet connection. Now what? You might want to look at ways to share data (such as your music collection) between the individual computing devices within your local network. Let's get to work on that!

To share files and printers, you need to turn on File and Printer Sharing and then organize networked computers in some fashion so they can see networked shares. Then you have to share folders and printers actively.

Enabling File and Printer Sharing

The first time you connect to a network using a Windows device, a box pops up asking about the network location. Depending on what you choose, Windows loosens network security settings for more trusted home or work networks and tightens them for less trusted public networks. Choosing Home or Work as the network location enables File and Printer Sharing; choosing Public disables it.

File and Printer Sharing enables the device to share folders and any directly connected printers with other devices on the network. Without it, none of the other sharing settings described in the upcoming sections are possible.

Here are the steps to check or adjust File and Printer Sharing settings:

1. Open the Control Panel (in Windows 8.1 or Windows 10, just right-click the Start button and select Control Panel).
2. Open the Network and Sharing Center applet.
3. Click Change advanced sharing settings.
4. In the Network discovery section, make sure Turn on network discovery is selected. This setting enables other computers to see your shared assets when they browse the network.
5. In the File and printer sharing section, make sure Turn on file and printer sharing is selected. See Figure 10-16.

https://t.me/learningnets

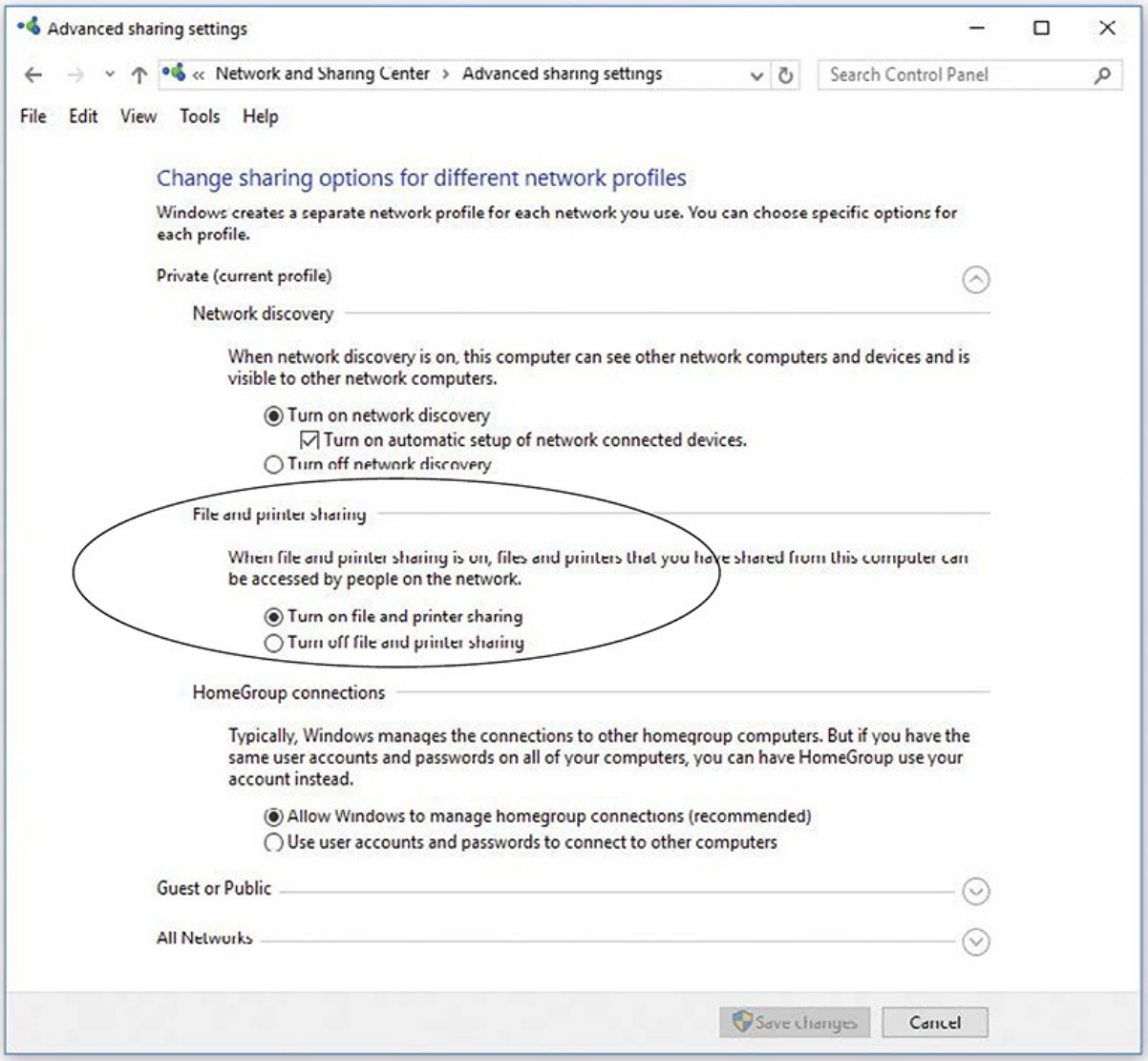


Figure 10-16 Enable File and Printer Sharing if needed.

6. If you made any changes, click Save changes.

Network Organization

Microsoft organizes networked Windows computers in three ways: workgroups, domains, and homegroups. Each network organization offers distinct advantages and disadvantages.

Workgroups

All PCs belong to a single *workgroup* by default, called WORKGROUP. Being

https://t.me/learningnets

in the same workgroup enables users to share access to files, folders, and printers. You can see your current workgroup name by opening the System applet in Control Panel (Figure 10-17).

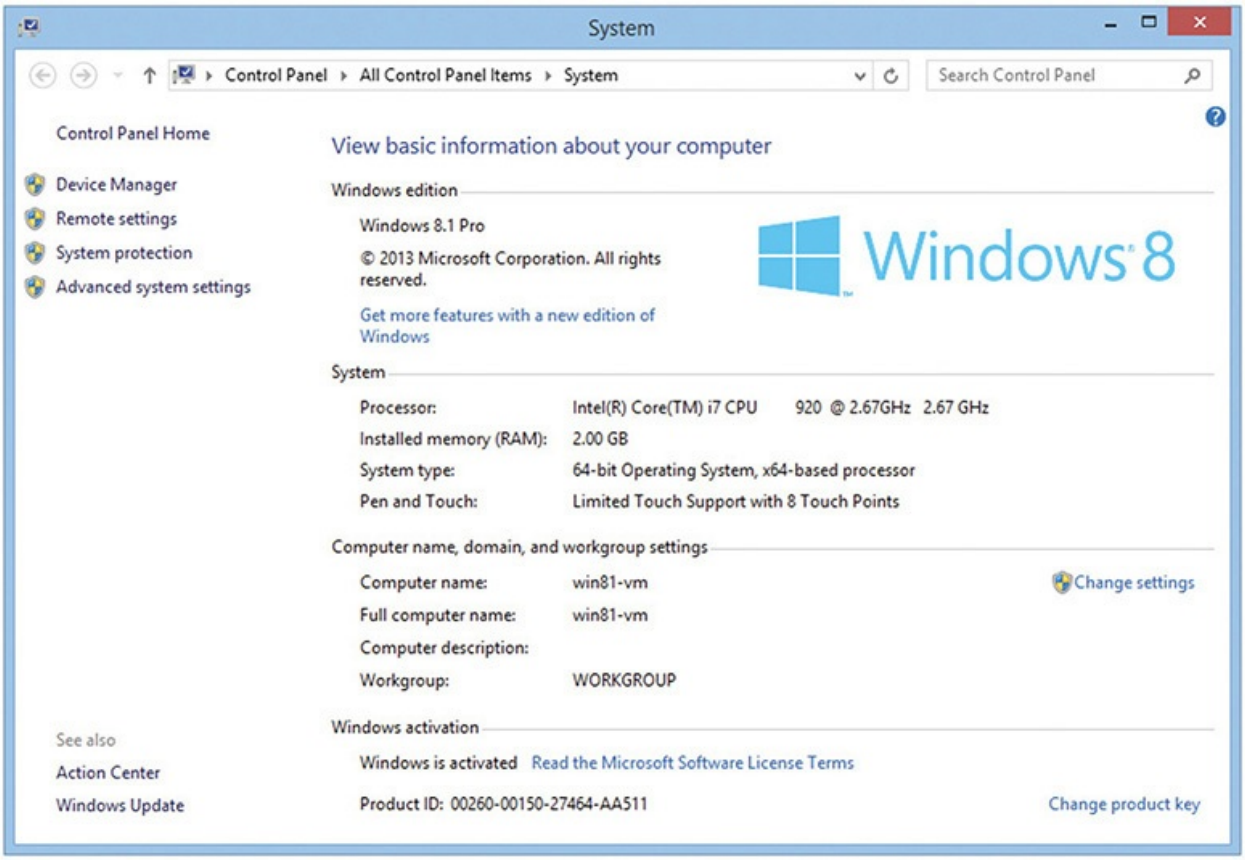


Figure 10-17 System information for a Windows 8 device in the default workgroup

The WORKGROUP name carries no special magic, and you can change it at will. The key thing to keep in mind is that computers need to share a workgroup to share files, folders, or printers.



NOTE Savvy readers might note that this discussion of workgroups does not use the term *LAN*. Workgroups and LANs function together but function differently. You can have ten computers plugged into the same LAN, for example, and have five set to a workgroup named BARCELONA and five set to a workgroup named MADRID. The workgroup simply serves as a way of

https://t.me/learningnets

organizing computers, just like folders on a disk can organize related files. Sharing folders and printers is separate from workgroups; in other words, computers in the BARCELONA workgroup can potentially access workgroup shared resources in BARCELONA and MADRID.

Workgroups lack central control; this works fine for small networks but falters when securing those with many users. The lack of central control means you have to log on to each individual system to use its resources. Either you need a password for a local account on each system or the system's administrator needs to set one up for you. All of these accounts quickly become an administrative chore as the workgroup grows.

Domains

Larger networks use *domains*, in which a server running Windows Server (Figure 10-18) controls access to network resources. A Microsoft Active Directory (AD) *domain* requires one or more servers to act as domain controllers (DCs), which are central hosts that store usernames, passwords, computer accounts, and other network configuration items. Users can log in from any computer connected to the domain—what's called *single sign-on*—and have access to everything they have permission to access. User authentication is performed by DCs. While domains rock, they fall well outside the scope of the CompTIA IT Fundamentals exam. You'll see the domain options when you click around in the System applet. Ignore domains until you're ready to start studying for CompTIA A+.

https://t.me/learningnets

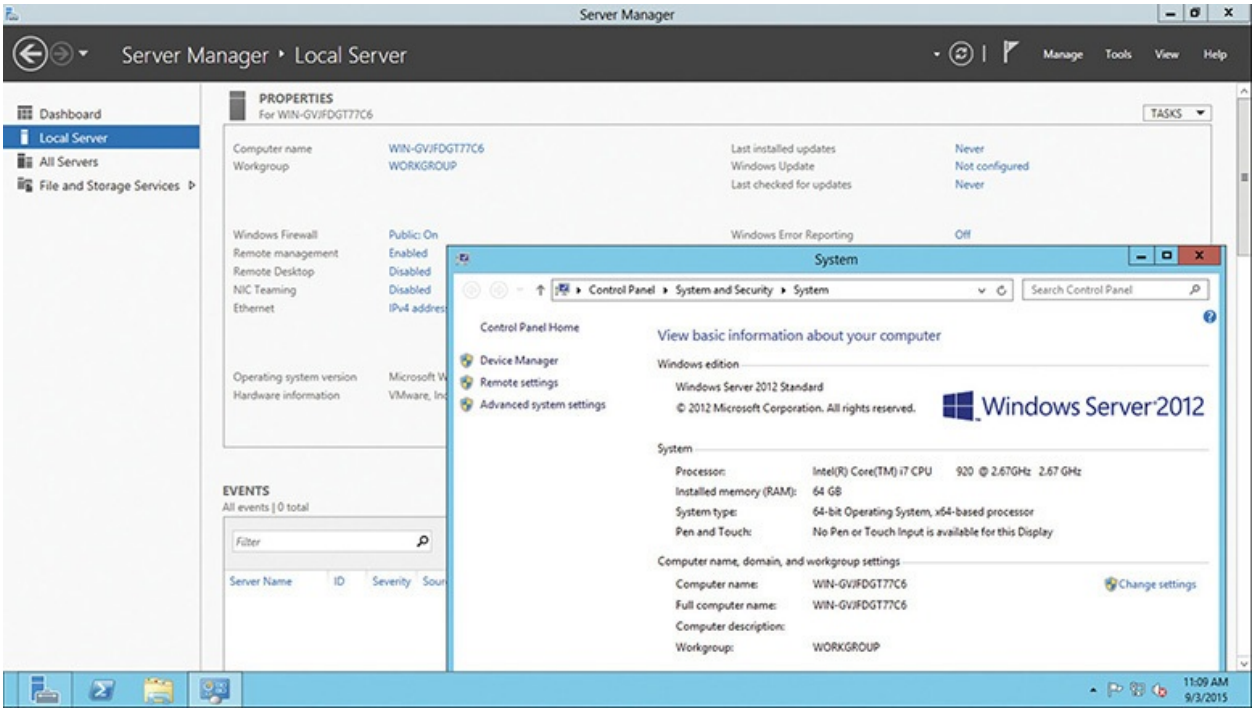


Figure 10-18 Windows Server

Homegroups

Workgroups provide no security and require lots of signing on to access resources; domains provide single sign-on and security at a cost. To split the difference, Microsoft introduced homegroups in Windows 7.



NOTE Homegroups are not available in macOS or any Linux distro.

Most people just want to share types of data, such as music, so homegroups just share Windows libraries. A homegroup connects computers (which can join only one homegroup at a time) via a common password—no extra usernames are required.



NOTE *Libraries* group files of specific types, regardless of where they reside on mass storage. You can access all your music files from the Music library, for example. Sharing that library makes your music accessible to all computers

https://t.me/learningnets

attached to the homegroup.

You create homegroups from the HomeGroup applet. If you're in a homegroup already, you'll have options to edit relevant settings. If you're in a workgroup and not a homegroup, you can click the Create a homegroup button to bring up the Create a Homegroup dialog (Figure 10-19), from which you select library types. When you click Next, you'll see the generated homegroup password (Figure 10-20).

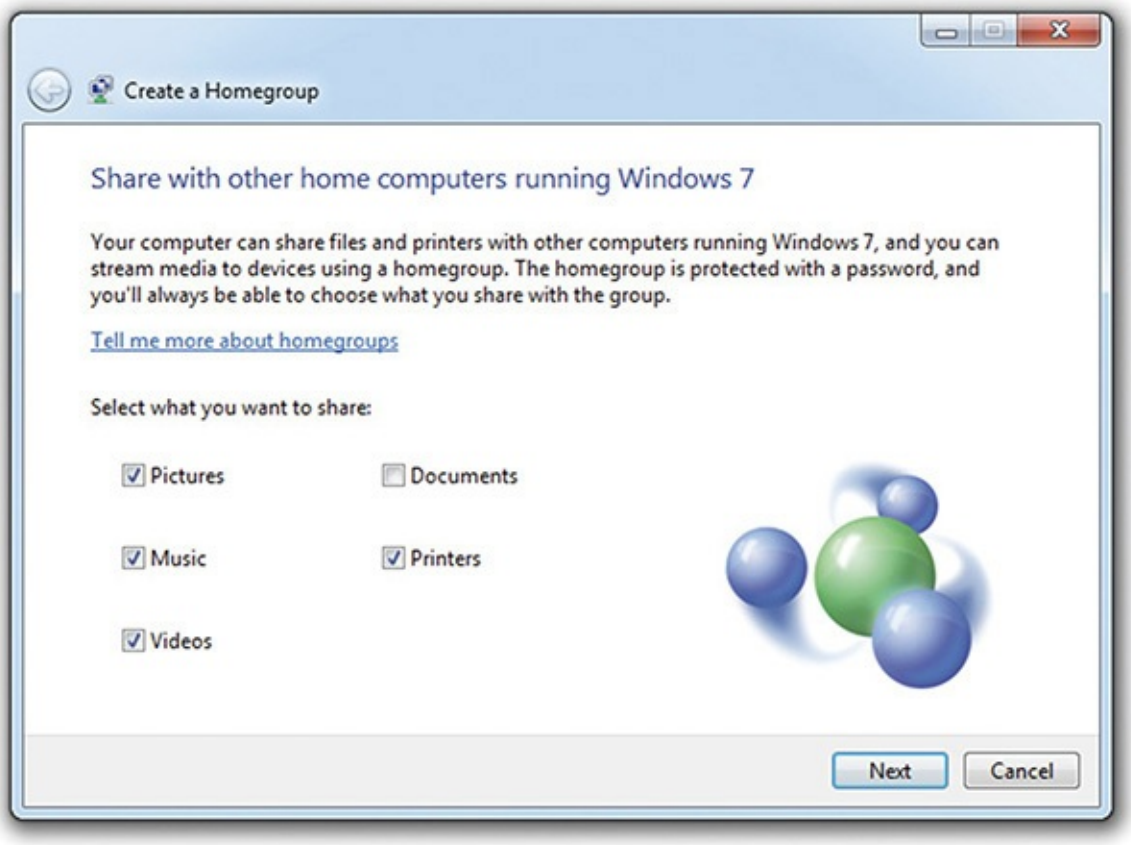


Figure 10-19 The Create a Homegroup dialog

https://t.me/learningnets

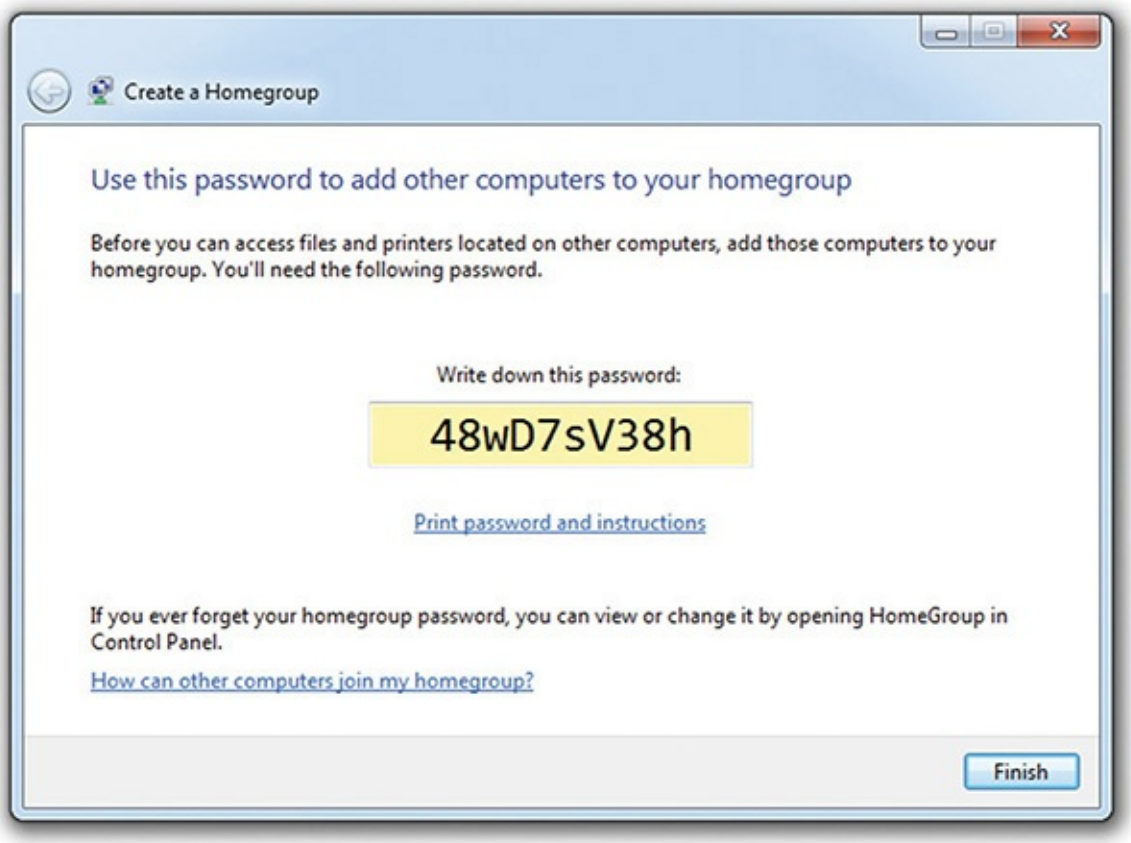


Figure 10-20 The homegroup's password

If you go to another computer on the network and open the HomeGroup applet, it will prompt you to join the existing homegroup. Just click the Join now button, enter the password, and pick libraries to share. You can browse your new homegroup through Windows Explorer or File Explorer (Figure 10-21). To add folders or libraries, right-click either the folder or the library, select Share with (Figure 10-22), and choose a Homegroup option.

https://t.me/learningnets

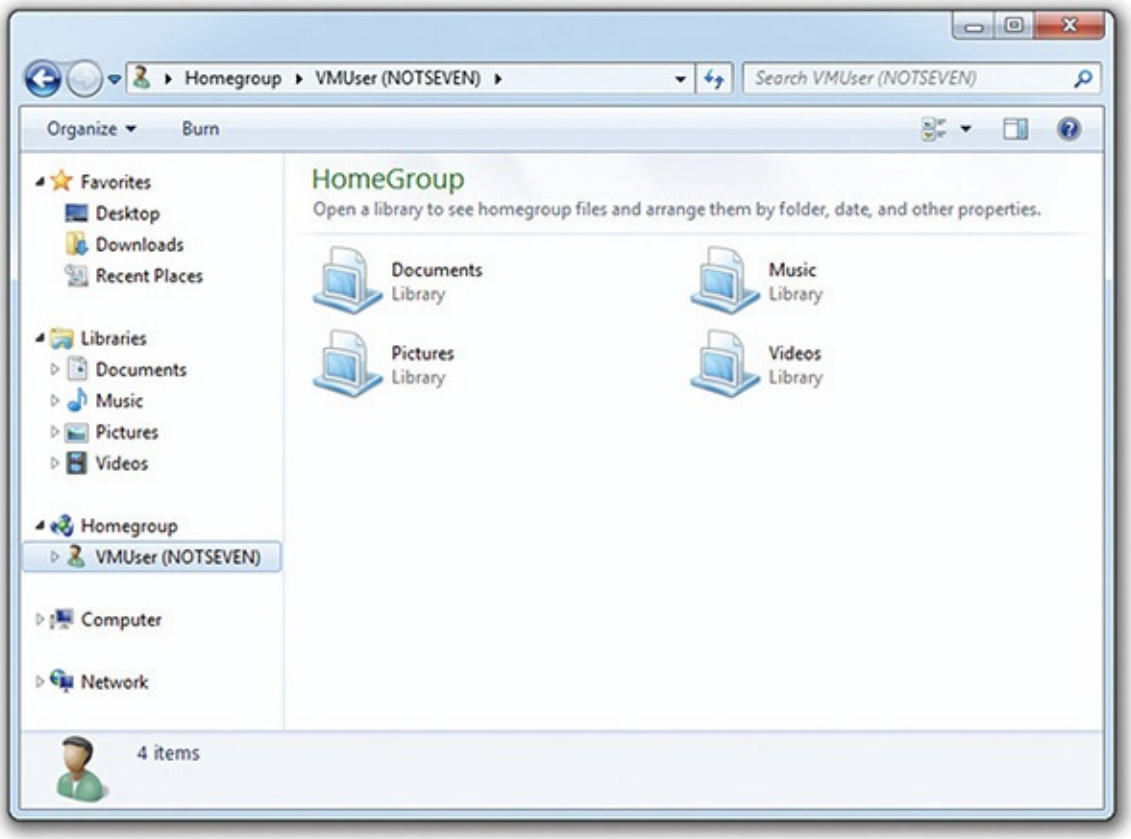


Figure 10-21 Using homegroups

https://t.me/learningnets

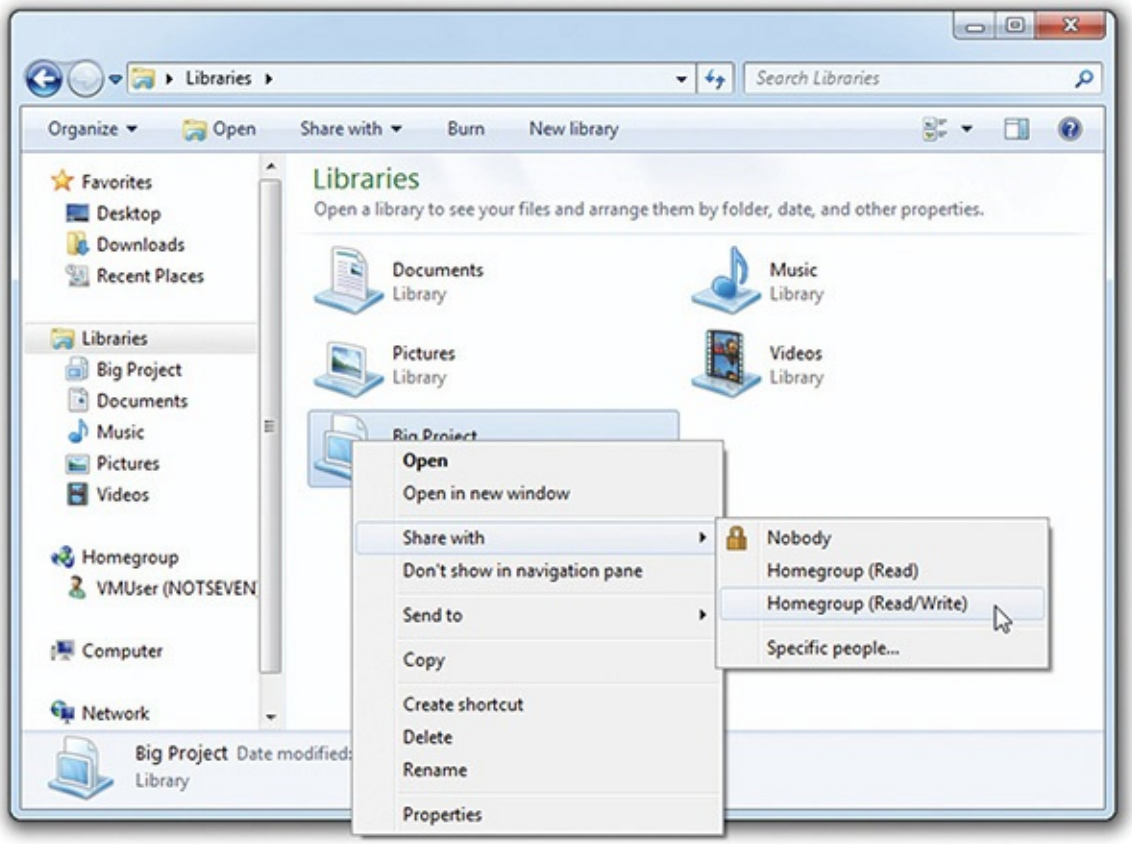


Figure 10-22 The Share with menu

Sharing

Windows systems can share files, folders, entire drives, printers, faxes, Internet connections, and much more—but the CompTIA IT Fundamentals exam limits its interest to folders and printers. You've already seen how to share with homegroups, but there are other ways to share folders and printers.

Sharing a Folder

The manual way to share a folder is to right-click it, select Properties, go to the Sharing tab, and select Advanced Sharing. From here, select the Share this folder check box and name the network share (Figure 10-23). By default, new Windows shares have only Read permission for everyone; click the Permissions button to set your share to Full Control (Figure 10-24).

https://t.me/learningnets

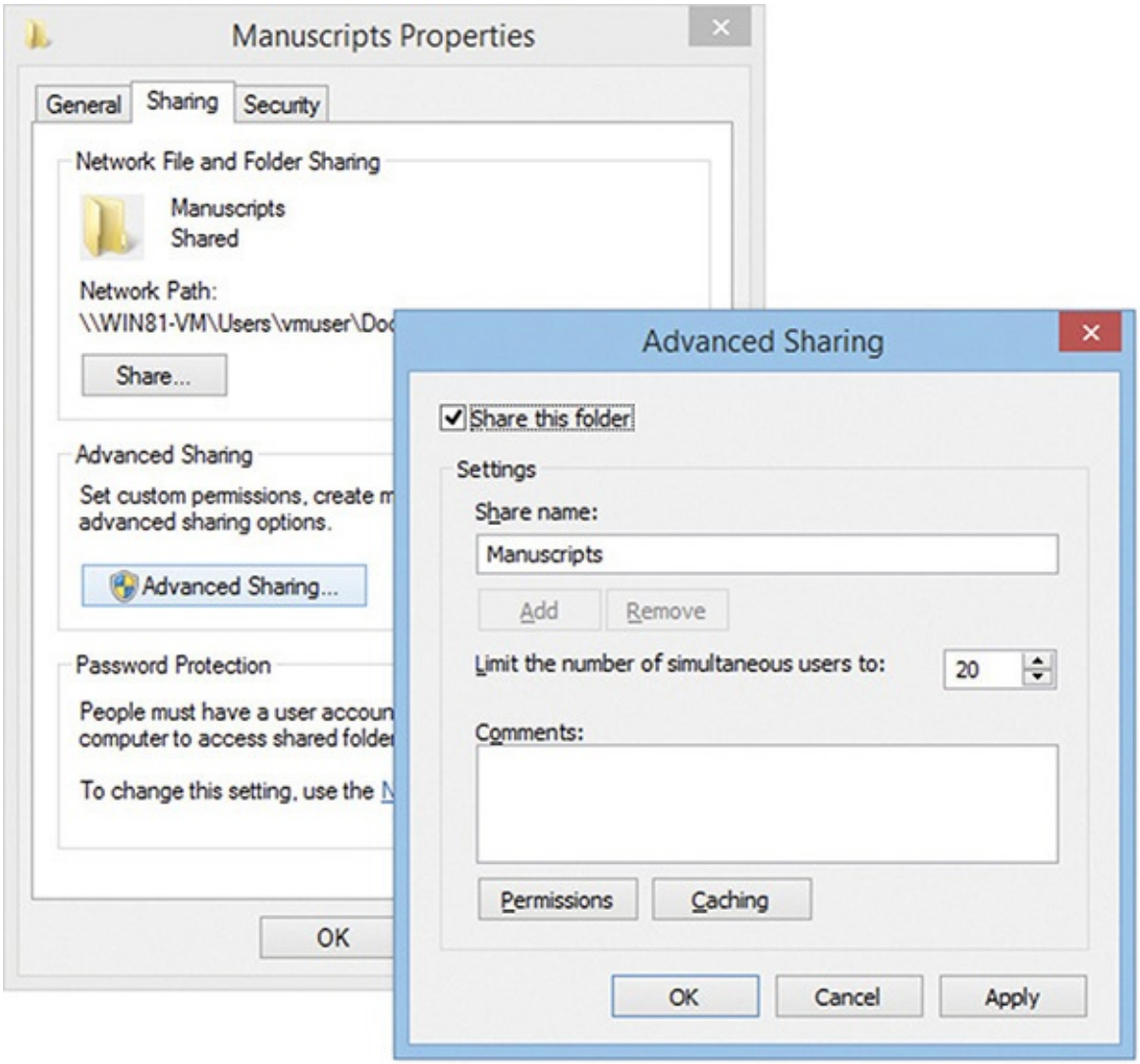


Figure 10-23 Advanced Sharing dialog

https://t.me/learningnets

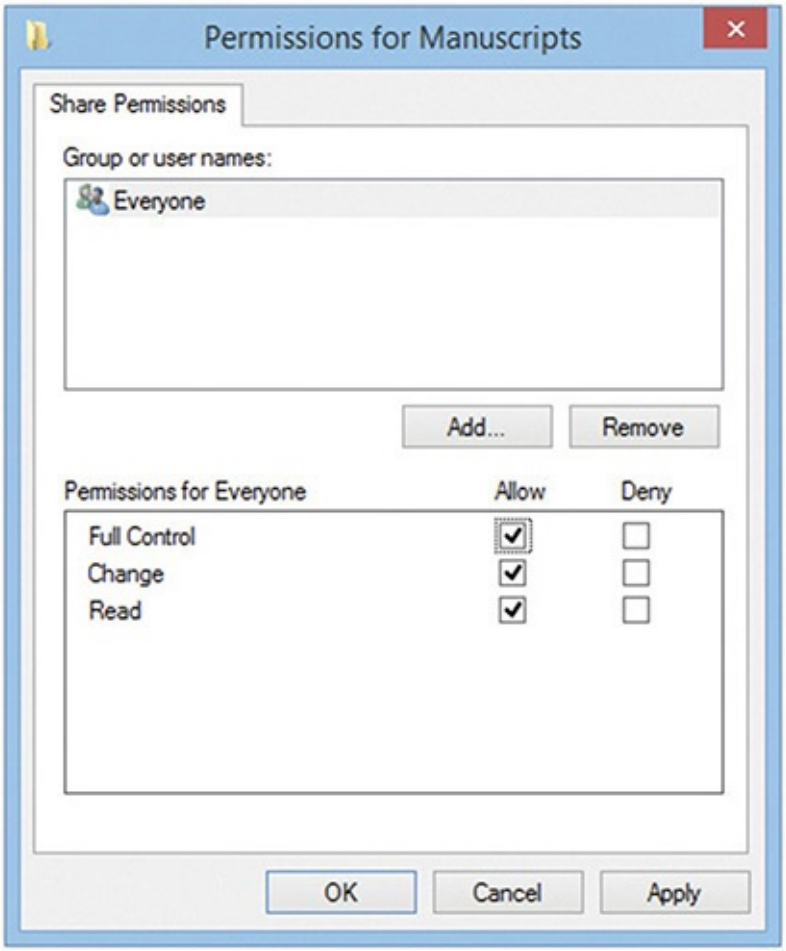


Figure 10-24 Setting the share to Full Control

A simpler (less powerful) method is to right-click a file or folder and select Share (or Share with) | Specific people to open the File Sharing dialog and select user accounts from a drop-down list. These will be local accounts unless your system is in a workgroup or domain, in which case you can select or search for remote accounts. When you select one, you can choose Read or Read/Write permissions (Figure 10-25).

https://t.me/learningnets

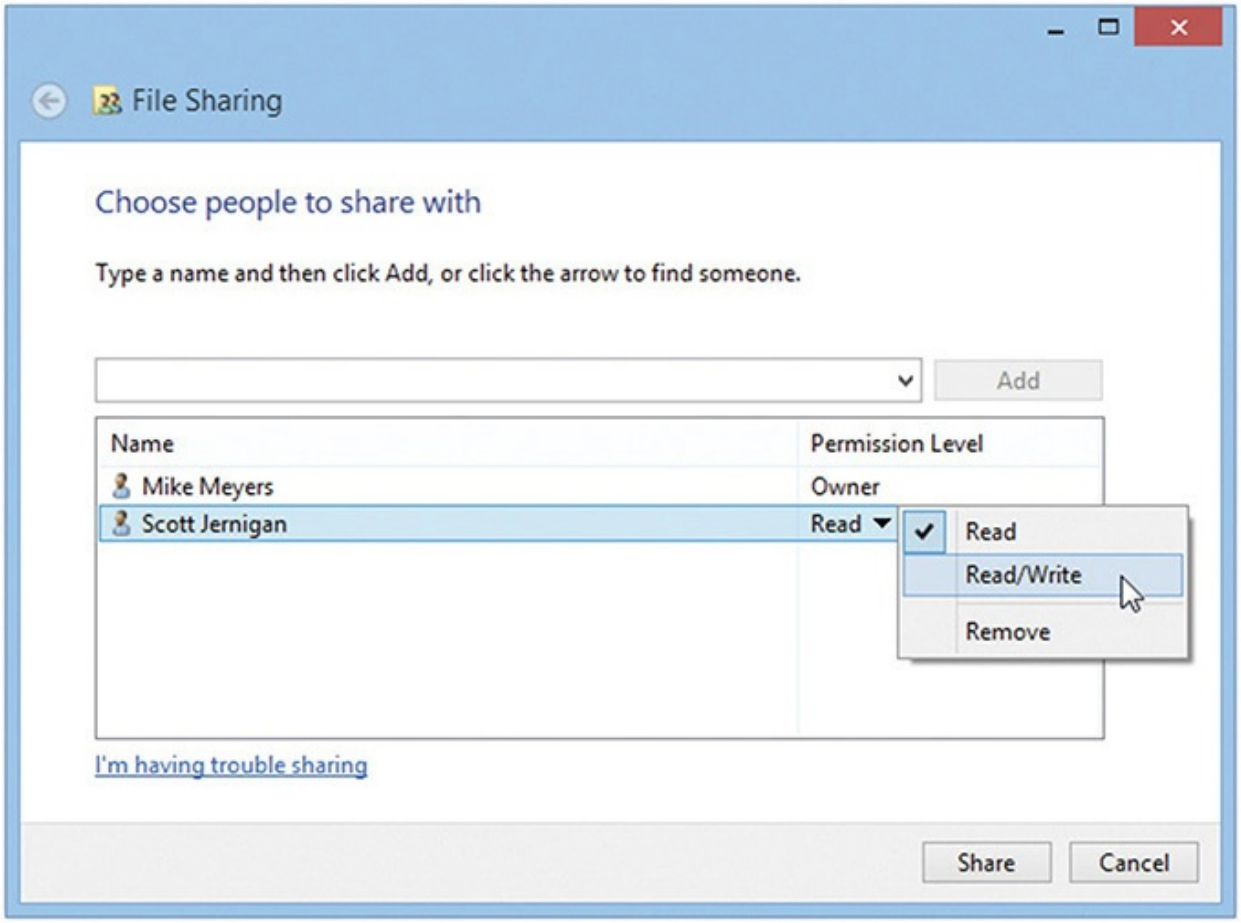


Figure 10-25 File Sharing dialog permissions options

Accessing Shared Network Volumes

To browse shared content on other computers, open File Explorer and click Network in the Navigation pane. From here, double-click the icon in the Computer section for the computer you want to browse.

If the user's shared folders are password-protected, you'll be prompted to enter a username and password for that computer. See Figure 10-26. If you don't have access to a user account on that computer, you won't be able to access the shared folders.

https://t.me/learningnets

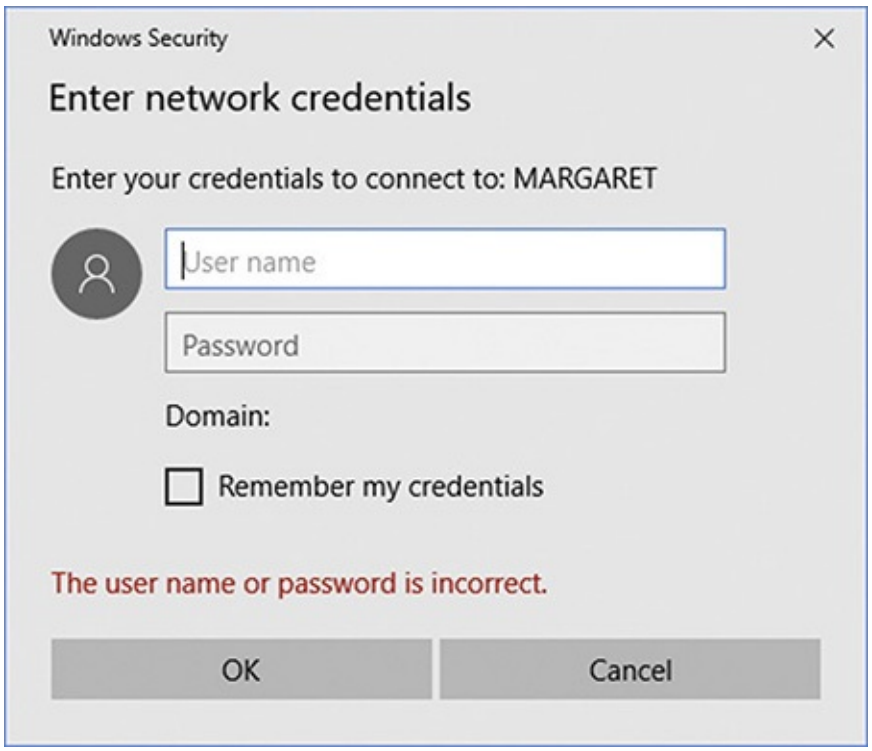


Figure 10-26 You might be prompted for credentials when attempting to access shared assets.

If you can access the system, you'll see icons for the shared folders. They are much like any other folder icons in File Explorer except they have a green network connector symbol underneath them, as shown in Figure 10-27.

https://t.me/learningnets

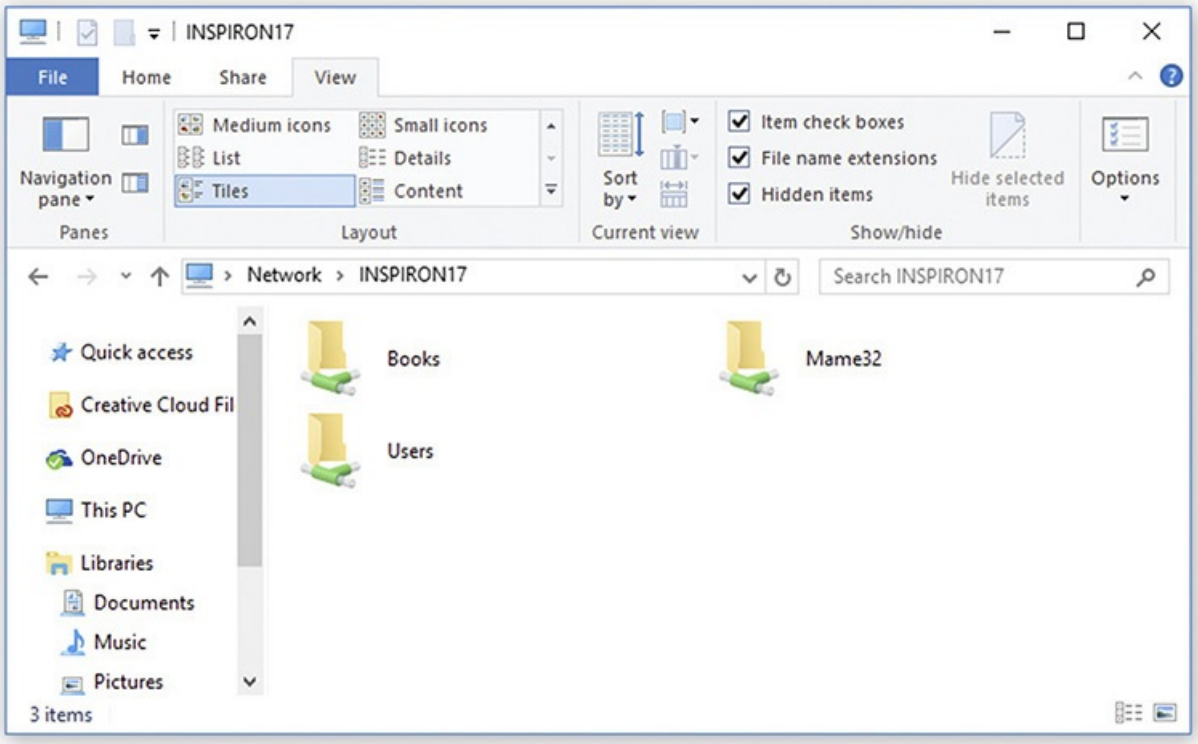


Figure 10-27 Shared folders in File Explorer

Installing and Sharing a Printer

There are two ways to share a printer on a network. One is to use a network-enabled printer (one with a built-in wired or wireless network adapter). Another way is to connect the printer directly to an individual computer, set it up as a local printer like you did in Chapter 3, and then make it available as a shared resource on the LAN. Let's look at sharing networked and local printers on both wired and wireless networks.

Network-Enabled Printers

You can connect a network-enabled printer directly to your switch. If the printer has a wireless network adapter in it, you can connect the printer to the WAP. (Most likely, your SOHO router includes both devices.) Follow the instructions in the printer's documentation to learn exactly how. You will need to enter the network's password (the preshared key) from the printer, most likely using the printer's LED display (and hardware buttons unless it is a touchscreen). This can be a bit tedious, but hang in there and follow the instructions; you shouldn't have to do this often.

https://t.me/learningnets

Any computer attached to the network should then have access to the printer. As you'll recall from Chapter 3, each workstation requires drivers installed for the specific printer. That includes printers directly connected to the network. Choose the Add a printer option in the Devices and Printers Control Panel applet to add a printer.

Sharing a Local Printer with Other Computers on the LAN

To share a printer attached to a workstation, open the Control Panel and open the Devices and Printers applet. Right-click the icon for the printer you want to share and select Printer properties. Click the Sharing tab and select the Share this printer check box. In the Share name box, type the name that will appear to other users on the LAN and click OK. See Figure 10-28.

https://t.me/learningnets

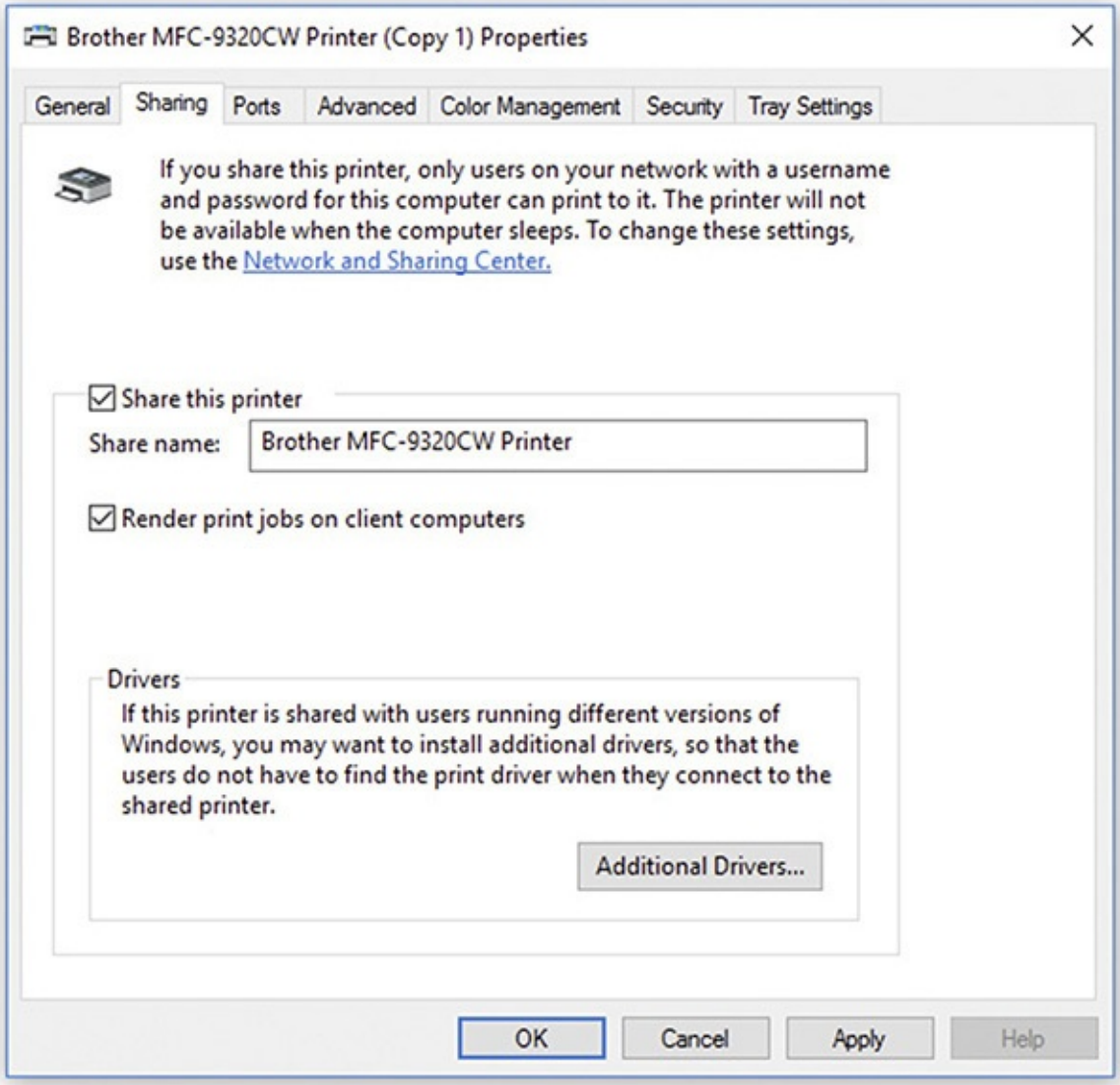


Figure 10-28 Share a printer with other computers on your LAN.

Chapter Review

In this chapter, you learned a little about networks. A LAN covers a small area, where all the computers connect via cables, wireless signals, or a combination of the two, through switches or WAPs. A WAN is a larger collection of connected LANs. Clients are the user PCs, and servers are the workhorses of a network. Client-server networks have both clients and servers, whereas peer-to-peer networks have only clients, each one of which takes on a bit of server responsibility to make it work.

To join a network, computers need a wired or wireless connection to a switch

https://t.me/learningnets

or router. Routers provide a path outside of the LAN, enabling SOHO networks to share an Internet connection. A SOHO router works with no configuration, but you should configure its security settings. This includes changing the SSID and router password and securing the network by enabling encryption.

When choosing among wired and wireless radio frequency networks in the form of WiFi, cellular, and satellite, you learned that cellular and satellite excel at mobility. A wired connection gets great marks for availability, bandwidth, latency, reliability, number of concurrent connections, and security. WiFi falls in between these areas.

To share files and printers on a LAN, first make sure File and Printer Sharing is enabled. Create or join a homegroup if desired. Computers that can't use homegroup can still connect to other computers on the LAN via workgroup. To share a folder, right-click it and choose Share with. Share a printer via the Sharing tab of the Printer Properties dialog box.

Questions

1. Which of these terms best describe a SOHO network? (Choose two.)
   - **A.** Peer-to-peer
   - **B.** Client-server
   - **C.** WAN
   - **D.** LAN
2. What differentiates a router from a switch?
   - **A.** Routers are for WANs, and switches are for LANs.
   - **B.** A router provides a path out of the LAN, such as to the Internet.
   - **C.** A switch provides a path out of the LAN, such as to the Internet.
   - **D.** Routers are for client-server networks, and switches are for peer-to-peer networks.
3. When shopping for a SOHO router, look for the latest available standard, which is:
   - **A.** 802.11b
   - **B.** 802.11ac
   - **C.** 802.11n
   - **D.** 802.11g

https://t.me/learningnets

4. What kind of ports are on the back of a SOHO router for making wired connections?
   - **A.** VGA
   - **B.** DVI
   - **C.** RJ-45
   - **D.** RJ-11
5. How do you access a router configuration utility?
   - **A.** Buttons on the top of the router
   - **B.** Buttons on the back of the router
   - **C.** IP address in a web browser
   - **D.** Domain name in a web browser
6. What is the router's SSID?
   - **A.** Network name
   - **B.** IP address
   - **C.** Serial number
   - **D.** Model number
7. Which wireless encryption standard is the most secure?
   - **A.** WEP
   - **B.** WPA
   - **C.** WPA2
   - **D.** WPS
8. In which way is a cellular Internet connection superior to wired and WiFi?
   - **A.** Bandwidth
   - **B.** Mobility
   - **C.** Number of concurrent connections
   - **D.** Security
9. What is an advantage of using a homegroup?
   - **A.** Higher security level
   - **B.** Easier folder and printer sharing
   - **C.** Makes router use less power
   - **D.** Faster file transfer

https://t.me/learningnets

10. Where in the Control Panel would you go to connect to a network printer on a client PC?
    - **A.** Devices and Printers
    - **B.** System and Security
    - **C.** Network and Internet
    - **D.** Ease of Access

Answers

1. **A, D**. A SOHO network is a peer-to-peer LAN. A WAN is a wide area network, where clients are not located near each other. A client-server network is a larger network that uses a server.
2. **B**. A router, not a switch, provides a path out of the LAN to other networks. Both routers and switches can be used with either WANs or LANs and with both client-server and peer-to-peer networks.
3. **B**. 802.11ac is the latest wireless standard. The others, from oldest to newest, are 802.11b, 802.11g, and 802.11n.
4. **C**. The RJ-45 ports on the back of a SOHO router are for wired Ethernet connections. An RJ-11 connector is for a telephone landline. VGA and DVI are video connectors.
5. **C**. Access a router's configuration utility by typing its IP address into a web browser. You cannot access the router configuration with buttons on the router. The router does not have a domain name.
6. **A**. The SSID is the router's WiFi network name. Its IP address is the address by which you access it for configuration. The serial number and model number have no role in router naming or configuration.
7. **C**. WPA2 is the most secure wireless encryption standard. WEP and WPA are not as good. WPS is not an encryption standard; it is a way of configuring a WiFi network connection by pressing a button on the router.
8. **B**. Wired connections excel at bandwidth, concurrent connections, and security. Cellular and satellite are better for mobility.
9. **B**. A homegroup simplifies folder and printer sharing. It does not change the security level, the router power, or the file transfer speed.
10. **A**. Printer settings are accessed from Devices and Printers in the Control Panel.

https://t.me/learningnets

CHAPTER 11

IT Security Threat Mitigation

In this chapter, you will learn how to

- Identify threats to local PC security
- Describe physical access control and device hardening
- Select appropriate user account types
- Define and compare types of malicious software
- Protect against malware and social engineering
- Describe browser privacy and security issues

These days, you can't afford to be blissfully unaware when it comes to computer security. Threats to your security, privacy, and computer lurk around every corner. Through your devices, a malicious person (an *attacker*) or automated malware can gain valuable information about you. An attacker can steal your files, monitor your web usage, encrypt your data files, or run programs that log your keystrokes to pilfer account names and passwords, credit card information, and more.

An attacker could even run software that takes over your computer to send spam or steal from others. Viruses and other malicious software can sneak into your system and destroy your data from anywhere in the world. The threats are real and immediate.



NOTE In computing and technology circles, *hacker* is often a term of reverence for talented experts driven to expand, extend, improve, overcome, and repurpose existing hardware, software, and systems. Since these talents can be used for good or bad (or even just for fun) and because some of the threats you'll see in this chapter are astonishingly low-tech, we use the more generic term

https://t.me/learningnets

attacker.

This chapter is all about IT security. We'll look at local security threats that can include viruses and other malware spread from other computers on your LAN to yours, physical security issues, and attempts to guess your passwords. We'll also talk about threats that come from *outside* your local environment (primarily from the Internet).

Finally, we'll discuss ways to make your computer less vulnerable to security threats.

Understanding Local Security Threats

A local security threat originates from your local environment. For example, a disgruntled employee might try to access private salary data or delete the customer database on the company network, or someone might steal the receptionist's laptop when he steps away for a moment. Many people are vigilant for viruses and other malware originating online but overlook equally real threats from inside the building.

Unauthorized Access

After successful authentication, users can then be *authorized* to access network resources for which they have been granted permissions. *Unauthorized access* occurs when a person accesses resources (such as data, applications, and hardware) without permission. A user can alter or delete data; access sensitive information, such as financial data, personnel files, or e-mail messages; or use a computer for purposes the owner did not intend.

Not all unauthorized access is malicious—often this problem arises when users who are randomly poking around in a computer discover that they can access resources in a fashion the primary user or administrator did not intend. Unauthorized access becomes malicious when outsiders knowingly and intentionally take advantage of weaknesses in your security to gain information, use resources, or destroy data.

Password Cracking

The most common way of gaining unauthorized access is to obtain a password that you aren't authorized to have.

Professional computer criminals often employ a technique called *password cracking* to obtain passwords. Cracking is more than just random guessing—it's

https://t.me/learningnets

a disciplined technique for obtaining a password through rapid-fire trial and error, often by employing password-cracking software. Password crackers who know something about the owner of the password can further target their guessing by including names and words that would be meaningful, like the name of a spouse or family pet, or a birthday or an anniversary date. Strong passwords should be used to make it more difficult for password-cracking programs to acquire your password. Later in this chapter you'll learn what constitutes a *strong password*.



NOTE Some people use the term *cracking* to broadly describe *malicious* hacking.

Even more common than software-based password cracking, however, is seeking out or stumbling upon a written password that has been poorly guarded. For example, a user might have a really difficult-to-guess password, but then he might write it on a slip of paper that he keeps in his desk drawer.

Dumpster Diving

Dumpster diving is the generic term for anytime an attacker goes through your refuse, looking for information. The amount of sensitive information that makes it into any organization's trash bin boggles the mind! Years ago, one IT security guru took a few IT people on a tour of an office's trash. In one 20-minute tour of the personal wastebaskets of one office area, they had enough information to access the network easily, as well as to embarrass more than a few people. When it comes to getting information, the trash is the place to look! To prevent this threat, shred sensitive information using a paper shredder.

Shoulder Surfing

Another type of theft to worry about when computing in public is theft of your passwords. *Shoulder surfing* is when people spy on you from behind, watching what you type. Even though most passwords appear on the screen as dots rather than characters you typed, the thief could be watching your fingers and memorizing keys you press. The danger from shoulder surfing increases the more frequently you work in a specific place. Each day, an observant person with bad intent can get another keystroke or two. Check before you type! Computer screen privacy filters are often used to prevent shoulder surfing by

https://t.me/learningnets

making a screen harder to read at an angle or from a distance.

Unauthorized WiFi Usage

As you learned in Chapter 10, failing to secure a wireless router means unauthorized users can join the network. If a PC on the network has File and Printer Sharing enabled, an intruder could potentially read and even modify or destroy that user's files. Even if all of your individual systems are locked down, an attacker could use your network to commit fraud, attack other networks, or engage in piracy and other illegal activities that could get traced back to you. The best defense against unauthorized WiFi use is to implement wireless encryption methods such as WPA2.

Data Destruction

Along with unauthorized access may come unauthorized modifying or deleting of files or changing of system settings. For example, suppose a family member signs into your PC with your password and deletes some of your files to make room to install a new game. There goes your final paper or your tax return files for the last five years! Data destruction can also be intentional and purposeful, such as an unhappy (or recently fired) employee destroying valuable company records and databases.

Theft

Thieves steal whatever you don't have locked down, either physically or electronically. If you turn your back on your laptop or tablet at the local coffee shop, for example, someone might take it. Even worse than the physical loss of your hardware, however, is the loss of the data that it contained and the loss of your privacy. If you stored passwords and credit card numbers on the stolen device, they are now in the hands of a thief.

Amazon and other retailers sell laptop lock cables that work just like a bike chain. Most laptops have a small security port where you insert the lock after wrapping the cable around something immovable, like a table leg or post (Figure 11-1).

https://t.me/learningnets



Figure 11-1 A standard laptop lock that protects against casual theft

Another, less obvious form of theft is the stealing of software and software licenses. Let’s say you bought a copy of Microsoft Office and its license allowed you to install it on two computers (that is, to use the product key to activate it on two computers). If someone steals your product key, they can use (or sell) an activation of the software.

Malware

Networks are without a doubt the fastest and most efficient vehicles for transferring computer malware among systems. Malware is malicious software written to do something unwelcome to your computer. Malware takes many forms, as we’ll discuss later in this chapter.

News reports focus attention on the many malware attacks from the Internet, but a huge amount of malware comes from users who bring in programs on USB drives and writable optical discs.

Physical Security

Once you’ve assessed the threats to your computers and local networks, you need to take steps to protect those valuable resources. This section explores physical security, including access control and device hardening.

Access Control

https://t.me/learningnets

The first order of security is keeping people who shouldn't have access away from the actual hardware. This isn't rocket science. Lock the door. Don't leave a PC unattended when logged in. In fact, don't ever leave a system logged in, even with a Guest or Standard user account. We pity the fool who walks away from a server still logged in as Administrator. Don't tempt fate.

Device Hardening

One important component of local device security is the practice of *device hardening*, which means to make the device as difficult as possible to compromise by changing hardware and software settings. Another term used to describe this is *reducing the attack surface*. Let's look at the following ways you can harden a device, whether it's a desktop or laptop, a tablet, or a smartphone:

- Disable unused wireless features.
- Set up lockout times.
- Enable security features.
- Use encryption.

Disable Unused Wireless

Disable any wireless features that you are not using, such as WiFi, Bluetooth, and near-field communication (NFC). You can easily reenable them when you want to use them, and keeping them turned off during downtimes ensures that nobody can gain access to your device through them without your permission. On a mobile device, you can do this via the Settings app. On a laptop, there may be hardware buttons on the computer that toggle wireless receivers on/off, or there may be an Airplane mode that does the same via software. You can also disable wireless adapters in Device Manager, which you can access via Control Panel | Hardware and Sound | Device Manager. In Figure 11-2, for example, you can tell that the Bluetooth adapter is disabled by the down-pointing arrow symbol on the device icon.

https://t.me/learningnets

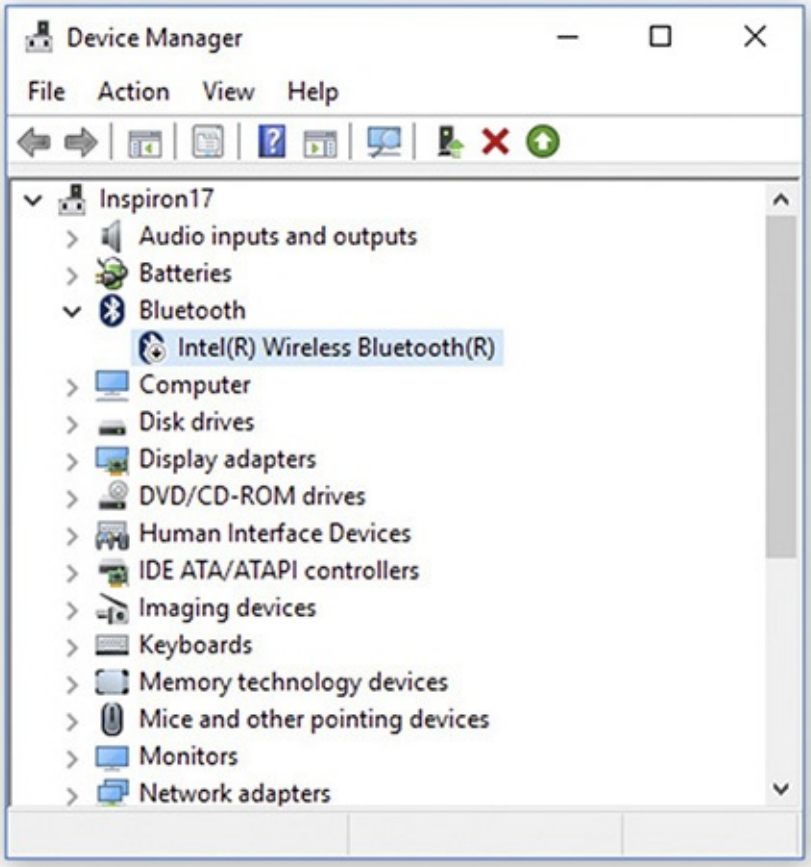


Figure 11-2 You can disable wireless adapters that you don't regularly use.

Configure Lockout

You can configure a lockout time so that a lock screen appears after a certain period of idleness; a password or PIN must be entered to get back in. This prevents someone from snooping around your device if you leave it unattended. Set the lockout time to the shortest option that doesn't drive you up the wall. Even a minute alone with an unlocked system is enough time for a cool-headed attacker to insert a USB drive, install malware, and walk away like nothing happened. On a mobile device, set the Lock Screen setting. In Windows, enable a screensaver in the Control Panel and set it to display the logon screen when waking from it. Then set the delay before the screensaver starts. See Figure 11-3.

https://t.me/learningnets

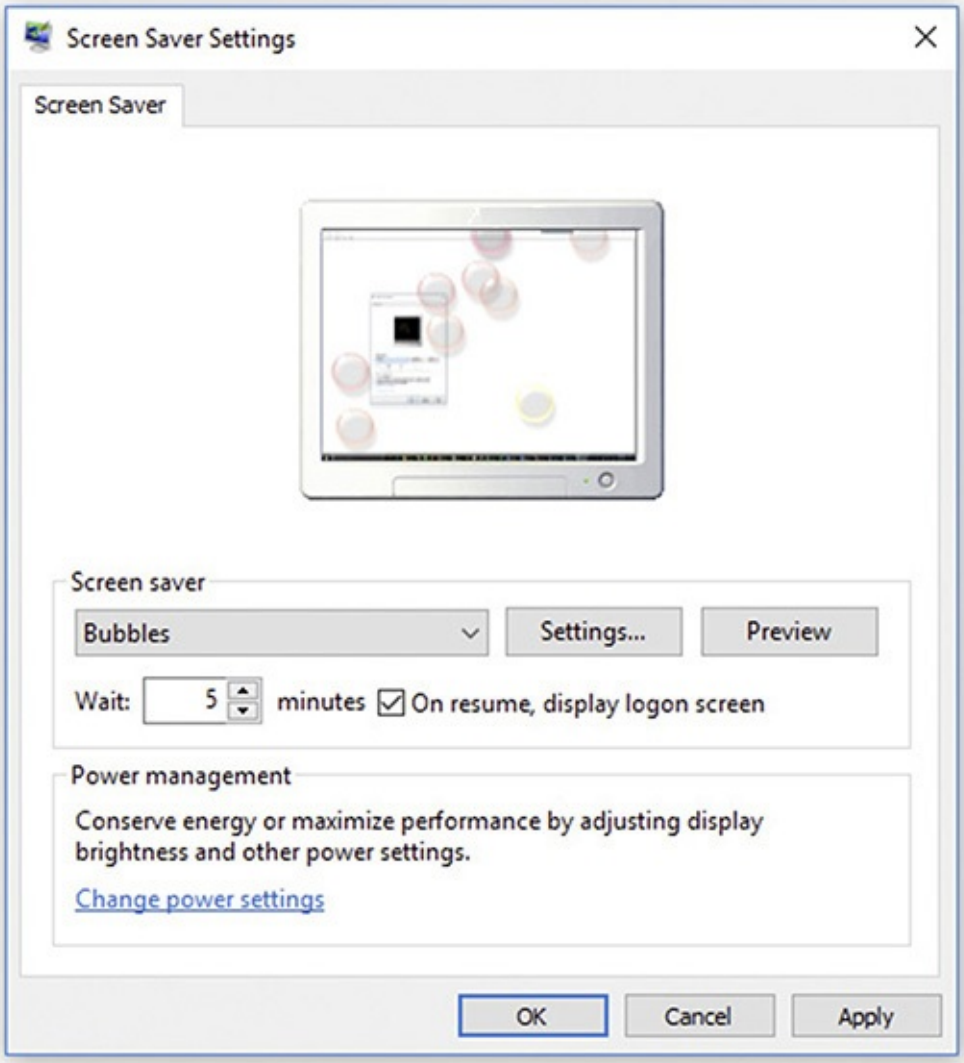


Figure 11-3 You can require a password when the PC wakes up from the screensaver.

Enable Security Features

Different operating systems have different security features that you can optionally enable to increase security. Windows has Windows Defender for malware, for example, and Windows Firewall for network attacks; some smartphones have fingerprint recognition and enhanced passcodes. Applying firmware and software updates not only introduces new features in some cases but also sometimes fixes security problems.

Encryption

https://t.me/learningnets

Encrypt files (data at rest). If your device uses a file system and OS version that support encrypting files on the hard drive, do so for all files containing sensitive data. That way even if your hard drive is stolen, nobody can view the files without signing in with your credentials. You learned about encrypted files in Chapter 8.

You can also encrypt your entire hard drive with a feature such as BitLocker (in Windows), which makes a hard drive unreadable if removed from the original PC in which it is installed. Smartphones also have encryption options available. On an iPhone, for instance, after setting your passcode, most of the data stored on the phone will automatically be encrypted.

Encrypt network transmissions (data in transit). This happens often, probably without you even noticing. Have you ever banked or shopped online? Accessed your e-mail through a web browser? Most web sites use an SSL (or TLS) certificate to encrypt and digitally sign all transmissions. Encryption feeds plaintext into an encryption algorithm along with a key, which results in encrypted data, otherwise called *ciphertext*.

Nonrepudiation is a term meaning the owner of a private key (stored within an SSL certificate) cannot deny having sent a digitally signed transmission. The reason is simple; possession of the private key is required to *create* the unique signature! It's similar to signing a receipt when you use your credit card to make a large purchase.



EXAM TIP Make sure you can explain why device hardening is important and list several ways to accomplish it.

Users and Passwords

User accounts play a huge role in the security of any computing device. A secure system controls user account types and implements authentication practices such as good password rules. Windows also has UAC to help you secure systems. Let's take a look.

Using Appropriate Account Types

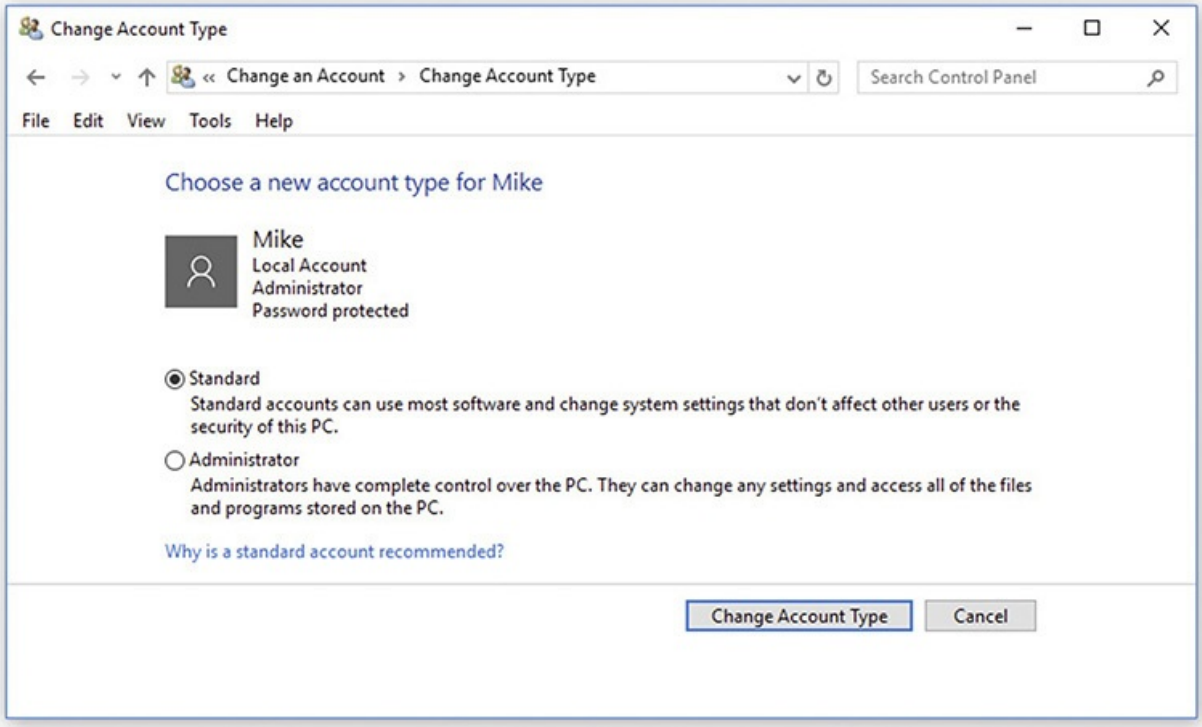
Every desktop/laptop OS enables you to create user accounts and grant different

https://t.me/learningnets

permissions to different kinds of accounts. In Windows, an Administrator account has full permission to do anything, whereas a Standard account can only make changes affecting that one account. Standard accounts can't easily affect other accounts. A Guest account can run only a few applications, such as a web browser, and can't change any settings.

When you install Windows, the first account you create is automatically an Administrator account. You must maintain at least one Administrator account on the computer. For better local security, however, create a Standard account for everyday use. Even if some guy named Jack steals your password and signs in to your Standard user account, he won't be able to harm the system as a whole (although he will be able to delete or change your personal files). Jack won't be able to remove applications or install malware.

Create a new account, set its account type to Standard, and make that your main account. Sign in using an Administrator account only when you need to do something that the Standard account can't do, such as install new applications or make system changes. Figure 11-4 shows the screen in the Control Panel where you would change the account type. To get there, open the Control Panel, choose User Accounts | Change Account Type, select the account, and choose Change Account Type.



https://t.me/learningnets

Figure 11-4 You can change the account you use for everyday activities to a Standard account.

If a guest in your home or business wants to use your PC, have that person sign in using the Guest account. This account has limited permissions, and the user won't be able to do too much damage.



EXAM TIP Make sure you understand the difference between (and appropriate uses for) the Administrator, Standard, and Guest accounts. Note that Microsoft removed the Guest account from Windows 10.

Authenticating Users

Authentication is verifying a user's identity to permit or block certain actions on a system. Most authentication relies on two things you know: usernames and passwords. Because both are *knowledge factors*, we call this scheme *single-factor authentication*. More secure *multifactor authentication* (MFA) schemes add a *possession factor* (such as a key or card that you have) or an *inherence factor* (things you *are*, such as fingerprints, retinal scans, facial recognition). Let's explore how to create and manage passwords for networks, online services, and operating systems.

The following are common examples of authentication factors:

- Username and password.
- PIN (which works only with physical access to a device).
- Hardware token such as a keyfob; a small display shows a numeric code synced with a server. The code is valid for only a short period of time and must be used in conjunction with other factors such as username and password.
- Software token; similar to a hardware token except it is an app.
- Biometric; fingerprints, voice scans, retinal scans.
- Location-based; using GPS coordinates or IP address prefixes, a user must be in a specific geographical region to successfully authenticate.

https://t.me/learningnets

In the following sections, you'll learn how to create and manage passwords. The same basic guidelines apply for both OS passwords and passwords you use on various web sites and online services.

Password Complexity

Always use a *strong password,* one too complicated for bad guys to crack easily. That means not using any words you'd find in the dictionary or encyclopedia—anything that a password-cracking program might try.

In the IT field, generally, a strong password:

- Is at least eight characters long
- Has both uppercase and lowercase letters
- Has numbers and symbols

Examine the following passwords. Can you guess which one is the strongest?

- abc768xyz5
- p1eRsqUred
- Fa$$1on8
- 1haveadreamthatallpeople

The third password wins in security terms. What makes it unique? Of the four, it alone has uppercase and lowercase letters, numbers, and nonalphanumeric characters. And it meets the minimum eight-character threshold.



EXAM TIP Remember that a strong password has at least eight characters and a mix of letters, numbers, and special characters.

Some operating systems enable you to set lockouts for passwords, and many secure web pages use timeouts as well. In Windows 7 and newer, you can set lockouts via the Local Security Policy app (found in the Control Panel under Administrative Tools). In the app, navigate to Security Settings | Account Policies | Account Lockout Policy. To set the number of wrong guesses allowed,

https://t.me/learningnets

set the Account lockout threshold. For the lockout duration, set the Account lockout duration.

Password Confidentiality

Even a strong password is no good if you don't keep it confidential. Don't use the same password for multiple services or web sites. You can use password manager software such as LastPass to securely generate and store passwords in a vault; the password manager itself uses a master password to the vault—don't forget this password! If you forget a password and need to have it reset by an administrator, make sure you change it immediately after logging in. If you're an administrator, force the issue by requiring users to change their passwords when logging in. This creates a temporary *one-time password*, keeping the user safe from any future potential mischief by an administrator.

Along those same lines, when you sign up for an online service or a secure web site, you might be assigned a default password. It's a good idea to change this at your first login to that site. The same is true for any default passwords including for wireless routers, tablets, smartphones—never keep the default password configured.

Password Expiration and Reuse

On some business networks, the network administrators set up password expiration to force users to change their passwords at certain intervals. This helps with overall security because the older a password is, the more likely someone unauthorized has gotten ahold of it. Similarly, these password change policies may prohibit users from reusing the same passwords they have used in the past, so, for example, you can't toggle back and forth between two different passwords each time a change is required.

Password Management

Most companies have a password management policy that establishes rules for several aspects of password usage, including complexity, expiration, and confidentiality. You can create your own password management policies for yourself and your home or small business by thoughtfully creating rules in each of those areas.

For example, you might have a policy like this:

- **Complexity** Passwords must be at least eight characters and must include at least one uppercase letter, one number, and one symbol.

https://t.me/learningnets

- **Expiration** Passwords must be changed every six months.
- **Reuse** Users may not reuse the last three passwords used.
- **Confidentiality** Users may not store passwords in unsecured files on any device; any password file must itself be password-protected. If passwords are stored on paper, the paper must be locked in a secure cabinet or drawer.

Single Sign-on Passwords

On some computer systems, password use is simplified by a single sign-on. That means you sign in once, and then that same authentication is used for multiple purposes. When you sign in to Windows using a Microsoft account, for example, you are also automatically signed into the OneDrive online file storage system. Similarly, many web sites allow you to sign in using your Facebook credentials so that you don't have to create separate accounts.

Single sign-on (SSO) systems can be convenient and can relieve you of the responsibility of remembering multiple passwords. They can also pose a security risk, however, because if the single password is compromised, all its other uses are compromised.

User Account Control

Windows uses *User Account Control* (UAC) to prevent malware or rogue web sites from making system changes without your knowledge and consent. When UAC is enabled (and it is enabled by default) and you attempt to make a system change that would affect other user accounts (such as installing new software), UAC opens a prompt that asks if you really want to do it. You must click Yes to continue. See Figure 11-5.

https://t.me/learningnets



Figure 11-5 User Account Control when signed in to the Administrator account

In addition, if you use a Standard Windows account, UAC will prompt for the PIN or password of the Administrator account before it will allow the change to be made. That way, you don't actually have to sign out of the Standard account and into the Administrator account to provide permission. See Figure 11-6.

https://t.me/learningnets

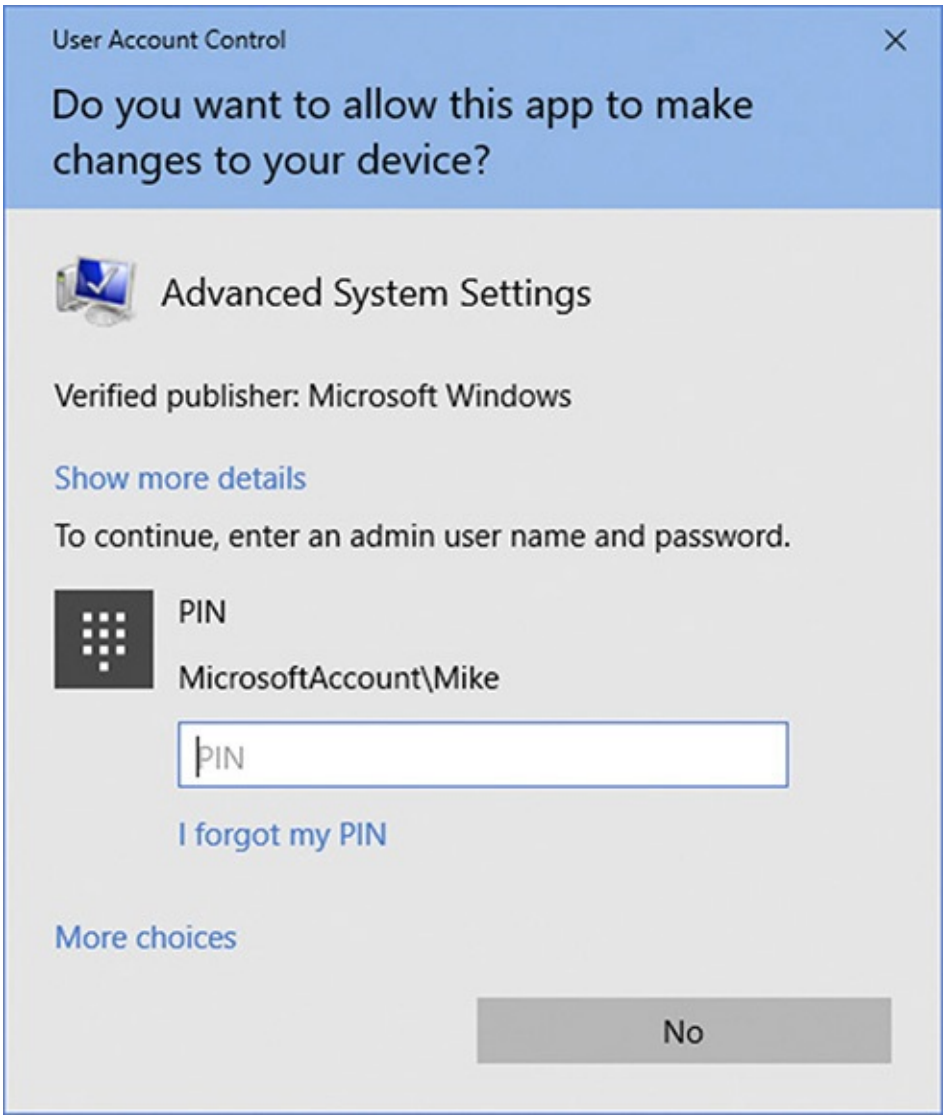


Figure 11-6 User Account Control when signed in as a Standard user

You can adjust the UAC setting from the Control Panel. Choose System and Security, and under the Security and Maintenance heading, click Change User Account Control settings. Drag the slider up or down to control the UAC level. Keep in mind that the highest level may become annoying because of its frequent prompting, whereas the lowest level may not offer adequate protection. See Figure 11-7.

https://t.me/learningnets

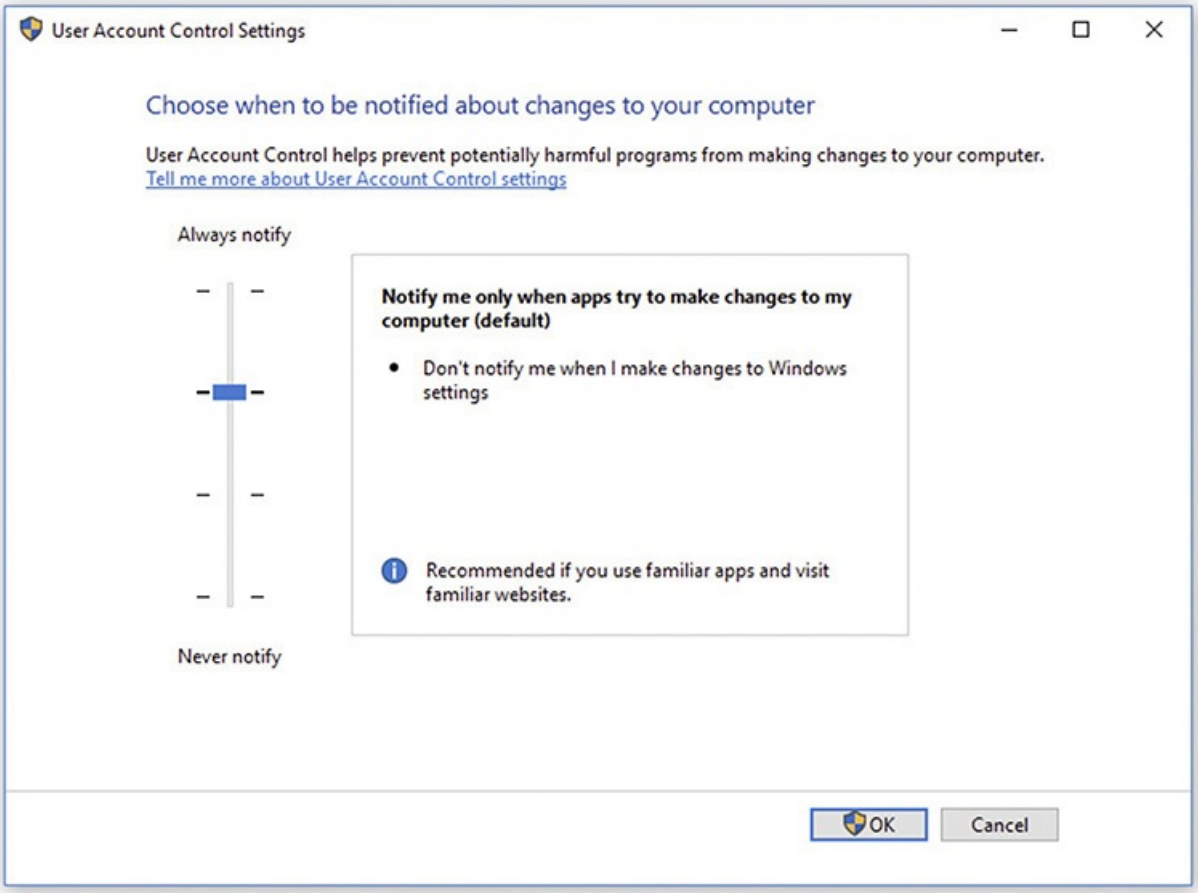


Figure 11-7 Adjust the level of UAC protection.

Malicious Software

The Internet enables you to access resources from just about anywhere on the globe, all from the comfort of your favorite chair. This connection, however, runs both ways, and people can potentially access your computer from the comfort of their evil lairs. The Internet is awash with malicious software —*malware*—that is, even at this moment, trying to infect your systems.



EXAM TIP While a lot of malicious software comes from the Internet or some type of storage device, it can also come from a local area network. Be careful when you connect to open (or free) wireless networks, such as those at

https://t.me/learningnets

coffee shops and bookstores.

Malware consists of computer programs designed to break into computers or cause havoc on computers. Malware uses your computer to do work you don't want it to do—work that usually harms you, benefits someone else, or both. What kind of work? Well, because malware can also use every other resource connected to the device, the only limit we've seen so far is imagination. It could quietly spy on you, hijack your accounts to post bogus reviews, hold your family photos ransom, or force your system to join a cyber-attack against a government server.

This first section looks at common types of malware, such as adware, spyware, and spam. We examine social engineering—attacks that directly manipulate people—and then wrap up with viruses, Trojan horses, and worms.

Adware

Adware is software that displays unsolicited advertisements on your computer. It may come to you in the form of a program that seems helpful, such as a toolbar for your browser, but instead of (or in addition to) whatever it purports to do, it causes ads to display. These ads are usually in the form of pop-ups, although the ads can also show up in other ways.

Adware has three main symptoms that clue you in to its presence: home page redirection, search engine redirection, and constant pop-ups.

- **Home page redirection** The adware changes your home page (the one that loads every time you open your browser). The adware company is hoping you won't know how to change it, and they'll profit from the extra ad views. In some really nasty adware installations, it locks the home page redirection in place, so you can't change back to your preferred page, or your preference is ignored.
- **Search engine redirection** Each browser has a default search engine. When you enter keywords in the Address bar, the default search engine processes them. Adware might change your browser's default to one tailored to serve search results that the company will profit from every time you click.
- **Constant pop-ups** A *pop-up* is an uninvited browser window that "pops up" when you visit certain web sites. Web site designers sometimes code pop-ups into their pages (usually to generate ad revenue), although it's considered bad web manners to do so. In addition, some adware pops up

https://t.me/learningnets

advertisement windows that may or may not have anything to do with the current web site.

Closing a pop-up window can actually be rather tricky. Some pop-up browser windows don't look like browser windows but more like dialog boxes, as in Figure 11-8. Some pop-up browser windows are deliberately designed to mimic OS alerts and dialogs to trick you into clicking them.



Figure 11-8 A pesky pop-up

To avoid clicking in the pop-up window and possibly triggering more ads to appear, use alternate means of closing a pop-up window. For instance, you can right-click the browser's icon in the taskbar and select Close. You can also press ALT-TAB to bring the browser window in question to the forefront and then press ALT-F4 to close it.

The larger question, of course, is how to prevent pop-ups in the future. Most web browsers have features to prevent pop-up ads in the first place. In addition, you can use browser add-ons or extensions (such as Adblock) to block a variety

https://t.me/learningnets

of ads, including pop-ups. Note that some of these blocking programs can interfere with legitimate web site content.

If you see constant pop-ups, you won't be able to control the problem with simple pop-up blockers. The underlying problem is adware infection; these are not normal pop-ups from web pages.



NOTE Browser toolbars from reputable companies (such as Yahoo! and Google) are adware too. They don't display constant pop-ups, but they do change your default home page and search engine to sites that generate revenue for their parent companies. The express or default install options for some free software include one of these "helpful" toolbars (or change your default search engine and home page). Choose the custom install option and pay careful attention to the choices.

When you see any adware symptoms, the first place to look is for some sneaky adware installed as a Windows program, such as a browser toolbar or unknown utility. Open the Control Panel, go to Programs and Features, and scan through the list of programs to find something with *toolbar* in the name, or some utility program that you don't recognize. It's probably an adware program that you have inadvertently installed or that installed itself when you downloaded some software. Try removing it as you would uninstall any application.



CAUTION When removing adware from Windows, the uninstaller might make it difficult for you, so pay attention to the prompts. We've seen all manner of trickiness, including "Are you sure?" messages where the Yes and No buttons are reversed in position from normal.

In other cases, the uninstaller redirects you to a web site where it tries to force you to enter feedback about why you are uninstalling. Use ALT-F4 to close those web sites. Don't click anything.

Some adware acts more like a virus than an application and can't be uninstalled via the Control Panel. In such cases, an anti-malware application may be able to help, or you can try manual removal instructions you find online.

https://t.me/learningnets

See “Anti-malware Programs” later in the chapter.

Spyware

Spyware monitors your computer usage habits and reports the information to the program’s owner. The data collected might be used for minimally intrusive purposes, such as to gather anonymous data about which web sites or browsers are most popular, but some types of spyware go considerably beyond the level of simple data collection.

Sensible people don’t download and install something that they know is going to compromise their computer. Malware developers know this, so they bundle their software with some other program or utility that purports to give you some benefit.

Would you like free access to movies, music, or games that you would normally have to pay for? Could you use a handy *e-wallet* utility that remembers your many screen names, passwords, and credit-card numbers to make online purchases easier and faster? How about browser enhancements, performance boosters, custom cursor effects, search utilities, buddy lists, file savers, or media players? Programs for *any* purpose could simply be window dressing for the *real* purpose of the software. You see, for the most part, malware doesn’t need to force its way into your PC. Instead, it saunters calmly through the front door.



CAUTION Plenty of sketchy software-download sites repackage legitimate software made by others with malware. Even if you recognize the name of the program and its developer, make sure you download the software itself from a reputable site.

Some spyware makers use more aggressive means to get you to install their software. Instead of offering you some sort of attractive utility, they instead use fear tactics and deception to try to trick you into installing their software. One popular method is to use pop-up browser windows crudely disguised as Microsoft’s own system warnings. When clicked, these may trigger a flood of other browser windows or may even start a file download. An even worse type of spyware installs a *keylogger* utility, which records every keystroke you make, including when you type usernames and passwords.

https://t.me/learningnets

The lesson here is simple: *don't install these programs!* Careful reading of the software's license agreement before you install a program is a good idea, but realistically, it does little to protect your PC.

Use anti-malware software to remove spyware. See the section "Protecting Against Malware" later in the chapter to see the steps.

Spam

E-mail that comes into your inbox from a source that's not a friend, family member, or colleague, and that you didn't ask for, can create huge problems for your computer and you. This unsolicited e-mail, called *spam*, accounts for a huge percentage of traffic on the Internet. Spam comes in many flavors, from real businesses trying to sell real products to scammers who just want to take your money (Figure 11-9). Hoaxes, pornography, and get-rich-quick schemes pour into the inboxes of most e-mail users. They waste your time and can easily offend.

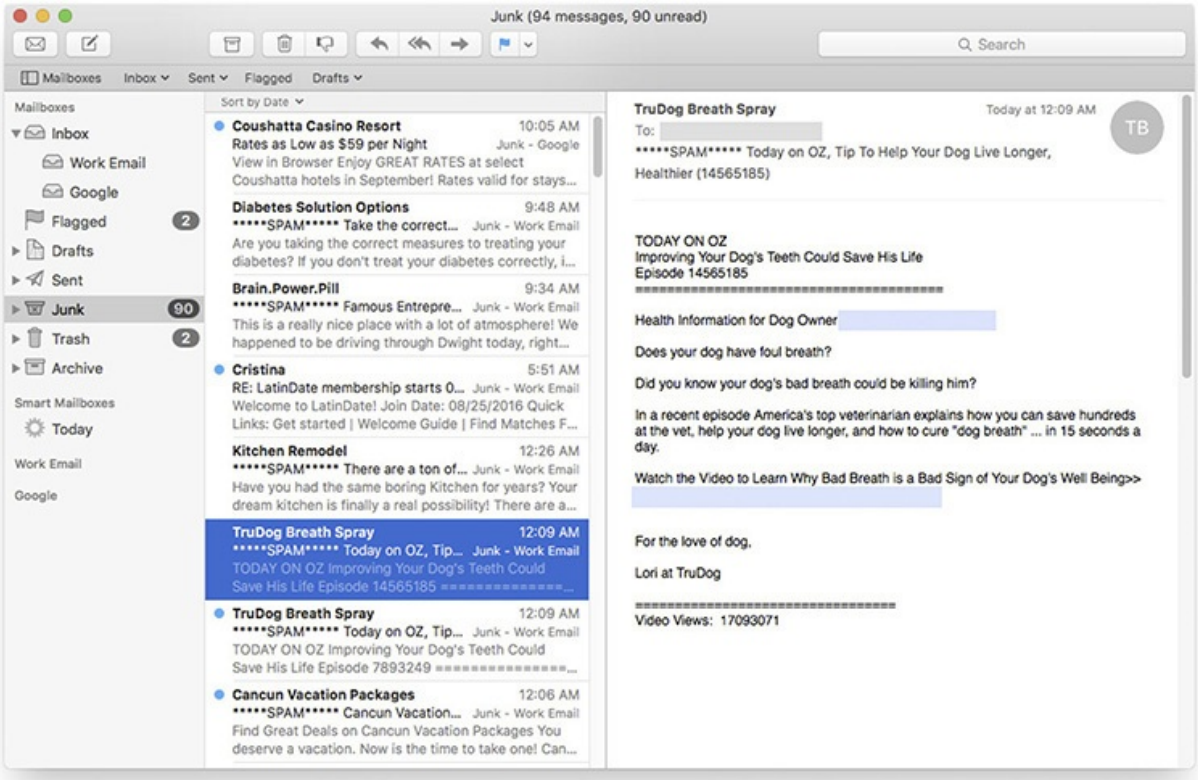


Figure 11-9 A spam message

https://t.me/learningnets

Even e-mail that comes from a friend can contain spam. If a friend's e-mail address is hijacked or his computer is infected with malware, it might send out spam from his e-mail account without permission. When you get it, you think he is the source, so you are less careful than you ought to be. If a message seems to come from a friend but doesn't sound like that friend, call or text them and ask if they really sent it.



CAUTION The Unsubscribe link in some spam doesn't actually unsubscribe you from anything; instead, it just confirms that your e-mail address is valid, and you get more spam. On the other hand, commercial messages from mainstream retail sites usually have a reliable unsubscribe link in them. It's sometimes a tough call to know how to proceed. If you have any doubts about the origin of an e-mail, it's best to delete it.

You can use several options to cope with the flood of spam. The first option is defense. Never post your e-mail address on the Internet. One study tested this theory and found that *more than 97 percent* of the spam received during the study went to e-mail addresses that had been posted on public web sites.

Filters and filtering software can block spam at your mail server, at your service, or at your computer. You can set most e-mail programs to block e-mail from specific people—good to use if someone is harassing you. You can block by subject or keywords.

Social Engineering

Social engineering is the process of using or manipulating people to gain access to that network from the outside—which covers the many ways humans can use other humans to gain unauthorized information. It can include situations that have nothing to do with computers, such as a phone call that claims to be from your credit card company and asks you to verify your Social Security number. The unauthorized information being gathered may be a network login, a credit card number, company customer data—almost anything you might imagine that one person or organization may not want others to access.

Social engineering attacks aren't hacking—at least in the classic sense of the word—although the goals are the same. Social engineering means people

https://t.me/learningnets

attacking an organization through the people in the organization or physically accessing the organization to get the information they need. The following are a few of the more classic types of social engineering attacks.



NOTE It's common for multiple social engineering attacks to be used together, so if you discover one of them being used against your organization, it's a good idea to look for others.

Infiltration

Attackers can physically enter your building under the guise of someone who might have a legitimate reason for being there, such as cleaning personnel, repair technicians, or messengers. They then snoop around desks, looking for whatever they can find. They might talk with people inside the organization, gathering names, office numbers, and department names—little things in and of themselves, but powerful tools when combined later with other social engineering attacks. This is called *infiltration*.

Dressing the part of a legitimate user—with fake badge and everything—enables malicious people to gain access to locations and thus potentially to your data. Following someone through a door as if you belong, what's called *tailgating,* is a common way to infiltrate.

Telephone Scams

Telephone scams are probably the most common social engineering attack. In this case, the attacker makes a phone call to gain information. The attacker attempts to come across as someone inside a trusted organization and uses this to get the desired information.

Probably the most famous of these scams is the "I forgot my password" scam. In this gambit, the attacker first learns the account name of a legitimate person in an organization, usually using the infiltration method. The attacker then calls someone in the organization, usually the help desk, in an attempt to gather information, in this case a password.

> **Hacker:** "Hi, this is John Anderson in accounting. I forgot my password. Can you reset it, please?"
>
> **Help Desk:** "Sure, what's your username?"

https://t.me/learningnets

Hacker: “j_w_Anderson.”
Help Desk: “OK, I reset it to e34rd3.”

Telephone scams aren’t limited to attempts to get network access. There are documented telephone scams aimed at getting cash, blackmail material, or other valuables.

E-mail Phishing

Phishing is the act of trying to get people to give their usernames, passwords, or other security information by pretending to be someone else electronically. A classic example is when a bad guy sends you an e-mail that’s supposedly from Twitter or Instagram saying that your account is on hold for some violation and you need to click the login link provided in the e-mail to straighten out the problem. Banking scams are also very popular, as shown in Figure 11-10.

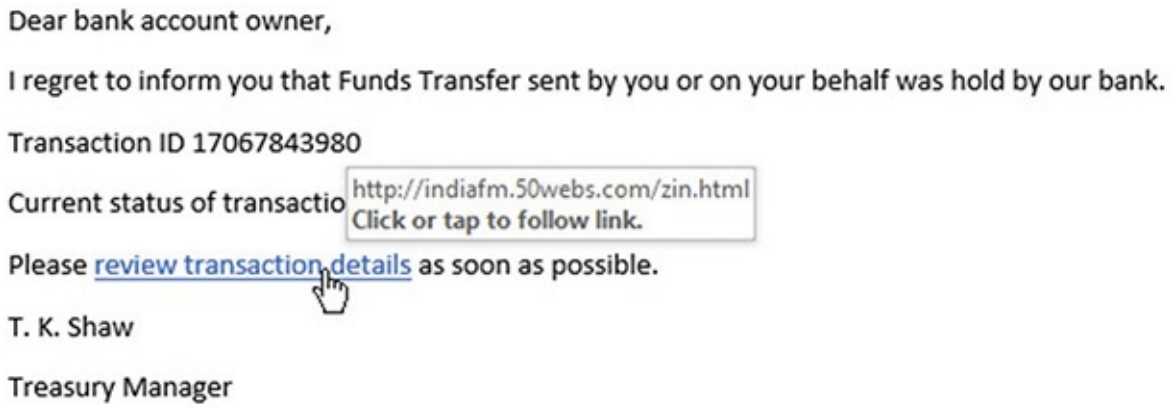


Figure 11-10 A phishing message

A phishing e-mail might contain a hyperlink that appears to point to a legitimate destination but actually points to a server run by the phisher. In Figure 11-10, for example, notice how the underlined text in the e-mail says one thing, and when you hover the mouse pointer over the link, the pop-up showing the actual address says quite another thing. Here are some other clues in this message that it is not legitimate:

- It does not identify the recipient by name in the body of the message.
- The banking institution is not named. There is no business name after the signature line.
- The first sentence contains a grammatical error (“was hold by our bank”).

https://t.me/learningnets

Security Messages: Fake and Real

Another way social engineering scammers try to trick users is by popping up fake security alerts. When you view a web site, for example, a pop-up might appear saying that your computer has been infected by malware, prompting you to click a link to download a malware removal utility. It's fake, though—you don't have malware yet. If you click that link, one of two things will happen: you will actually *get* malware of some sort or someone will try to sell you software that will "fix" a problem that doesn't exist.

It can be difficult to distinguish such messages from legitimate security software alerts. If in doubt, shut down all browser windows by right-clicking their icons on the taskbar and choosing Close. If the alert persists, it was not generated by a pop-up. Next, verify the warning is from a security application you actually have installed. Look in the Control Panel in the Programs section to see whether the program names match.

It's important to act on *legitimate* security software alerts instead of ignoring them, so close the alert window, open the full version of the security software, and run a full system scan. If the error reappears, it's probably legitimate. Illegitimate alerts are a good hint your device has malware.

Viruses

Just as a biological virus gets passed from person to person, a computer *virus* is a piece of malicious software that gets passed from computer to computer. A computer virus is designed to attach itself to a program on your computer and execute when the program executes. It could be your e-mail program, your word processor, or even a game. Whenever you use the infected program, the virus goes into action and does whatever it was designed to do. It can wipe out your e-mail or even erase your entire hard drive! Viruses are also sometimes used to steal information or send spam e-mail to everyone in your address book.

Trojan Horses

Trojan horses (sometimes just called *Trojans*) are freestanding programs that do something other than what the person who runs the program thinks they will. Much as the Trojan horse in antiquity, you invite these programs in, unaware of what lurks inside. An example of a Trojan horse is a program that a person thinks is an antivirus program but is actually a virus. Some Trojan horses are quite sophisticated. It might be a game that works perfectly well but causes some type of damage when the user quits the game.

https://t.me/learningnets

Worms

Similar to a Trojan horse, a *worm* is a complete program that travels from machine to machine, usually through computer networks. Most worms are designed to take advantage of security problems in operating systems and install themselves on vulnerable machines that might not have the latest updates applied. They can copy themselves over and over again on infected networks, potentially creating so much activity that they overload the network by consuming bandwidth. A fast-spreading worm might even bring chunks of the entire Internet to a halt.

Ransomware

One particularly nasty type of malware, *ransomware*, locks down your computer and holds it for ransom, displaying some threatening warning that if you don't pay up (usually by sending money via wire transfer), your files will be deleted. Some smoke-and-mirrors ransomware doesn't actually harm your PC beyond locking it down until you pay or remove the ransomware; other versions actually do delete files. What differentiates this from most types of malware is that it's not a sneaky attack. It's blatant, obvious extortion. Figure 11-11 shows an example. This type of malware is usually spread via infected .zip files sent as e-mail attachments.



https://t.me/learningnets

Figure 11-11 A ransomware warning (courtesy of Motormille2 at Wikimedia Commons, CC BY-SA 4.0)

There are three basic types of ransomware: scareware, lock-screen, and encryption.

- **Scareware** This is ransomware that just scares you. It tries to sell you bogus antivirus or cleanup tools to fix a problem that doesn't exist. You can still use your PC but you might be bombarded with pop-ups, or you might be prevented from running programs. These are the easiest to remove.
- **Lock-screen** This type doesn't allow you to use your PC in any way. It shows a full-size window warning you that you have violated the law and must pay a fine. Figure 12-4 shows this form.
- **Encrypting** This is the worst stuff because it encrypts and locks your personal files until you pay. Even if you manage to remove the malware, your files are useless without the decryption key, which you can't get without paying.

Protecting Against Malware

You can do several things to protect yourself and your data against online threats. First, keep the OS patched. Second, make sure your computer runs up-to-date anti-malware software, especially if you connect to the Internet via an always-on broadband connection. You should also be protected by a firewall, either as part of your network hardware or by means of a software program. (See the sections on anti-malware programs and firewalls coming up in this chapter.)

Windows Update

Because malware can infect systems through security flaws in operating systems, the next defense against them is to make sure you have the latest security patches installed on your version of Windows. A *security patch* is an addition to the operating system to patch a hole in the operating system code. Keeping your patches up to date, called *patch management,* goes a long way toward keeping your system safe.

Microsoft's Windows Update tool is handy for Windows users because it provides a simple method to ensure that your version's security is up-to-date.

https://t.me/learningnets

Windows Update is set to download and install updates automatically by default. (You should not change that setting unless specifically directed to do so by your IT department.) You might occasionally be prompted to give permission to install a certain update, but for the most part, Windows Update works silently and automatically behind the scenes.

You can adjust Windows Update settings through the Control Panel or the Settings applet (in Windows 10). You can configure several settings.

- **Change active hours** Windows will not automatically restart between the hours you specify here, so an update won't interrupt your work.
- **Restart options** When a restart is scheduled, this option is available to specify an exact restart time (on a one-time basis).
- **Advanced options** Here you can choose whether to also receive updates for Microsoft applications with Windows Update.



NOTE Application updates were covered in Chapter 9.

Anti-malware Programs

An *anti-malware* program, such as a classic *antivirus program*, protects your PC in two ways. It can be both sword and shield, working in an active seek-and-destroy mode and in a passive sentry mode. When ordered to seek and destroy, the program scans the computer's files for viruses (as shown in Figure 11-12) and, if it finds any, presents you with the available options for removing or disabling them. Antivirus programs can also operate as *virus shields* that passively monitor your computer's activity, checking for viruses only when certain events occur, such as a program executing or a file being downloaded.

https://t.me/learningnets

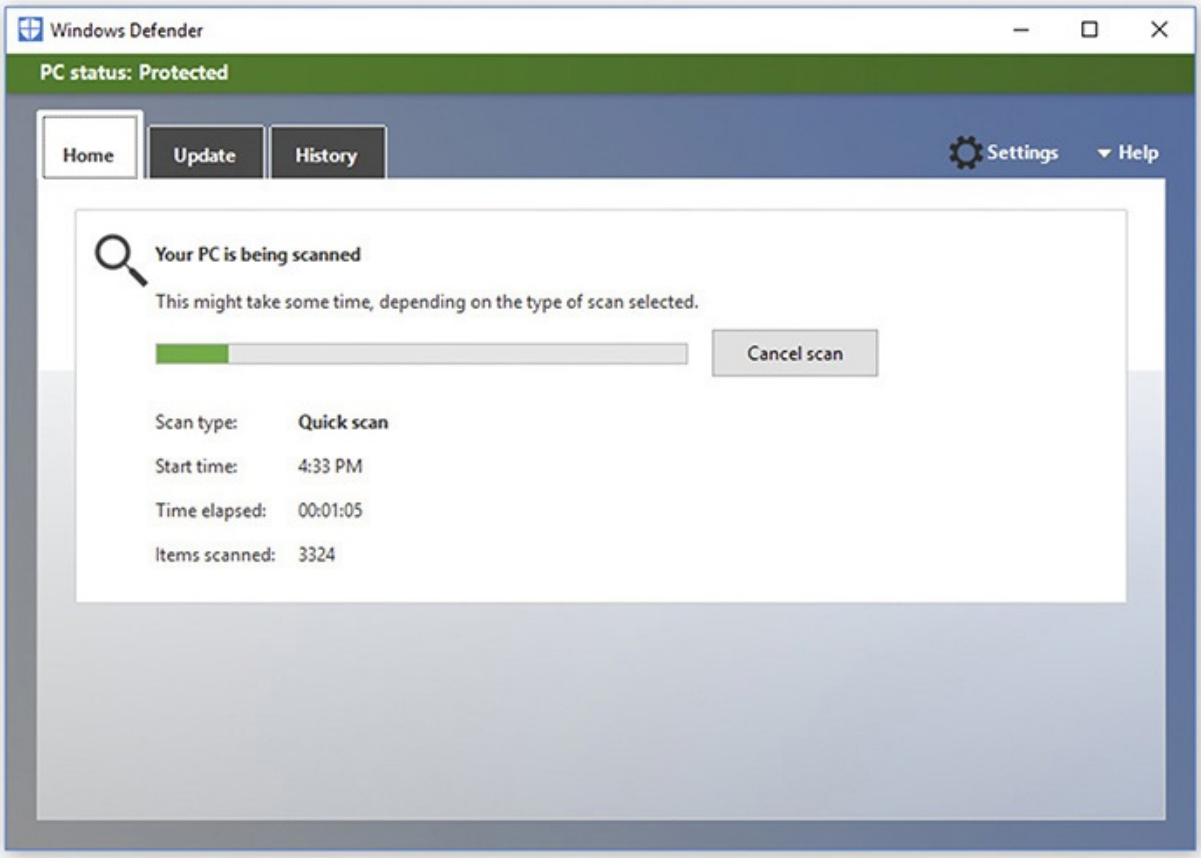


Figure 11-12 Windows Defender scanning Windows 10 for viruses and other malware

The antivirus program uses a library of signatures to detect viruses. A *signature* is the code pattern of a known virus. The antivirus program compares an executable file to its library of signatures. Sometimes a perfectly clean program coincidentally holds a virus signature. Usually the antivirus program's creator provides a patch to prevent further false alarms.



NOTE The term *antivirus* (and *antispyware*, or anti-anything) is becoming obsolete. Viruses are only a small component of the many types of malware. Many people continue to use the term as a synonym for anti-malware.

Malware Prevention Tips

https://t.me/learningnets

The secret to preventing damage from a malicious software attack is to keep from getting malware in the first place. As discussed earlier, all good anti-malware programs include a malware shield that scans e-mail, downloaded files, running programs, and so on, automatically.

Know the source of any software before you load it. Although the chance of commercial, shrink-wrapped software having malware is virtually nil (there have been a couple of well-publicized exceptions), that illegal copy of *Modern Warfare 3* you downloaded might really make you *pay*. Be very careful with e-mail attachments and hyperlinks. If the e-mail they arrive in is even remotely suspicious, don't open, click, or download them. Even if the e-mail is from a good friend, be cautious: your good friend's device or account could be compromised.

Keep your anti-malware program updated. New malware programs appear daily, and your program needs to know about them. The list of virus signatures your anti-malware program can recognize is called the *definition file*, and you must keep that definition file up-to-date so that your antivirus software has the latest signatures. Fortunately, most antivirus programs update themselves automatically. Further, you should periodically update the core antivirus software programming—called the *engine*—to employ the latest refinements the developers have included.

Malware Recovery Tips

When the inevitable happens, you need to follow certain steps to stop the malware from spreading and get the computer back into service safely. Here's a good five-step process:

1. Recognize.
2. Quarantine.
3. Search and destroy.
4. Remediate.
5. Educate.

Recognize

The first step is to recognize that a potential malware outbreak has occurred. For example, if the computer was running snappily the day before but seems sluggish today, it could be a symptom of a virus or other malware attack.

https://t.me/learningnets

Quarantine

Malware can spread, so you need to quarantine the infected computer to cut it off from the rest of the network. One easy method for doing this is to disconnect the network cable from the back of the system and disable any wireless adapters. Once you are sure the machine isn't capable of infecting others, you're ready to find the malware and get rid of it.

Search and Destroy

Once you've isolated the infected computer (or computers), you need to find the malware using an anti-malware application and allow the application to remove it. The process varies among the various anti-malware tools available. Follow the developer's instructions that apply to your OS.

E-mail is still a common source of malware, and opening infected e-mail is a common way to get infected. Viewing an e-mail in a preview window opens the e-mail message and exposes your computer to some malware. Download files only from sites you know to be safe; the less reputable corners of the Internet are the most likely places to pick up computer infections.

Remediate

Malware can do a lot of damage to a system, especially to sensitive files needed to load Windows, so you might need to remediate formerly infected systems after cleaning off the drive or drives. *Remediation* simply means that you fix things the malware harmed. This usually means replacing corrupted or destroyed files with your backups—you did make backups, right? The Backup and Restore applet in the Windows Control Panel will walk you through restoring the backed-up files to your PC. Time Machine in macOS can likewise restore damaged or missing files.

Educate

The best way to keep from having to deal with malware is education. Educate other people in your home or office who may be inadvertently putting their own computer and others at risk, explaining what you have learned in this chapter. Any user who understands the risks of questionable actions on their computers will usually do the right thing and stay away from malware.



https://t.me/learningnets

NOTE If, at any point, you don't think you can fix the problem or are unsure if you completely removed the malware, be sure to *escalate* the issue. Escalation is the process of handing off your task to someone else, such as an IT professional. For example, you might decide that you need to hire an expert to come to your home or take your computer to a repair shop.

Network Threats

There are other ways that the bad guys can wreak havoc on your computer or even on your entire network. Sometimes you can control inbound traffic to your network, but if you're hosting a publicly visible web site, you need to allow incoming TCP port 80 and possibly 443 traffic. Attackers can take advantage of these types of situations.

Eavesdropping

There are plenty of freely available packet sniffing (also called *capturing*) tools such as Wireshark. Given that you are on a network where all traffic is visible, you can capture network traffic and then analyze it for troubleshooting, performance, or security reasons. This is analogous to wiretaps on phone lines to listen in on conversations.

Man-in-the-Middle Attacks

Capturing existing network conversations is often the first step in a man-in-the-middle (MiTM) attack where the attacker system impersonates, or assumes the identity of, one machine in the network conversation. The attacker could then potentially modify and then replay captured traffic.

Bear in mind that laws vary by jurisdiction; capturing network traffic might be frowned upon, even on open networks. Encrypting network traffic with TLS or by other means such as a virtual private network (VPN) will still allow the traffic to be captured, but attackers wouldn't be able to make sense of the data because the packet payloads are encrypted.

VPNs connect two endpoints over the Internet and create an encrypted transmission tunnel, such as from an off-site user to a corporate network or across two corporate networks that are connected. All traffic sent through the VPN tunnel is encrypted as it traverses the Internet, but it is decrypted after going through the target VPN device.

https://t.me/learningnets

Denial-of-Service Attacks

Intentionally preventing the legitimate use of an IT service is considered denial of service (DoS). This could be something as simple as crashing a remote server by sending it a specially crafted network packet or even just intentionally unplugging the power cord if you have local access! Some DoS attacks can even *brick* hardware devices. Bricking a device adversely affects the electronics or firmware in a device so that it no longer functions—it just sits there like a brick.

When multiple systems under the attacker's control (often called a *botnet* or *zombienet*) are used to render a service such as public web site unresponsive, by flooding it with large volumes of network traffic, a *distributed* DoS (DDoS) is said to have occurred.

DDoS attacks could target a single host, a group of hosts, an entire corporate network, or even a cloud-based service such as Google Apps. Often, attackers will demand ransom payment to cease a DDoS attack.

But what can be done about DDoS attacks? They normally stem from benign infected systems under the attacker's control. There are companies that specialize in DDoS mitigation techniques. Let's say a DDoS attack has been started against www.fakegetrichquick.com. In some cases simply modifying a DNS A record for the host to point to an invalid IP address can redirect the DDoS; however, that also means legitimate users won't be able to connect to www.fakegetrichquick.com. Blocking port 80 or 443 isn't great for the long term either; that's how people connect to the web site!

Common solutions often include monitoring the amount of traffic sent within a short period of time to a single destination and taking steps to block traffic from those hosts.

Being a Smart Web User

Many of the ways you can protect your system while browsing the Web aren't tied to any particular setting but are instead a combination of being skeptical and understanding what you are seeing. The following sections explain some best practices for browsing.

Understanding the Risks of Public Workstations

In many places, such as hotel lobbies, conference centers, and libraries, you may find public workstations that anyone can use to access the Internet and run basic applications. Use these with great caution. You never know what malware lurks

https://t.me/learningnets

there. An unsupervised terminal could even contain a keylogger program that can steal usernames and passwords. The company providing the terminal is probably not out to steal your data, but if the workstation's maintenance and upkeep is left to unqualified staff who don't know how to lock down the security on a workstation, any public user can accidentally or intentionally install malware on it.

Public workstations also pose privacy risks. Some browsers are set to automatically remember the text you enter into form fields, so they could remember your name, address, and even credit card data for the next person to see who sits down at that workstation. Other users can also review the history in the browser to see what web sites you have used.

When using a browser on a public workstation, your best bet is to use the high-privacy mode for that browser. In Internet Explorer and Microsoft Edge it is called InPrivate Browsing (see Figure 11-13), and you activate it by pressing CTRL-SHIFT-P or pressing ALT-T to open the Tools menu and then clicking InPrivate Browsing. In this high-privacy mode, nothing about your session is retained in the browser: no form fields, no history, no temporary files. An InPrivate session continues until you close its window. Some other browsers have their own high-privacy modes. For example, in Google Chrome the feature is called Incognito Window.

https://t.me/learningnets

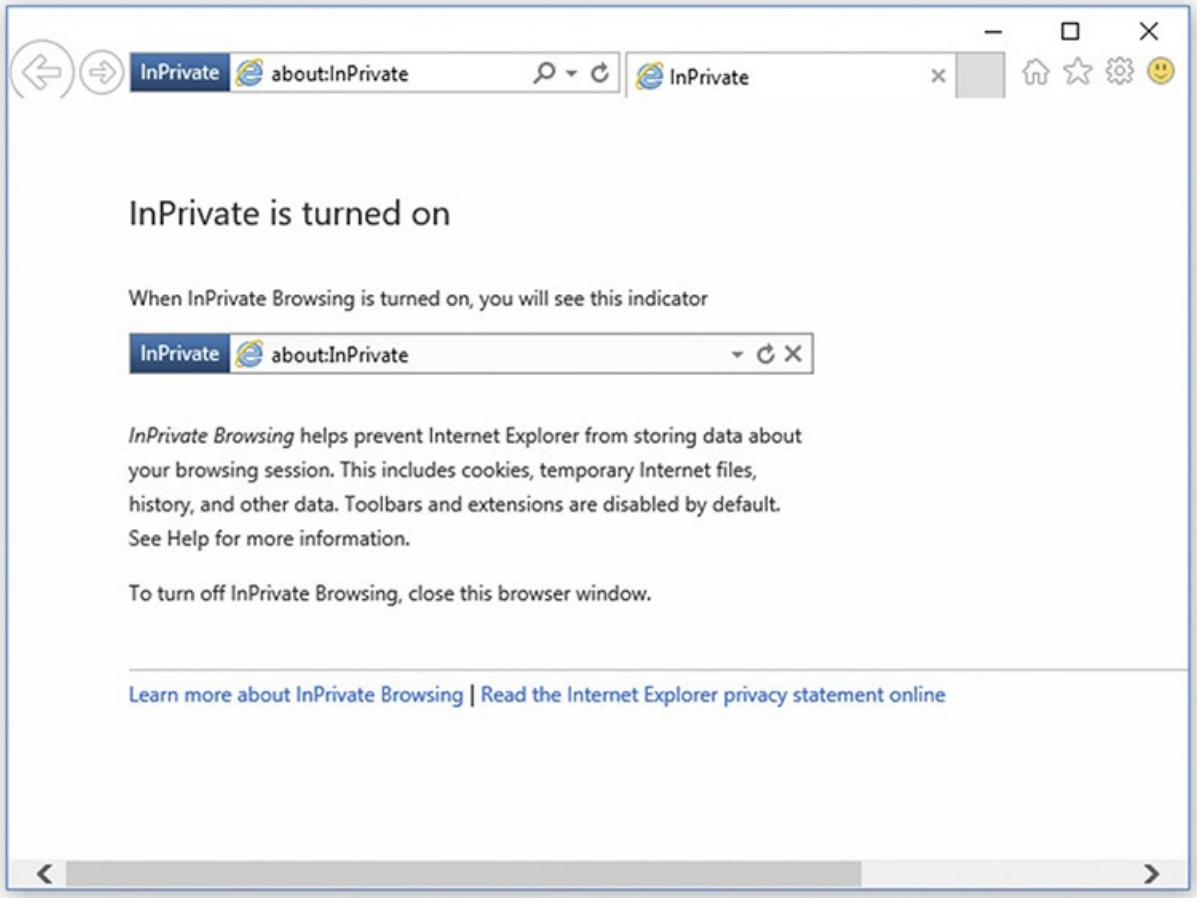


Figure 11-13 InPrivate Browsing protects your privacy as you use a public workstation.



NOTE You can use high-privacy settings in just about every browser, including the ones on mobile devices. Apple Safari and Mozilla Firefox both enable you to open a private session by selecting File | New Private Window. Safari in iOS has a Private toggle button to go into Private Browsing mode.

Playing Smart with Secure Web Sites

You should enter private information (such as credit card numbers) only on secure, trusted web sites. A *secure* site is one that encrypts the transmission between you and the web site so that it cannot be intercepted and snooped along the way. A *trusted* site is one that you trust will not do anything illegal or

https://t.me/learningnets

unethical with the information you provide.



NOTE It is much easier to determine whether a site is secure than whether you should trust it. Anyone can set up a secure site and prove that it is secure, but trust is more subjective. Will that online merchant safeguard your credit card data adequately? Will they sell your contact information to a marketing company? That's where reference organizations like the Better Business Bureau come in.

Recognizing a Secure Web Site

A secure web site uses encryption protocols (rules) to create secure communications between your computer and the server hosting the web site. One popular protocol is *Transport Layer Security* (TLS); it is a modern update of the older *Secure Sockets Layer* (SSL) protocol. A web site address that uses SSL or TLS starts with *https://* (which stands for Hypertext Transfer Protocol over SSL) instead of http://. So, one way to recognize a secure site right off the bat is to look for https:// in the address bar.

Another clue that a web site is secure is a lock symbol in or near the address bar. In some browsers, the address bar turns green when using a secure URL. Figure 11-14 shows a secure URL in Internet Explorer.



Figure 11-14 A secure URL



EXAM TIP You should be able to recognize the signs of a secure connection in a browser window, including https:// and the lock symbol.

Recognizing Invalid Certificate Warnings

Encrypted transmission by itself doesn't guarantee *who* you are communicating with, so the identity of a secure site is authenticated by a digital certificate. In

https://t.me/learningnets

other words, you know that when you receive data from PayPal.com, it's really from PayPal.com and not from some rogue site intercepting the transmission and pretending to be PayPal. When a company sets up a secure web site, they buy a certificate from a certificate authority.

When you visit a secure web site, your browser asks for verification from the certificate authority that the secure site is authentic. If all goes well with that transaction, it's invisible. However, if there's a problem with the certificate, you might see a certificate warning. It might report, for example, that the certificate has expired or the name on the certificate doesn't match the name sent with the request.

In some cases, a certificate warning can be safely dismissed, especially if it's for a company you know to be reputable and the warning is about a minor issue like the name not matching exactly. However, if it's for a company you don't know and trust or if anything looks amiss with the web site, be cautious about providing any personal or financial information on that site. If the error is that the security certificate was not issued by a trusted certificate authority or was issued for a different web site's address, that could indicate a fraudulent site.

Recognizing Untrusted Source Warnings

In the course of your web browsing, you might see a message when attempting to open a web page that the source is untrusted, as in Figure 11-15. Depending on the browser and the exact problem, this warning may be worded in a number of ways.

https://t.me/learningnets

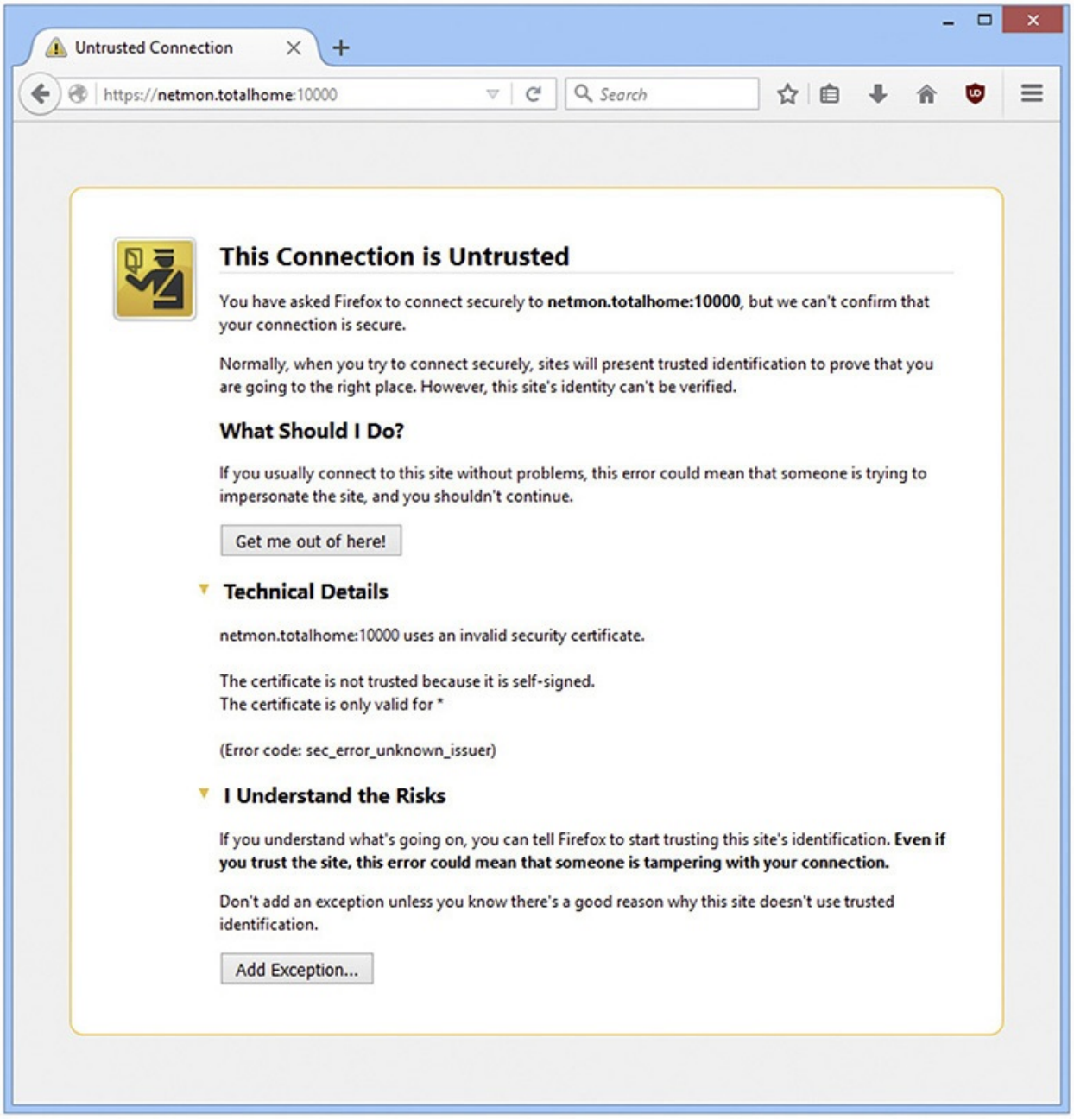


Figure 11-15 A certificate warning may be harmless, or it may indicate a fraudulent site.

A source (that is, a web site) may be untrusted for any of several reason. Its certificate may not have been issued by a trusted certificate authority. It might be a known phishing site that your browser (or a security add-on) has on its “do not trust” list. The web site might attempt to load software when you visit it, which is suspicious and triggers some browsers to warn you.

https://t.me/learningnets

Pay attention to these warnings! If there is any doubt about the site's safety (or you don't understand the warning), do not proceed.

Recognizing Suspicious Links

On a web site or in an e-mail message, there are a number of ways to spot a hyperlink that is likely to get you into trouble.

First, take a look at the address that the hyperlink really points to. Hover the mouse pointer over the hyperlink to see the actual URL, either in a pop-up ScreenTip or in the browser's status bar at the bottom of its window.

Beware of URLs that use an IP address instead of a domain name. Domain Name System (DNS) is a lookup service that translates URLs into IP addresses. Usually when someone uses the IP address, they're trying to make it hard for you to see the domain name for some reason.

When evaluating a URL, find the first single / in the address and read backward from there to see the domain name of the site. For example, in http://answers.yahoo.com/question/index;_ylv=3, the first slash comes after .com. The text immediately before that slash is yahoo.com, which is a well-known site, so this URL is probably safe.

On the other hand, if there is some other domain name before the first slash, it is probably a fraudulent site. Here is an example:

http://hackerz.com/chaseonline.chase.com/survey.html

In that one, even though the URL contains a legitimate domain name (chase.com), it's not before the *first* slash. This URL would actually direct you to hackerz.com.

Here's another example:

http://www.chase.com@209.131.36.168/survey.jsp

Yes, this example includes chase.com, but immediately before the slash is an IP address, not the domain name. Remember, whatever is immediately before the first slash is the actual site.

Here's another one:

http://onlinebanking-chase.com/survey.php

This one does have chase.com immediately before the slash, but look closely. The actual domain is onlinebanking-chase.com, which is an entirely different

https://t.me/learningnets

domain that has nothing to do with the real chase.com.

Be careful also of variants that look right at a glance but are actually malformed, like these:

- wwwchase.com
- www-chase.com
- www.chasecom.com
- chase.com.cc
- www.chase.com-sweepstakes.info



EXAM TIP Given a link, you should be able to point out characteristics in the address that make you suspect that it either is or isn't fraudulent.

Recognizing Suspicious Banner Ads

Banner ads are the advertisements that appear along the top or side of a web page. They are third-party ads, not provided by owner of the site you are visiting. For the most part, they are harmless. They generate ad revenue for the site owner so he or she can afford to keep the web site running. However, some unscrupulous malware distributors have been known to use banner ads, even at well-known, trusted web sites, to spread nasty malware, including ransomware.

There are no ironclad ways to tell whether a banner ad is legitimate just by looking at it. If a banner ad promises something that sounds too good to be true, however, or is obviously trying to manipulate you into clicking it by dangling some tantalizing piece of information in front of you, be wary. Watch also for poor-quality, low-resolution graphics in the banner and for ads that seem oddly placed (for example, a banner ad for "adult content" on a site that sells children's toys). Banner ad space is sometimes sold on a clearinghouse basis, where the actual company purchasing the ad space is not the company that chooses and places the ad there. A legitimate site could contract with a legitimate banner ad company, which could in turn subcontract that space to a company that had malicious intent, and nobody would notice until people started getting phished or scammed.

You can protect your computer from banner ads with malicious content by not clicking them. You can also minimize your risk by uninstalling any third-party

https://t.me/learningnets

browser extensions that you don't use, such as Adobe Flash, Oracle Java, and Microsoft Silverlight. It's also important to install updates for your browser as soon as they become available and to use the 64-bit version of your browser if possible.

Limiting Use of Personally Identifiable Information Online

It's amazing how much *personally identifiable information* (PII) a determined sleuth can find out about you online. There are databases that have your phone number, your current and last several addresses, your employers, and even your government records like parking tickets and arrests, available to anyone with a credit card.

Organizations handling sensitive information about people are often governed by laws and regulations that determine how confidential data should be handled. For example, the PCI DSS security standard applies to merchants dealing with credit and debit cardholder information, and there are guidelines that specify how the networks related to this information should be secured.

You can't stop people from searching public records, so it's difficult to keep your personal information off the Internet entirely. You don't have to volunteer it up to anyone who asks. Even though there is no real way to guarantee full privacy on the Internet, here are some tips for limiting the amount of personal information you share online:

- Have a separate e-mail address that you use only for filling in online forms and making online purchases. Don't use your main e-mail address. This will help minimize the amount of spam you receive.
- When asked to enter a phone number in an online form, unless you are making a purchase, use a fake phone number, or use 000-000-0000. The same goes for entering a mailing address. If you're not making a purchase, they don't need to know where you live.
- When a site asks for your birthdate, indicate that you are younger than 13. It is illegal in many places for marketers to market to people younger than 13, so they will exclude you from any marketing they send out. (Of course, don't do this if you are visiting a site that has a minimum age to use the site.)
- Look yourself up on sites that offer personal information about people and see whether there is a way to have your information removed. Most such sites will remove your data if you go through the proper channels to make such a request.

https://t.me/learningnets



EXAM TIP You should be able to identify the risks involved in putting personal information on the Internet and some strategies for minimizing your exposure while still participating in online activities.

Updating Browsers and Plug-ins

Most malware that comes through a web browser does so because of exploits from out-of-date browser software or plug-ins. The classic *plug-ins* added functionality to early web browsers for various purposes. Some enabled you to access more interactive features of a site that supported those plug-ins. Most modern browsers don't use them (see "Disabling Unneeded Plug-ins, Toolbars, and Extensions" later in the chapter for more details).

It's essential, therefore, that you keep browsers updated, installing the latest versions whenever they become available. Windows Update will update the Internet Explorer and Microsoft Edge browsers automatically for you. Other browsers may update themselves automatically when you run them. In Google Chrome, you can check whether your version is up-to-date by choosing Tools | Settings | About. In Mozilla Firefox, choose Tools | Options | Advanced | Update to get to a screen where you can enable or disable automatic updates.

While we're on the subject of browsers, note that *legacy browsers* (that is, older versions of the browser) suffer from all of the same security risks as an un-updated browser of the current version. For example, if you're using a computer with Windows XP on it, you're probably using Internet Explorer 7, which is woefully underprepared for today's web security threats. In some cases, you can install a newer browser version, but in old operating systems you cannot go past a certain level.

Configuring Browser Security and Privacy Settings

Some of the settings for your browser are purely superficial; you can customize the size and type of fonts used on web sites with your own styles. But you also have power over privacy and security features such as cookies, the Internet cache, and add-ons that enhance the abilities of your browser. Browser proxy settings funnel outbound traffic through a proxy server which can allow or deny specific connections. If these settings are configured improperly, you may be opening yourself up to outside attacks. The exact names of the settings and the

https://t.me/learningnets

processes of accessing them vary between browsers; in this chapter we examine them in Internet Explorer.

Adjusting Browser Security Settings

In a browser context, *security* means the ability to prevent your computer from being harmed by malware. When you crank up security settings, you minimize the chance that visiting web site with malicious code will infect your computer and cause problems. High security settings may prevent some web sites from performing as intended, though; for example, some shopping sites won't work with security settings at their highest levels such as disabling client-side scripting, which is used by some web sites.

Internet Explorer has a special security feature that most other browsers lack: it uses multiple security zones. This feature enables you to differentiate between risky sites and safe ones. A *security zone* is a group of settings that are applicable to a certain trust level for web sites. There are four zones: Internet, Local intranet, Trusted sites, and Restricted sites. Internet is the default. The other three zones enable you to assign web sites to them. To control which sites are in a zone, click the zone and then click the Sites button. Using zones enables you to have different security settings for sites that you trust, like your banking institution, than from sites you don't trust, like one that illegally streams live sporting events.

To change the security level for a zone, choose Tools | Internet Options in Internet Explorer and click the Security tab. Click the zone icon at the top and then drag the slider bar up or down (see Figure 11-16). You can also click Custom level and fine-tune the security settings for the chosen zone.

https://t.me/learningnets

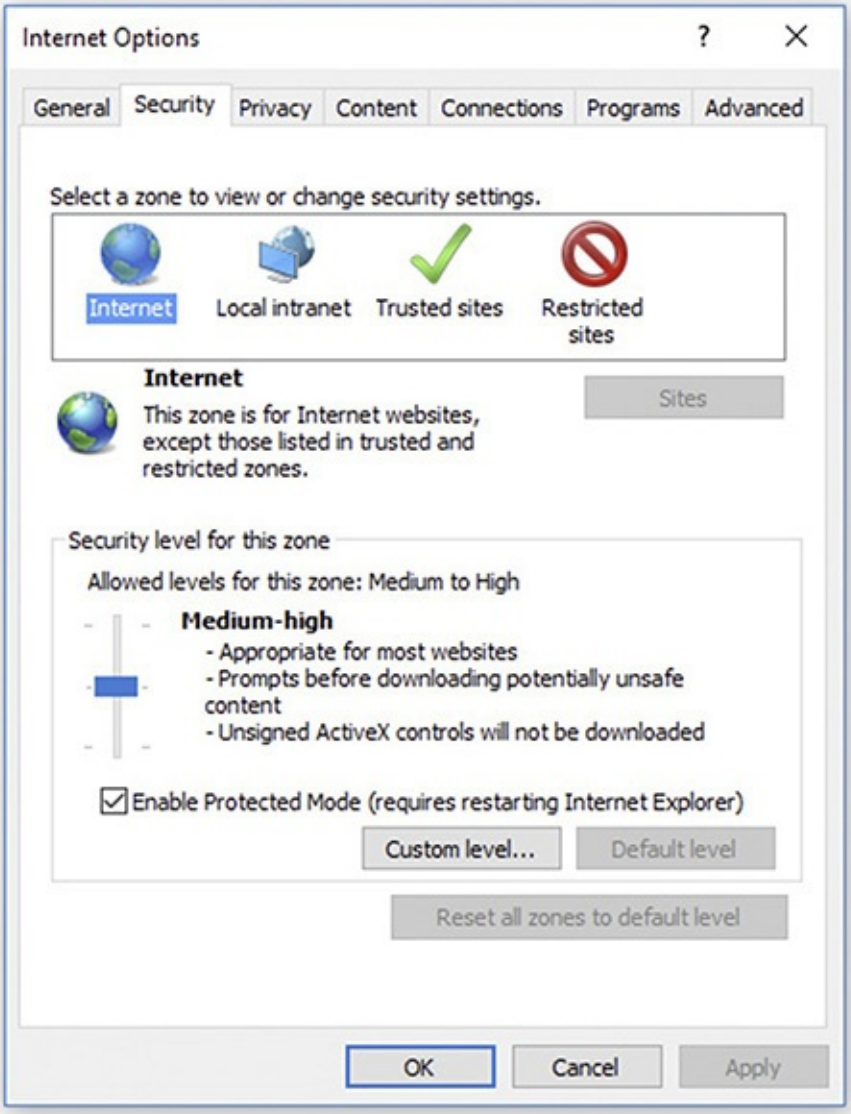


Figure 11-16 Change the security settings for a particular zone.

Clearing Your Cookies

When you go to a web site, browsers store copies of the graphics and other items so the page will load more quickly the next time you access it. These are part of the *Internet cache* or *temporary Internet files*. One of the types of information that a web site may store on your computer is a cookie. A *cookie* is a small text file containing information about you. The data stored in cookies is used for a variety of purposes, listed here:

- To authenticate or identify you as a registered user of a web site so it will

https://t.me/learningnets

remember you on future visits

- To track items in your shopping basket or cart
- To present different content to different users
- To style or theme the site based on user preference
- To track your access to web sites, including what products you look at, even if you don't buy them

Not all cookies (or Temporary Internet Files) are happy and friendly, though. Malicious cookies, installed by some type of malware, can track your Internet activities and report to its creator. This information is often sold to advertisers so that they can better target you. The best way to defend against these bad cookies is to guard against all malware. Some browsers and browser add-ons can be set to partially or completely block cookies.

Cookies come from two different sources. A *first-party cookie* comes from the web site you are actually visiting. First-party cookies can be helpful. A *third-party cookie* comes from another source, such as an advertisement on the web page. Third-party cookies have no benefit to you as a user.

On the Privacy tab in Internet Explorer's Internet Options dialog box (Figure 11-17), you can click the Advanced button to open the Advanced Privacy Settings dialog box. From here you can choose how to handle first-party and third-party cookies. Your choices are to allow them, block them, or get a prompt each time one tries to write to your hard drive. You can click the Sites button to open a dialog box where you can indicate certain web sites to always allow or always block from using cookies.

https://t.me/learningnets

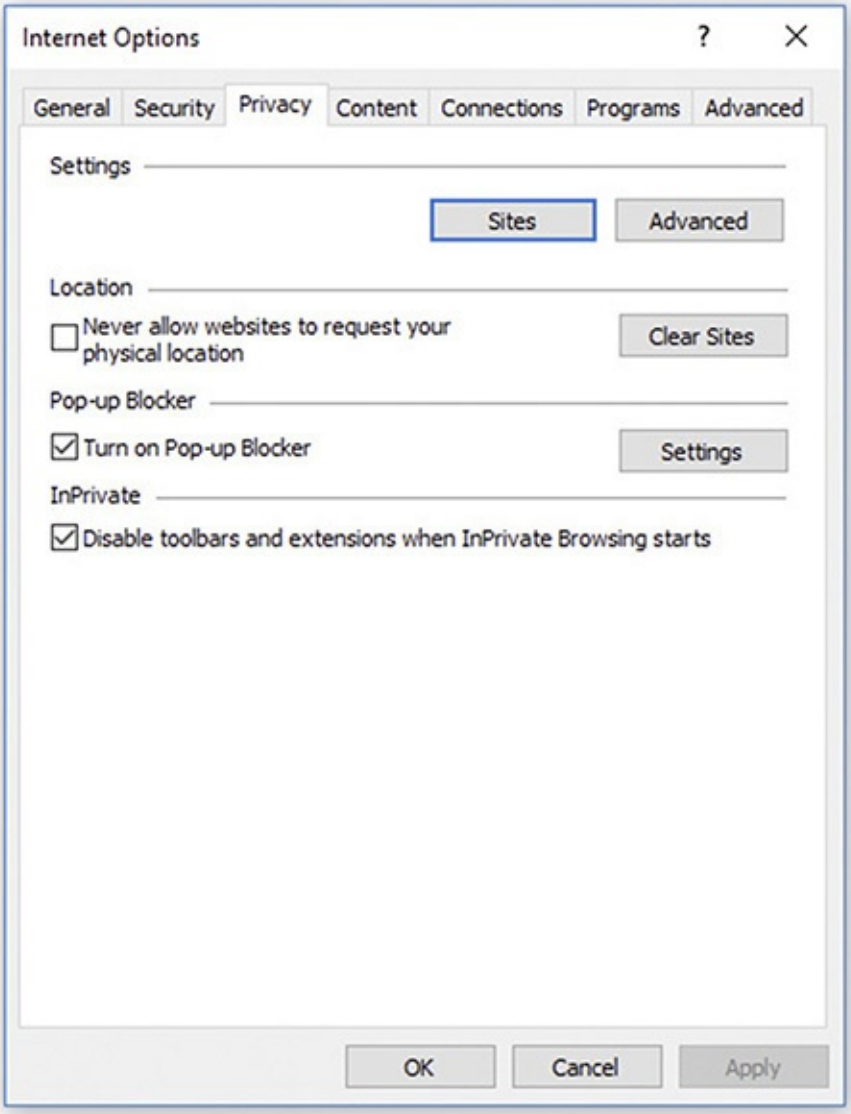


Figure 11-17 On the Privacy tab you can control the use of cookies (via the Advanced button) and pop-ups.

Microsoft Edge has fewer cookie settings you can change. Choose Tools | Settings | View Advanced Settings and then scroll down to the Cookies section. Open the Cookies drop-down list and then choose Block all cookies, Block only third party cookies, or Don't block cookies.

Clearing the History and Temporary Internet Files

Most browsers track the web sites you visit over time—your history—and store any relevant information about the site as temporary Internet files (also called

https://t.me/learningnets

your web browser *cache*). You can remove the history and temporary Internet files to erase your tracks.

In Internet Explorer, choose Tools | Internet Options, and on the General tab, select the Delete browsing history on exit check box. That takes care of the future. To wipe up the past, click the Delete button and then mark or clear the check boxes for the types of content you want to delete. For example, you can wipe out cookies and web site data from here, as well as history, temporary Internet files, and saved passwords. See Figure 11-18. Then click Delete.

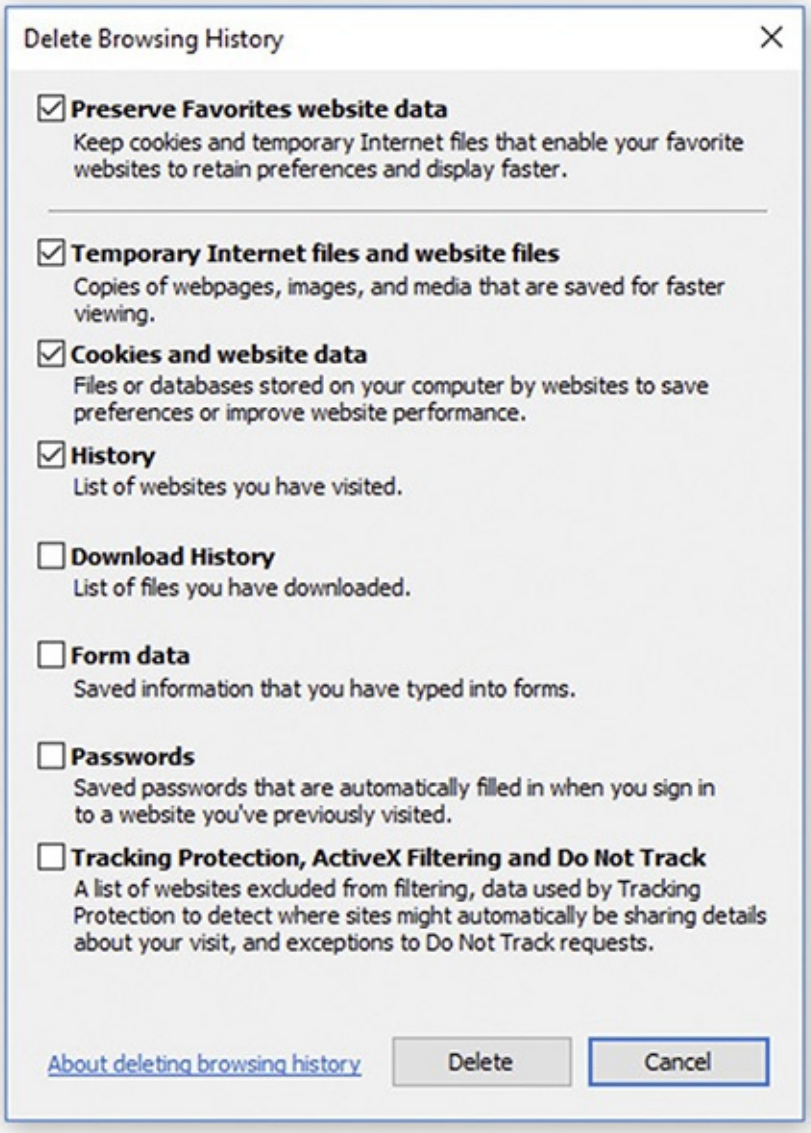


Figure 11-18 Clear your browsing history and other information about your browsing habits.

https://t.me/learningnets

In Microsoft Edge, choose Tools | Settings; under the Clear browsing data heading, click Choose what to clear. Select or clear the check boxes for the various types of content and click Clear.



EXAM TIP Make sure you understand the benefits and drawbacks of clearing the browser cache, history, and cookies.

Disabling Unneeded Plug-ins, Toolbars, and Extensions

The problem with classic plug-ins (also called *add-ons*) was that they exercised a lot of control over the user's web browser and could do malicious things.

According to the CompTIA IT Fundamentals exam, you should uninstall unused plug-ins. Get that correct on the test. For web browser use today, in contrast, don't use any classic plug-in. Instead use extensions (more on these shortly).

Various third-party companies create toolbars for browsers that add certain features. The Yahoo! toolbar, for example, added a Yahoo! search field, access to Yahoo! mail, a stock ticker, and so forth. A lot of people enjoyed the added features (though Yahoo! stopped making the toolbar in favor of a customized Firefox browser).

The problem with toolbars comes from less-reputable companies that add aggressive toolbars during the installation of other programs. They can prove to be hard to remove and use up valuable resources. If you accidentally install one of these predatory toolbars, such as Jeeves from Ask.com, uninstall it immediately.

Modern browsers use extensions to add functionality, in some cases to allow browser-based cloud application to run. Extensions are usually tightly written code with discrete functions. Adblock, for example, just blocks ads from appearing on web pages you visit. It doesn't take over your browser or redirect you somewhere. It just does its job.

You can and should disable unused extensions. Figure 11-19 shows the Extensions list in Google Chrome browser. Note the 3D Viewer for IKEA and Adobe Acrobat are disabled. You can add, disable, and remove extensions through the Tools menu in most browsers.

https://t.me/learningnets

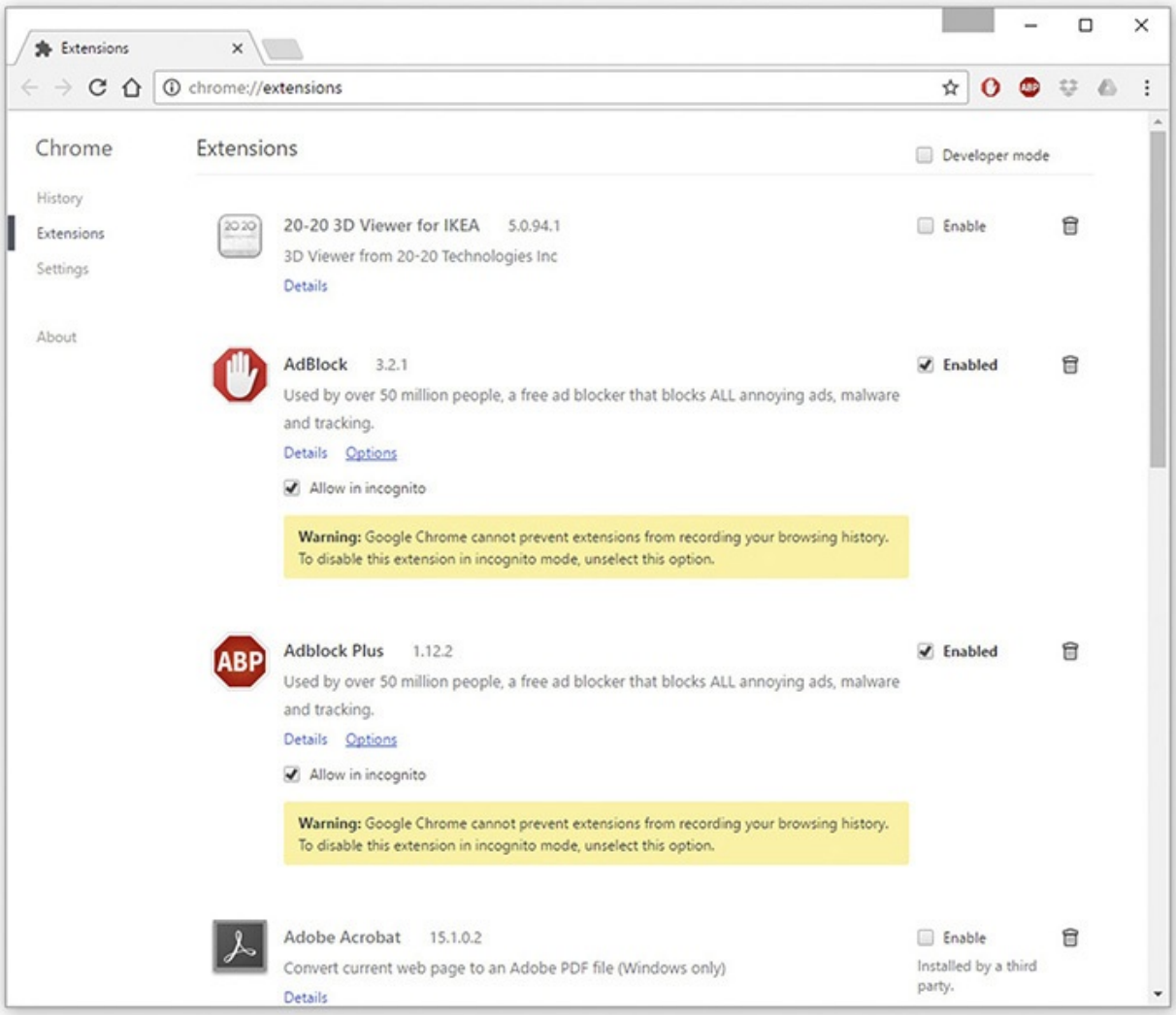


Figure 11-19 Extensions in Chrome

Disabling AutoFill Forms and Passwords

Most browsers have a convenient feature that allows you to automatically fill in forms that ask for your name, address, phone, and other contact information, as well as passwords for web sites you have previously signed into. This feature saves a lot of time on a computer that is physically secure all the time. However, if your computer is not under your control and monitoring all the time, you might not want the browser to save that kind of data.

To disable autofill for forms and passwords in Internet Explorer, choose Tools | Internet Options to open the Internet Options dialog box, select the Content tab, and click Settings in the AutoComplete section. In the AutoComplete Settings dialog box (Figure 11-20), select or clear the check boxes to control what is

https://t.me/learningnets

saved. To manage saved passwords, click the Manage Passwords button there.

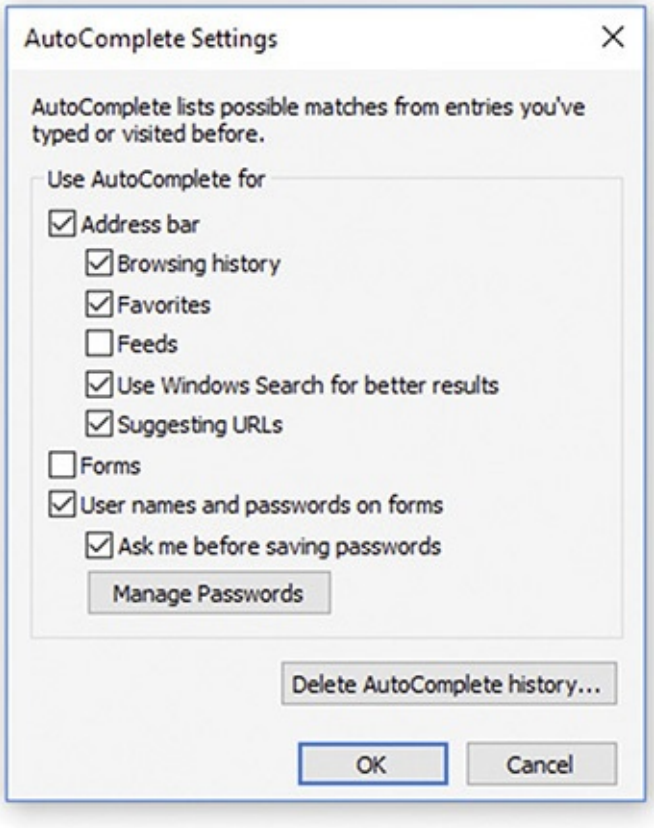


Figure 11-20 Choose what your browser saves automatically when you enter passwords and fill in forms.

Firewalls

Firewalls are devices or software that protect computers from unauthorized access to and from the Internet at large. Hardware firewalls use a number of methods to protect networks, such as hiding IP addresses and blocking TCP/IP ports. Most small office/home office networks use a hardware firewall built into the SOHO router. Many routers use access control lists (ACLs) that can filter by port number, IP address, or several other attributes.

Windows comes with an excellent software firewall called Windows Firewall. It can also handle the heavy lifting of port blocking, security logging, and more. You can access Windows Firewall by opening the Windows Firewall applet in the Control Panel. Windows Firewall is mostly self-managing; you need to configure it only if it is blocking an application that you want to use.

https://t.me/learningnets

Chapter Review

Local security threats are often overlooked but are very real. A computer can be compromised by password cracking, dumpster diving, or shoulder surfing, for example. The network can be threatened by unauthorized users on the network, such as someone joining the WiFi network without permission. Unauthorized access can result in data destruction, theft, spying, and the introduction of malware.

To combat local threats, you must control access.

- Harden devices to make them as difficult as possible for unauthorized people to access by changing hardware and software settings.
- Use Standard user accounts rather than Administrator accounts for everyday use.
- Employ safe password management practices, including establishing rules for password complexity, confidentiality, expiration, and reuse.
- Use the appropriate level of User Access Control that balances convenience with security.
- Malicious software can destroy your data or report your personal information back to whoever wrote the program. Viruses, Trojan horses, and worms can all infiltrate your system, often posing as something more legitimate, such as (not without irony) a malware scanner. These bad programs also have a habit of growing worse over time, as they destroy more data or infect more systems.
- Spyware and adware do not necessarily do harm to your PC, but they can make using it a pain by causing ads to pop up in front of your browser or slowing down your computer. Spam is any unwanted e-mail that appears in your inbox. These are usually scams for money. Don’t reply to them—delete them.
- There are tools for all of these that scan for any malware currently on your system and defend against future infiltration. If your system becomes infected with malware, be sure you know what to do to get rid of it: recognize the malware attack, quarantine the entire PC, search for and destroy the malware using anti-malware software, remediate by restoring your PC with previously made backups, and educate yourself and anyone else who may have allowed the infection to occur. Also, be sure to escalate the problem to a boss or co-worker if you are unable to fix it yourself.

https://t.me/learningnets

- Proper browser configuration can often prevent malware from getting onto your PC. You can delete history, cookies, and temporary Internet files, which can be used to track your browsing. Don't use classic plug-ins.
- Being a smart web user includes understanding the risks of public workstations, identifying and using secure web sites, recognizing invalid certificates, untrusted sources, suspicious links and banner ads, limiting personally identifiable information exposure, and configuring browser security and privacy settings.

Questions

1. What is a person doing when searching trash for useful information?
   - **A.** Dumpster diving
   - **B.** Garbage mining
   - **C.** Cracking
   - **D.** Trash talking
2. Edward loiters at the local café, taking notes on what people type on their computers, especially at the login screens. What kind of theft does he practice?
   - **A.** Cracking
   - **B.** Dumpster diving
   - **C.** Infiltration
   - **D.** Shoulder surfing
3. Disabling the Bluetooth adapter on a laptop when it is not in use is an example of:
   - **A.** Dumpster diving
   - **B.** Cracking
   - **C.** Device hardening
   - **D.** Hardware theft prevention
4. Which of the following can prevent people from snooping on a device that you leave unattended for several minutes?
   - **A.** Configuring a lock-out time

https://t.me/learningnets

B. Shoulder surfing

C. Using a strong password

D. Disabling WiFi

5. After you have recognized that there is a virus on your PC, what is the next step to removing the virus?

A. To educate

B. To search and destroy

C. To quarantine

D. To remediate

6. How can you defend against malware delivered by e-mail?

A. Delete old messages regularly.

B. Don’t open attachments from unknown senders.

C. Only use the preview window.

D. Only use Mozilla Thunderbird.

7. Which type of file tracks your activities on the Internet?

A. Spam

B. Java

C. Pop-up

D. Cookie

8. Which of the following might you want to disable to protect your privacy?

A. Autofill forms

B. Hyperlinks

C. Certificates

D. InPrivate browsing

9. Which type of malware tries to get you to pay a fee to decrypt your files?

A. Trojan

B. Worm

C. Spyware

D. Ransomware

10. What indicates that you’ve browsed to a secure web page? (Choose two.)

A. The web address starts with http://.

https://t.me/learningnets

B. The web address starts with https://.

C. A small lock appears in the browser.

D. A small key appears in the browser.

Answers

1. **A**. Digging through the trash looking for useful information is called dumpster diving.
2. **D**. Edward uses shoulder surfing to gain access to people's accounts.
3. **C**. Device hardening involves blocking all unnecessary points of access, such as an unused wireless connection.
4. **A**. A lockout time will lock the device after a certain idle time period, preventing snoops from looking at it.
5. **C**. After you recognize that there is a virus on your machine, you need to quarantine, either by using anti-malware software or by disconnecting the infected machine from the network.
6. **B**. The best defense against e-mail messages with malware is not opening e-mail messages from unknown senders.
7. **D**. Web browsers use cookies to track certain things you do on the Internet.
8. **A**. Autofill forms can make your previously entered form data available to others who use your computer.
9. **D**. Ransomware holds your data for ransom by demanding that you pay a fee.
10. **B**, **C**. Secure web pages have addresses that start with https://, and a small lock appears in the browser.

https://t.me/learningnets

CHAPTER 12

Computer Maintenance and Management

In this chapter, you will learn how to

- Manage power usage
- Clean and maintain hardware
- Dispose of computer equipment responsibly
- Recover from disasters

Keeping a computer working well isn't that difficult these days. Most of the maintenance utilities that IT professionals used to recommend you run manually are now handled automatically in the OS, including running Windows Update and checking the hard drive for storage errors.

So, what's left for the average user to do? The main things are to manage the computer's power usage effectively, keep it clean (inside and out), and recycle or dispose of it properly when it's beyond repair or no longer cost-effective to upgrade.

In this chapter, we look at those three important topics as well as continuity considerations to keep business processes running smoothly.



NOTE This chapter provides good general guidelines, but you should also follow the manufacturer's safety guidelines. These guidelines help you use, maintain, repair, and dispose of your devices safely.

Power Management Basics

https://t.me/learningnets

Broadly, *power management* means controlling how a computer uses power, with a focus on using less power and making sure power is available when needed (for example, by conserving battery life).

Choose Energy-Efficient Devices

In addition to the power management changes you can make in Windows (covered next), you can also achieve some power savings by choosing energy-efficient devices. Look for components that have the Energy Star logo; these are certified to be energy efficient. An energy-efficient device may have special power-conserving features, such as shutting itself off or putting itself in a low-power mode after a period of inactivity.



EXAM TIP An *energy-efficient device* uses less energy overall than nonefficient equivalents and may have special energy conservation features. Look for comparative questions on the exam.

What do you do when you're going to be away from the computer for a while? The following sections can help you decide.

Leave the PC Running

Some people like to leave their computers on 24/7 so they never have to wait for the computer to start up when they want to use it. That's okay, but it has some consequences.

First, there's the financial side. If you leave a desktop computer on all the time, you will pay about $200 a year for its electricity (assuming a cost of about 12 cents per kilowatt per hour). A laptop is much less, around $65 per year. That may not be a bank-breaker, but it's not small change, either. The busier a computer is—such as with increased disk I/O, a larger monitor, and so on—the more power it will consume. If your machine has a malware infection that mines Bitcoins for attackers even more power is drawn because of the mathematical complexity and how busy the CPU is!

Next, there's the fact that a running computer generates heat, and heat is an enemy of computers. If certain chips (like the CPU) get too hot, they stop

https://t.me/learningnets

working until they cool down enough. Very high temperatures can damage a chip immediately, but damage from less intense heat can also accumulate until the chip fails. That's why there are all those heat sinks and fans inside a computer, as you learned in Chapter 2. Even with all that heat-reducing equipment, though, heat is still an issue.

Finally, if your computer runs on battery power, leaving it on all the time drains the battery. That's fine if you are close to an AC outlet where you can recharge the battery, but you won't always be.

For all those reasons, you should consider either shutting the computer down entirely or putting it in a low-power mode whenever you are going to be away from it for more than a few minutes.

Shut Down the PC

Shutting down completely eliminates all three of the problems described earlier, but it has one big disadvantage: it's inconvenient. A typical Windows PC takes a minute or two to start up, and meanwhile you're sitting there drumming your fingers on the desk impatiently. If you're coming back to the computer relatively quickly (say, within a day or so), you might want to consider an alternative that will enable you to resume your work more quickly.

Low-Power Modes

Windows supports two power-saving modes:

- **Sleep** Keeps memory powered but shuts down all other components. As a result, the computer uses very little power—just enough to allow the memory to retain its contents. On battery power, a laptop can last about a day in this mode (depending on battery capacity and condition, of course). Resuming from Sleep mode is very fast, just a few seconds in most cases.
- **Hibernate** Copies memory content to a reserved area of the hard drive and then powers off all components. Since the PC is not using any power, it can remain in Hibernate mode indefinitely. Resuming from Hibernate takes slightly longer than from Sleep, about 15 seconds on the average.



https://t.me/learningnets

NOTE In Windows 8 and newer, Sleep mode is actually a hybrid sleep. It starts out in Sleep mode, but if the battery reaches a critically low threshold or if a certain amount of time passes (as specified in Power Options), Windows switches to Hibernate automatically.

To enter Sleep mode manually, click the Start button, click Power, and then click Sleep or Hibernate. See Figure 12-1. You can also configure the PC to enter Sleep or Hibernate mode automatically after a certain amount of idle time by setting that up in a power profile, described next.

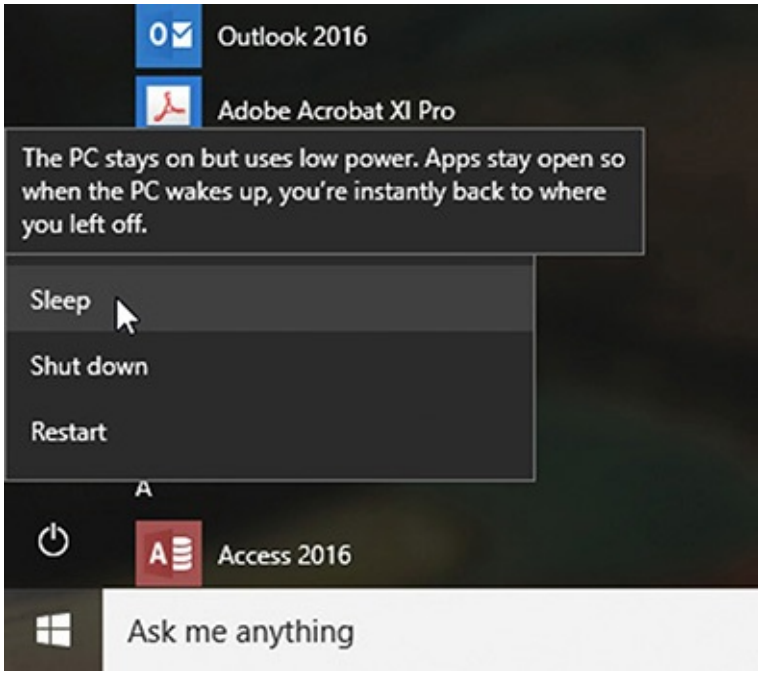


Figure 12-1 Put the PC to sleep before you walk away.

If Hibernate doesn't appear on the Power menu (as it doesn't in Figure 12-1), you can make it appear by going to Control Panel | Hardware and Sound | Power Options | System Settings (shown later in this chapter in Figure 12-5) and marking the Hibernate check box. If the check box isn't selectable, click the Change settings that are currently unavailable hyperlink near the top of the dialog box. Be aware, however, that on systems where Hibernate is not enabled by default, it is sometimes because the hardware doesn't work well with the feature. If you experience a problem using Hibernate, you might decide it's better not to use it.

https://t.me/learningnets



TIP If your PC won't wake up from Sleep or Hibernate, press and hold the Power button on the computer for ten seconds and then press it again to restart.

Power Plans

A *power profile* is a collection of settings that determine how Windows manages power use. All Windows PCs have at least three power plans corresponding to three levels of power-saving aggressiveness.

- **High performance** Use when power consumption and battery life are less important than the PC always being instantly available.
- **Balanced** This provides moderate power savings; this is the default.
- **Power savings** This gives the most power savings; use this when conserving power and/or battery time is important.

You can choose one of these power profiles and use its default settings, or you can modify the settings. You can easily switch between power profiles whenever your needs change.

To access the power profiles, open Control Panel | Hardware and Sound | Power Options. Then, click the option button of the desired power plan. Choose the one that describes your general situation the best, as in Figure 12-2. Then click the Change plan settings hyperlink for the chosen plan.

https://t.me/learningnets

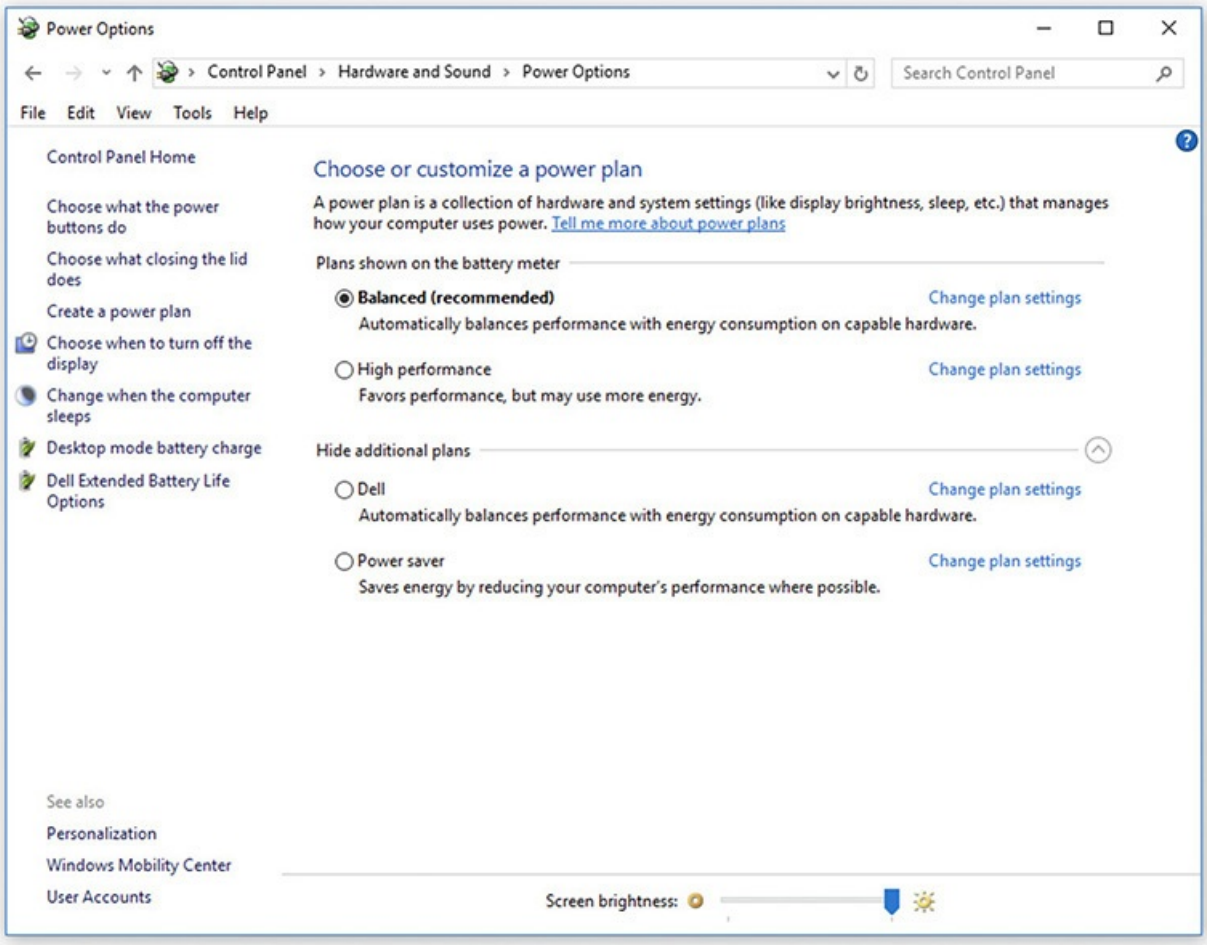


Figure 12-2 Select a power plan.



TIP There may be an additional power plan, such as the Dell plan shown in Figure 12-2.

The Edit Plan Settings section (shown in Figure 12-3) enables you to choose two important aspects of the power plan: when to just turn off the display and when to put the whole computer to sleep. On a laptop you'll see separate settings for On battery and Plugged in and also be able to adjust display brightness for the plan.

https://t.me/learningnets

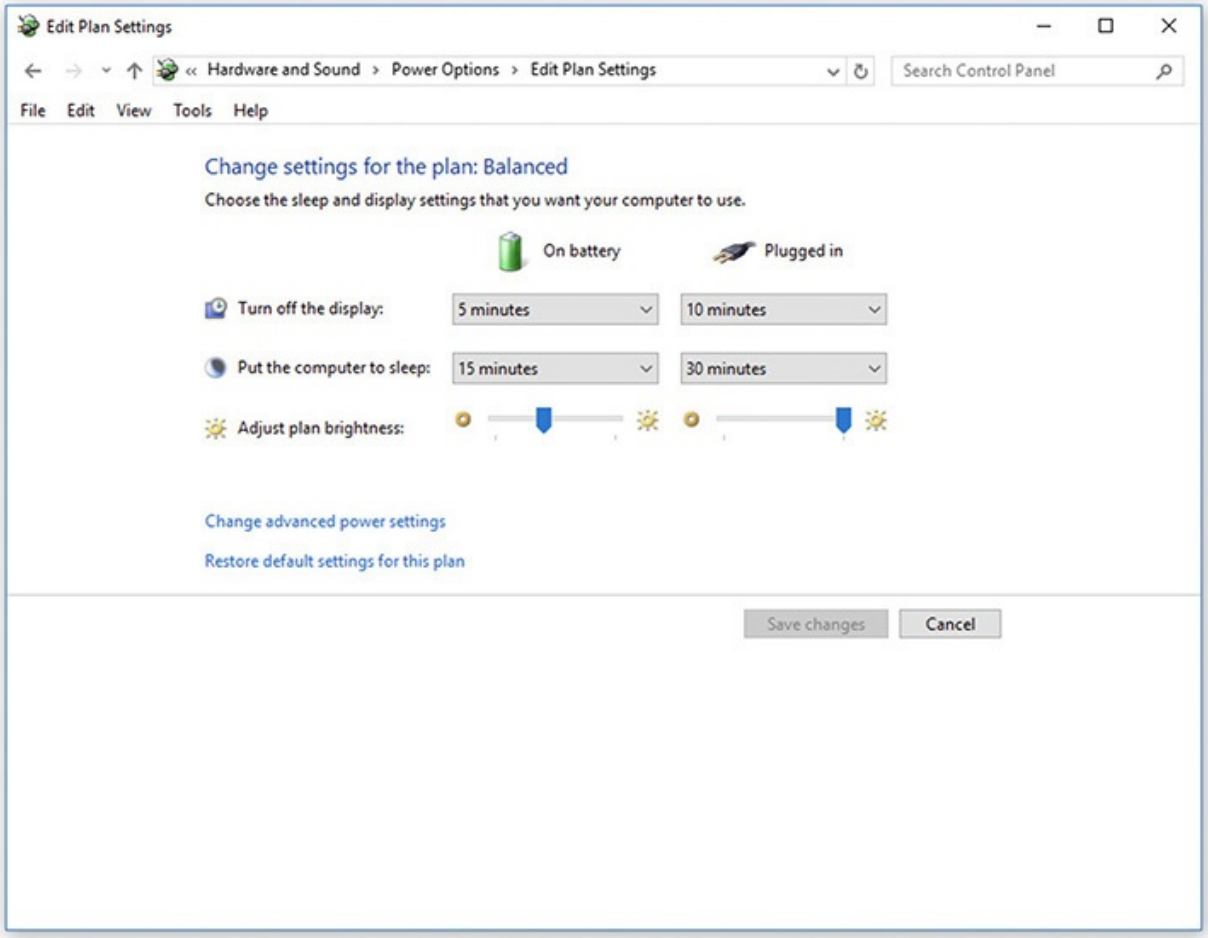


Figure 12-3 Edit the power plan.

For even more control, click Change advanced power settings, opening the Power Options dialog box. From here you can fine-tune many subtle aspects of the power plan, such as when/whether to turn off wireless adapters, USB ports, and PCI Express slots. If you expand the Sleep section in this dialog box, you come to settings (shown in Figure 12-4) for the amount of idle time before Sleep and Hibernate start.

https://t.me/learningnets

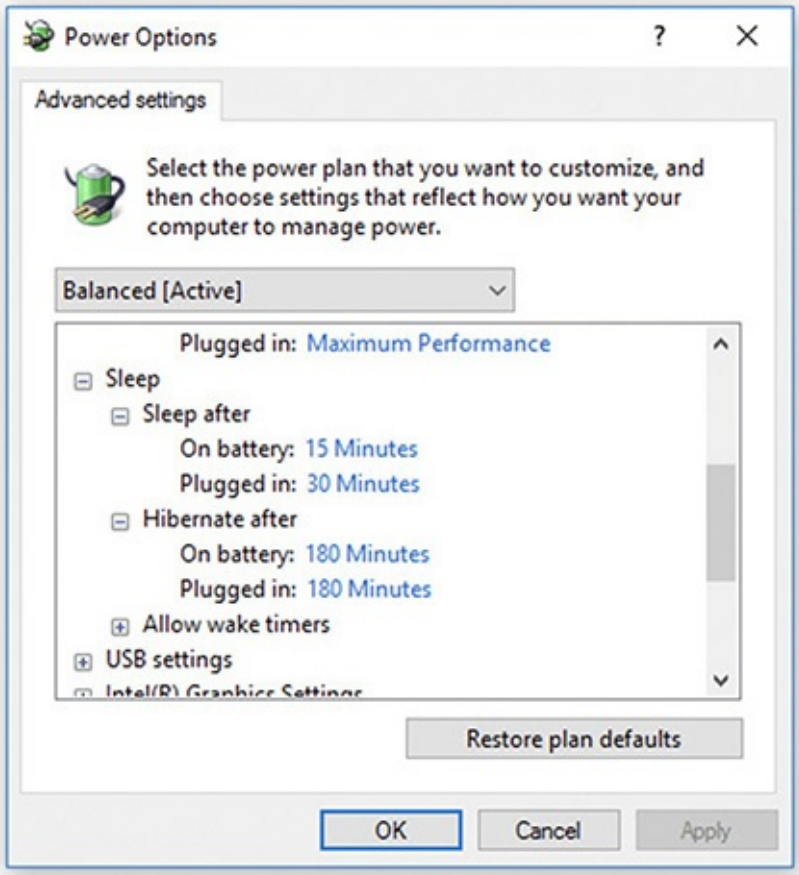


Figure 12-4 Fine-tune the power plan.

Choosing Actions for Power Buttons or Closing the Lid

You can also put the computer in Sleep or Hibernate by closing the lid (for a laptop) or pressing a hardware button. These actions will have some effect on your system by default, but you can also adjust how your system will respond to them. Just navigate to Control Panel | Hardware and Sound | Power Options | Choose what the power buttons do (see Figure 12-5). For example, you could set the PC to sleep when you close the lid but hibernate when you press the power button.

https://t.me/learningnets

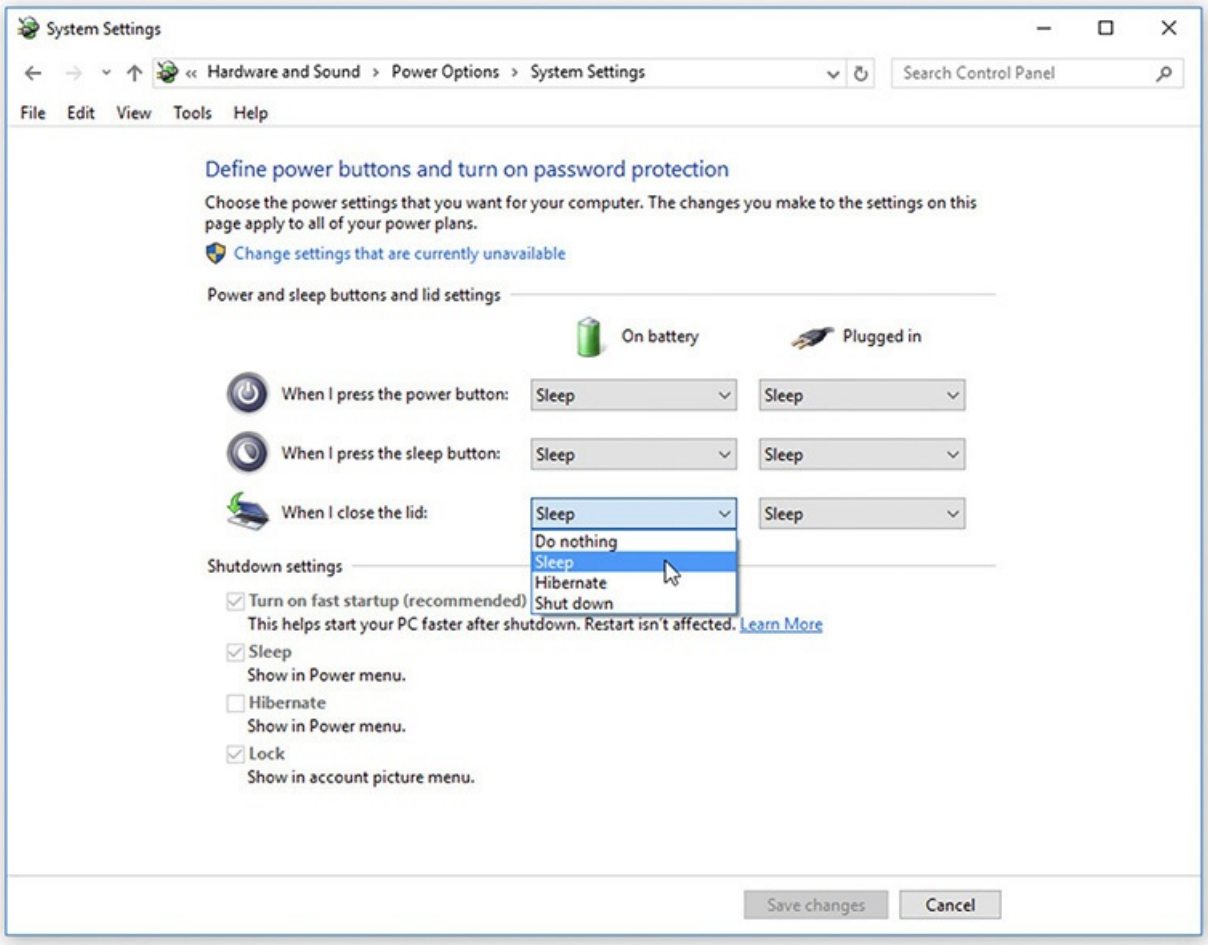


Figure 12-5 Defining power buttons and lid action

Cleaning and Maintaining Computer Hardware

A properly maintained computer starts with a clean, orderly environment. You should also keep external components clean and free of dust and hair. Take care to use proper cleaning solutions and methods, especially for sensitive components such as monitors.

Proper Cleaning Materials

Aside from dust, the exterior parts of a computer don’t get very dirty in a typical environment. Use a vacuum cleaner or soft cloth to clean the case, mouse, and keyboard. Use special glass cleaner designed for computer monitors, not standard household glass cleaner. For exterior components, use a spray cleaner designed for electronics. (Such a cleaner includes antistatic properties, unlike

https://t.me/learningnets

regular household cleaners.)



TIP Special vacuum cleaners are available for use on computer equipment and other electronics, but they're mainly useful when cleaning the inside parts. See the section "Cleaning Inside" later in this chapter for details.

In a nontypical environment, more aggressive cleaning is required. For a PC in an automotive shop or other high-grime environment, use a mild soap and water solution on exterior components. Unplug keyboards from the PC first and allow them to dry completely before reattaching. If you plug in a keyboard with any moisture inside, it'll short out and become more landfill fodder. You may prefer to use denatured alcohol when cleaning a keyboard.



EXAM TIP Use mild soap and water with a soft cloth to clean any dirty external parts of the computer.

Cleaning Monitors and Removable Media

Cleaning monitors and removable media requires a little caution, especially with the substances used to clean them. Glass cleaners containing ammonia, for example, will harm some LCD screens. A tiny bit of moisture under the screen panel on any monitor can take out the electronics as soon as you plug in the monitor.

To clean a monitor, use a damp cloth or a mild soap and water solution. Make sure the cloth itself is super-soft, like a chamois or microfiber towel. Spray the cleaner on the cloth and then wipe; don't spray directly onto the screen.

With removable media, such as CD-R and BD-RE discs, you need to take care not to scratch, crack, or warp the media when cleaning. As in Figure 12-6, use a soft cloth, possibly damp, and wipe from the inside edge to the outside edge with a straight movement (*not* by wiping in a circular motion). Don't run optical discs through the dishwasher unless you enjoy the sound of dying data.

https://t.me/learningnets

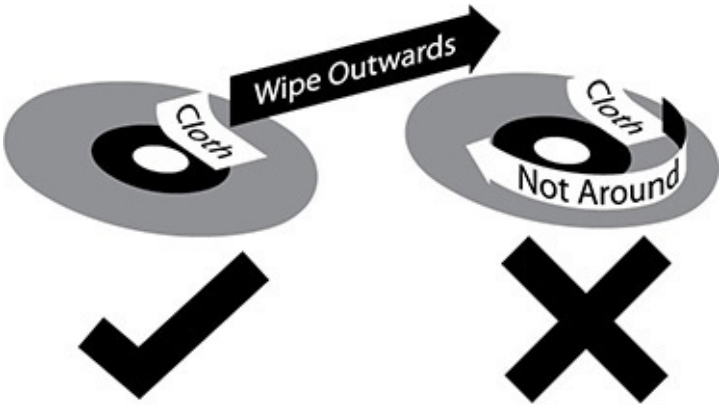


Figure 12-6 Cleaning an optical disc

Cleaning Inside a Desktop PC

Computers aren't solid; they're a collection of parts inside a box. The box or case usually has vents, and over time the inside can accumulate dust and hair. If too much debris builds up, the computer could overheat and break down. It is important to open the case and clean the inside every once in a while.

The first step is getting inside. Some desktop cases have a side panel that you can remove with two screws, as in Figure 12-7. Others have a clamshell design that unlatches when you press buttons, and still others have a single U-shaped cover that exposes three sides at once when removed.



Figure 12-7 Remove these two screws and the side will come off.

Avoiding ESD

Electrostatic discharge (ESD) can permanently damage or destroy computer components inside the case. ESD is the transfer of static electricity from you to

https://t.me/learningnets

something you touch. If you've ever been shocked when touching a door knob in the winter time, you know exactly what ESD feels like. Unlike you, though, a computer component can't say "Ouch!" and flinch from the contact. It just dies a little, inside, where it counts.

As soon as you open the case, touch the metal of the power supply (Figure 12-8). This will discharge any static electricity you have without harming anything.



Figure 12-8 Touching the power supply

If you plan to be inside the computer case for a while, purchase an *antistatic wrist strap.* Connect one side to your wrist and the other to the power supply or case (Figure 12-9). This keeps everything safe from ESD.

https://t.me/learningnets

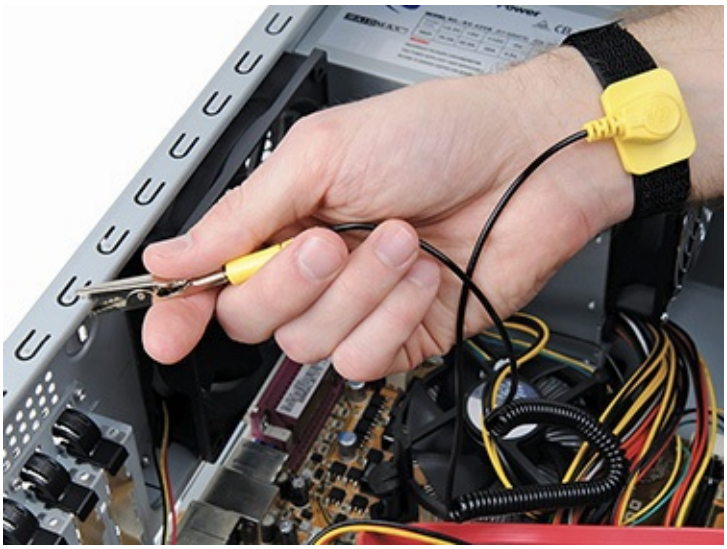


Figure 12-9 An antistatic wrist strap connected to a PC



EXAM TIP Connecting to the power supply or metal frame of a case with an antistatic wrist strap is the best way to avoid ESD when working inside a computer.

Cleaning Inside

Once inside the case, you have two basic options for getting rid of dust and hair inside a PC: you can blow the dust out, or you can vacuum it out.

You use a product called *compressed air* to blow out dust, cat hair, and anything else out of the case. Compressed air comes in small cans like spray paint, usually with a little tube for precise aiming (Figure 12-10). You can purchase compressed air at any electronics or computer retail store. Just make sure to do the blowing outdoors, not inside! Otherwise, you'll make a huge mess.

https://t.me/learningnets

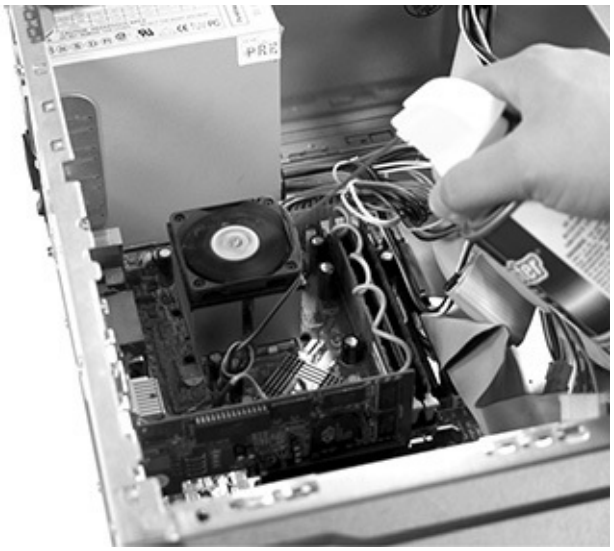


Figure 12-10 Compressed air

You can use a special vacuum cleaner designed for electronics to vacuum out the inside of the case (Figure 12-11). Normal vacuum cleaners create a static electricity charge as the dust flows through the plastic nozzle, so you shouldn't use them inside a computer. You can find electronics or *antistatic vacuums* at computer and electronics stores.



Figure 12-11 Antistatic vacuum



CAUTION Don't vacuum up spilled toner from a laser printer toner cartridge with a regular household vacuum. The filter is not usually fine enough to catch the particles. The particles can become airborne and irritate your lungs if you inhale them. Wipe up spilled toner with a damp paper towel.

https://t.me/learningnets

Ventilation, Dust, and Moisture Control

A well-maintained computer ensures proper ventilation and limits the amount of dust that comes into the case. Further, the case protects the inside from any unwanted moisture. The key issue from a maintenance standpoint is to make sure the case covers are properly in place.

Case manufacturers design cases for air to flow across the drives and motherboard. The front of the PC usually has extra covers for drives you might want to add later, and the back usually has slot covers for unused expansion slots. Don’t leave unused covers off, as in Figure 12-12 and Figure 12-13, because missing covers can disrupt the flow (causing overheating) and let in even more airborne debris. Finally, make sure air vents on computer equipment aren’t directly up against a wall or crammed under a desk where there is minimal airflow.



Figure 12-12 Drive cover missing on the front of a PC

https://t.me/learningnets



Figure 12-13 Slot cover missing on the back of a PC

Environmentally Aware Computer Disposal

When a computer (or component) reaches the end of its useful life, don't just throw it in the trash can along with your everyday waste! Many computer components contain materials that are bad for the environment, such as cadmium, mercury, and lead. In addition, the plastics and metals will probably end up in a landfill with your regular trash, when they could possibly be recycled into some other product.

Most computer part makers have adopted the Restriction of Hazardous Substances (RoHS) directive to make their products more environmentally friendly and thus easily disposed of (Figure 12-14). The RoHS guidelines are a European Union (EU) standard that regulates toxic substances, such as lead, mercury, and cadmium. RoHS has helped change the way manufacturers create circuit boards. *Solder* is used to make a connection point (which resembles a little glob of solid silver) between wires. In recent years, most computer part makers have shifted from lead-based solder to tin-based solder. This helps

https://t.me/learningnets

reduce the risk of lead exposure to the people who work in electronics recycling around the world.



Figure 12-14 RoHS-compliance labeling

Many major cities offer convenient recycling centers for hazardous household materials, and some electronics retailers have electronics-specific recycling programs. Check online to find the nearest recycling center that will take electronics.

Disaster Recovery

Bad things happen. Sometimes we can't control that, but the good news is that we can control our response to these negative incidents. Having contingency plans in place minimizes how these situations affect IT systems and related business processes.

In Chapter 8 we discussed file management including backup both on-premises and in the cloud. Restoring data also means making sure the correct people have access to that data. Data backups are always relevant with disaster recovery to get data in place as quickly as possible, ideally with no lost work, but what about IT systems and services that support that data?

Incident Response

Incident response plans (IRPs) provide detailed direction when negative incidents occur. Assessing the situation is the first thing that must happen, followed by determining the severity of the incident and prioritizing incident response activities.

The IRP also provides details such as which activities people are assigned to

https://t.me/learningnets

along with contact information. In some cases, the IRP will specify that the situation should be escalated to a different team.

Disaster Recovery Plans

Each IT system or service should have its own disaster recovery plan (DRP). The DRP contains detailed procedures related to the recovery of a specific system or service with the least minimal impact.

For example, a DRP for a database server could specify data restoration steps and even disk imaging steps to quickly get the server up and running. These steps would differ from the DRP for fixing malware infections, for fixing cloud service access issues, and so on.

Chapter Review

Power management features in Windows (and other operating systems) save electricity or battery charge time by placing the computer in a low-power state after a certain time idle. In Windows, you can define the parameters of that low-power state using Power Options. This can include specifying when Sleep and Hibernate modes occur.

Clean the exterior of a PC with a mild (preferably antistatic) cleaner. Don’t use regular glass cleaner on a monitor. When cleaning inside a PC, you should use compressed air or an antistatic electronics vacuum cleaner to clean the inside of the case. Touch the power supply or use an antistatic wrist strap to avoid damaging components with ESD. Keep slot covers in place to make sure the computer cools things properly and the dust stays outside.

When disposing of computer equipment, use your local recycling center for large plastic items like CRTs, printers, and scanners, and for items that contain circuit boards with lead in them. Recycle ink and toner cartridges when possible too. Recycle rechargeable batteries such as from laptops; small alkaline batteries can be disposed of with regular trash (except in California, where they must be recycled).

Contingency planning allows for a focused and directed response to the chaos that often results from negative incidents. Incident response plans deal with situation assessment and activity prioritization. Disaster recovery plans provides details on how to get a failed system or data back to a functional state as quickly and efficiently as possible.

https://t.me/learningnets

Questions

1. In Sleep mode, the _____ remains powered; everything else shuts off.
   - **A.** Hard drive
   - **B.** Monitor
   - **C.** Memory
   - **D.** CPU
2. How long can a laptop remain in Hibernate mode without running out of battery power?
   - **A.** 36 hours.
   - **B.** 12 hours.
   - **C.** It depends on the battery condition and capacity.
   - **D.** Indefinitely.
3. How should you clean removable media, such as a DVD?
   - **A.** Use a soft cloth and wipe with a circular movement.
   - **B.** Use a soft cloth and wipe inside to outside with a straight movement.
   - **C.** Use a soft scrub brush and wipe left to right.
   - **D.** Put the disc in the dishwashing machine.
4. Rich has inherited a computer that used to live in his uncle's machine shop. What should he use to clean up parts such as the case, keyboard, and mouse?
   - **A.** A dry, soft cloth
   - **B.** A soft cloth with distilled water
   - **C.** A soft cloth with mild soap and water
   - **D.** A soft cloth with a commercial cleaning solution
5. What standard offers computer part makers guidelines for making environmentally friendly parts?
   - **A.** FTC
   - **B.** RIAA
   - **C.** RoHS
   - **D.** VHS

https://t.me/learningnets

6. What can you use to prevent ESD from damaging components when cleaning inside a computer?
   - **A.** Antistatic wrist strap.
   - **B.** Antistatic bag.
   - **C.** Antistatic wipe.
   - **D.** ESD presents no danger to components, so nothing special is needed.
7. What should you use to remove dust and animal hair from inside a computer case?
   - **A.** Blow dryer
   - **B.** Compressed air
   - **C.** Household vacuum cleaner
   - **D.** Mild soap and water
8. What problem can missing slot covers on the case cause?
   - **A.** Electromagnetic interference from other electronics nearby
   - **B.** Electrostatic discharge from dust and animal hair
   - **C.** Disruption of airflow inside the computer leading to overheating
   - **D.** Disruption of airflow outside the computer leading to overheating
9. What computer component contains a lot of lead and must be recycled?
   - **A.** CRT
   - **B.** Toner cartridge
   - **C.** Ink cartridge
   - **D.** Hard disk drive
10. In California, how should small alkaline batteries be disposed of?
   - **A.** Regular trash
   - **B.** Recycling center
   - **C.** Incinerated
   - **D.** Any of the above
11. Which type of contingency plan is specific to an IT system or service?
   - **A.** Business continuity
   - **B.** Incident response
   - **C.** Disaster recovery

https://t.me/learningnets

D. Data restoration

Answers

1. **C**. Memory remains powered in Sleep mode; everything else turns off.
2. **D**. Hibernate mode uses no power, so it can remain in that state indefinitely, regardless of the battery state or capacity.
3. **B**. To clean removable media discs, use a soft cloth, possibly damp, and wipe from the inside edge to the outside edge with a straight movement.
4. **C**. Mild soap and water are about as fierce a solution as may be needed for cleaning external parts of the computer.
5. **C**. The Restriction of Hazardous Substances (RoHS) directive has guidelines for making products more environmentally friendly.
6. **A**. Connect to the power supply with an antistatic wrist strap to protect the PC from ESD.
7. **B.** Use compressed air outdoors to blow out dust and hair. An electronics or antistatic vacuum will also work.
8. **C**. Missing slot covers can disrupt airflow inside the case and can lead to overheating. They can also lead to excessive dust and animal hair inside the case. This can cause overheating too.
9. **A**. A CRT monitor contains lead, so it must be disposed of properly, not thrown out with regular trash.
10. **B**. In California, small alkaline batteries must be taken to a recycling center. Elsewhere in the United States, they can be thrown in the regular trash. Batteries should never be incinerated.
11. **C.** The disaster recovery plan provides details for how to restore a specific failed IT system or service to a functional state as quickly as possible.

https://t.me/learningnets

CHAPTER 13

IT Troubleshooting

In this chapter, you will learn how to

- Approach IT problems using a standard troubleshooting methodology
- Troubleshoot common computer problems
- Get help with your computer

Most people don't realize how dependent they are on their computers until that moment when the computer won't work as usual. If you've experienced that moment, then you know the anxiety that comes with it. *How will I get my work done? Are my files okay? How much is this going to cost to fix?*

Computer users should know how to troubleshoot basic computer problems. Plus, you need to know how to get help when the problem goes beyond your current knowledge. Just like every rider should know what to do when a chain pops off the sprocket on his or her bike, savvy computer users can fix typical issues such as a frozen computer or a dead PC.

This chapter looks first at problems that happen when external factors intervene, such as a jostled cable or an operating system (OS) that hangs at boot up. The second part of the chapter explores ways to get help when you need it.

Troubleshooting Methodology

A structured troubleshooting approach will get you back up and running as quickly as possible with minimal cost and headaches.

Table 13-1 summarizes standard troubleshooting steps.

https://t.me/learningnets

Step	Description
1. Identify the problem.	• Break large problems down into smaller problems. • Consider scope; who or what is affected? • Gather details about the issue; ask users, view logs. • Determine whether anything has changed. • Duplicate the problem.
2. Research.	• Refer to past help desk tickets. • Search through private or public knowledge bases. • Ask friends or colleagues. • Internet search.
3. Establish a theory of probable cause.	• Eliminate the simple and obvious possible causes. • Consider factors that can indirectly cause problems.
4. Test the theory.	• Change and test only one potential solution at a time. • Determine the root cause of the issue. • Escalate the issue to a professional if necessary.
5. Establish a plan of action.	• Prepare a specific method to implement the solution. • Test the plan in an isolated sandboxed environment. • Notify other users if the solution could possibly affect them. • Escalate the issue to a professional if necessary.
6. Implement or escalate.	• Back up configurations and data first. • If the problem is complex, monitor implementation progress.
7. Verify functionality.	• Ensure the solution has solved the original problem. • Ensure the new problems have not been introduced. • Consult a subject-matter expert if needed. • Configure preventative measure if appropriate.
8. Document the solution.	• Document the problem and steps taken in the solution. • Update old documentation with new knowledge.

Table 13-1 Troubleshooting Steps



EXAM TIP You might see a question or two on the exam with a specific troubleshooting scenario that requires you to identify the correct sequence of the listed troubleshooting steps.

https://t.me/learningnets

Solvable Common Computer Problems

You can solve common problems by recognizing symptoms and implementing solutions. Typical problems you'll run into include no power, physical damage, failed boot, application failure to load, and peripherals that don't function as they should. Let's take a look at each issue.

No Power

It's dead, Jim.

—Dr. McCoy

You press the power button and nothing happens. *Nada*. No lights, no sound, nothing on the screen. Don't panic!

First, make sure the device has power. If the device runs off batteries, make sure the battery has a charge or plug it into AC power if possible. If the device runs on AC, check for a firm power cord connection and confirm the outlet works. If the workstation uses a power strip, surge protector, UPS, or the like, make sure it isn't switched off and confirm the device itself is connected.

In the case of a laptop computer that refuses to start up, consider removing the battery and plugging the device in using the supplied power cable. You might need to press and hold the power button for up to 30 seconds. After releasing the power button, press it normally to see whether it starts up.

Some PCs fail to come out of Sleep or Hibernate mode and get stuck there, so they seem completely dead. To make sure that isn't the case with your dead PC, hold down the power button for five to ten seconds and then release it and press it again. This resets any low-power mode that might be in effect.

An apparently dead handheld mobile device like a smartphone or tablet can sometimes be rescued with a reset. Try a soft reset first (one that does not destroy data); if that doesn't work, try a hard reset. Check the device documentation or search online for the procedure. See Chapter 7 for more on resetting mobile devices.



CAUTION Before assuming your dead mobile device needs to be reset, make sure that the problem is not just a drained battery. Plug the device into AC power

https://t.me/learningnets

for at least four hours to make sure.

If the device remains completely lifeless after trying all that, it may be time to consult a professional.



EXAM TIP Make sure you can explain several reasons why a device might not power up and how to differentiate between them. Check for dead batteries, loose cables and power connections, and possible physical damage, which is covered next.

Physical Damage

Aside from the occasional move, desktops don't have many chances to get seriously damaged. As portable and mobile devices become more popular, though, more and more of us have had to watch a device drop, slide, fly, clink, shatter, crunch, or splash its way to a violent end or watery grave.

Computers like to run in a cool and dry environment, but extreme heat or cold won't usually bother them as long as they are not running. When bringing a computer in from a hot or cold environment, wait for it to come to room temperature before starting it.



CAUTION Still, don't tempt fate. Many devices use plastics or adhesives that may melt as they warm, and intense heat can also damage batteries. If you *can* avoid exposing a device to extreme temperatures, do.

Water is the number-one enemy of electronics, including computers and smartphones. Unfortunately, water damage is common for smartphones. People drop them into toilets, fountains, and wishing wells all the time. Even if you aren't the least bit clumsy, you (and your device) can get caught out in a rainstorm. If your device is on when it gets wet, it will probably short-circuit, which may or may not ruin a circuit board inside it. If the device is off (completely off, not just sleeping), you stand a slightly better chance of avoiding

https://t.me/learningnets

damage. Some newer smartphones are splash-resistant or even waterproof, but don't rely on that to save you.



EXAM TIP You should understand the causes and consequences of physical damage to both desktop and portable computing devices, how to assess the level of damage, and what the repair options are.

If the battery is removable, act quickly to pop it out; if not, turn off the device. Let the device dry out completely. Take it apart if possible, and let the pieces air-dry. Put it in a bag of rice to help absorb the moisture. Don't try to turn it back on for at least 72 hours. If there's any water remaining when you turn it back on again, you run the risk of further short-circuiting.

A cracked display screen is also common. If you can still see the display panel updating properly—without any strange visual artifacts—under the cracked glass, it probably just needs a glass replacement; the screen itself (that is, the LCD or OLED panel) is likely still intact. Consult a repair shop that specializes in your type of device.

A dropped computer might suffer from the trauma, but circuit boards inside a case are not particularly vulnerable to these physical jolts. If a computer doesn't work after a fall, it might have some loose cables inside. If it's a desktop, open up the case and look for any loose or disconnected cables. Checking all of the connectors in mobile and portable devices is best left to a specialist—it takes special tools and expertise to take one apart without breaking or losing anything.



NOTE Hard drives, because they have moving parts, don't fare as well; falls can damage the mechanical parts or even the surface of the platters (though damage to the latter isn't usually immediately apparent). Thankfully, many modern devices use solid-state memory or drives with no moving parts.

Won't Start Up Normally

If the computer won't start up, think about it like a detective would. What has changed? Did you install any new hardware or software? Has the computer been

https://t.me/learningnets

moved, such that some cables might have come loose? Did the OS restart itself after installing an update?

Occasionally after an OS update, the computer might start up badly (that is, slowly or with errors). Sometimes you can fix that by simply rebooting. If that doesn't help and you're using a Windows client operating system, try using the System Restore feature to revert to a previous day's restore point. Using a restore point will not cause you to lose any recent data file edits. Here's how in Windows 10:

1. Right-click the Start button and click System.
2. Click System protection.
3. Click System Restore.
4. Click Next.
5. Select a restore point. If you have a choice (there's just one available restore point in Figure 13-1), pick the one immediately before the problem started.

https://t.me/learningnets

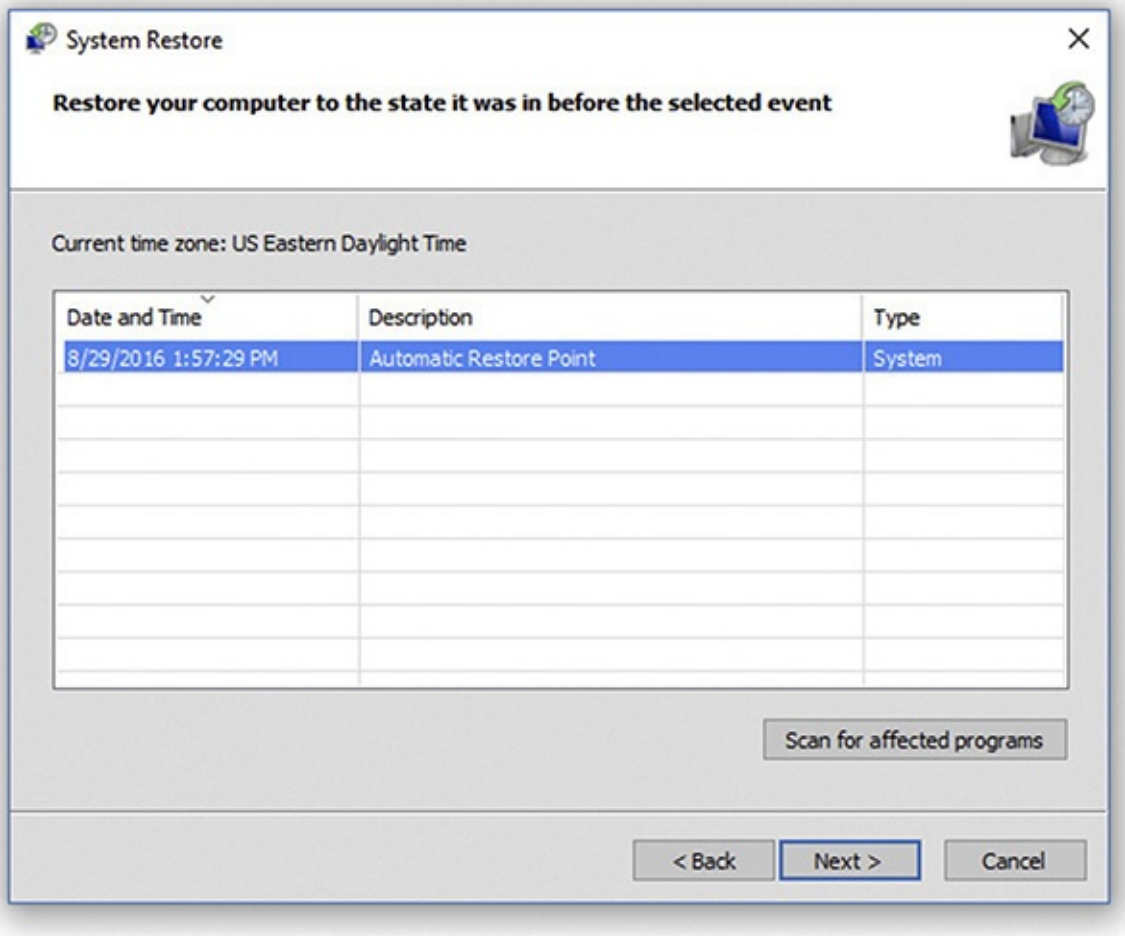


Figure 13-1 Choose a restore point.



NOTE When Windows Update installs system updates, it sometimes erases all the restore points to prevent users from creating system file problems by reverting to earlier versions that the update doesn't support. If you don't have many (or any) restore points available, that's probably why.

6. Follow the prompts to complete the restoration of the system files to that point in time.

System Restore is completely reversible; just run it again and follow the prompts to undo the restoration.

If the OS won't start at all, you might see a prompt offering to boot into a

https://t.me/learningnets

recovery or troubleshooting mode. Do that, if it's offered. If it's not, try booting from the operating system's removable installation media, if you have it, and choosing the Repair option to enter the Windows Recovery Environment (RE). You can also get there in Windows 10 through the Settings app (Update & Security | Recovery | Advanced Startup | Restart Now).

A Certain App Won't Install or Run

Problems with a specific application are often because of hardware incompatibility, especially with the display adapter. The latest games often require specific, high-powered display adapters with the latest driver versions. The application's installation program should check your hardware and let you know whether there are any problems. If it doesn't and you experience problems after starting the application, check online for any known incompatibilities between that application and certain hardware. Try updating your video card (display adapter) driver by downloading the latest driver version from the adapter manufacturer's web site.

Next, look at the application manufacturer's web site to see whether there is a patch or update available for download. If you can't find patches for or information about problems that match what you're experiencing, it's probably a glitch in your own system, such as a minor incompatibility between the application, the OS, and some piece of hardware. Try uninstalling and reinstalling the application; this fixes the problem more often than you might think.

Still no luck? Check to see what version of Windows the application requires. If it's designed for an older Windows version, see whether there's a newer version of the software available. If not, try using Compatibility Mode to see if you can get it to run better by emulating an earlier Windows version. To use the Program Compatibility Troubleshooter, right-click the shortcut for running the application (or its executable file) and choose Troubleshoot compatibility. Click Try recommended settings to let Windows try to guess the right settings. See Figure 13-2. You can also manually troubleshoot compatibility from the Compatibility tab in the program's Properties box, choosing a specific older Windows version to emulate.

https://t.me/learningnets

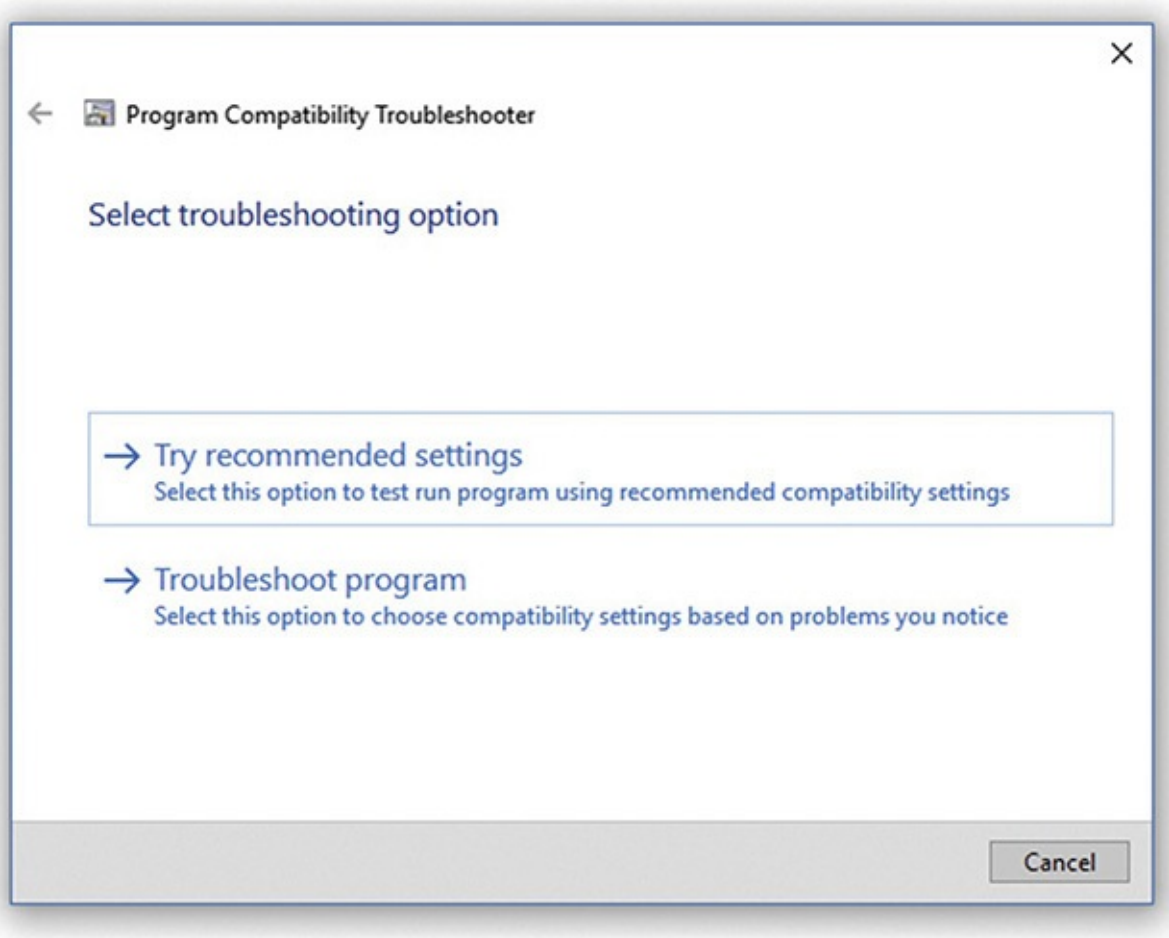


Figure 13-2 Try configuring Compatibility Mode for an application that doesn't run well.

Apps Run but Sometimes Freeze

Today's operating systems, including those for mobile devices, are designed to run many processes at once. The processes are scheduled to consume processor time such that it appears many apps are running simultaneously. But, these software applications occasionally misbehave; they freeze, and you can't close them using the normal methods. In this case, there are ways to force them to exit:

- **Windows** Press CTRL+ALT+DEL to open the Task Manager; from the list of running processes you can right-click the misbehaving app and choose End task to kill the process.
- **macOS** Choose Force Quit from the Apple menu.

https://t.me/learningnets

- **Linux** Issue the *ps* command to view process identifiers (PIDs) assigned by the Linux kernel to running processes. Given the PID, the process can be terminated using this: *kill -9 <PID>*; -9 is the SIGKILL signal that can terminate misbehaving processes.
- **Android-based smartphone** Open the Settings app, choose Apps, select the app from the list, and tap the Force Stop button.
- **iOS 11.*x*** Press the left edge of the iPhone screen, move your finger to the center of the screen, and swipe the app card up and off the screen.

Peripherals Won't Work

When peripherals don't work, it's usually for one of these reasons:

- The cable/cord is bad or isn't snugly connected on each end.
- If wireless, the device's power switch may be off, its batteries drained, or the transceiver (the wireless transmitter/receiver that plugs into the USB port) isn't snugly connected to the computer's USB port.
- If the device uses AC power and you've confirmed the connection, the power cord or the outlet may be bad.
- The device itself is defective.
- The port on the computer is defective.

Check the items on this list to make sure there is no physical problem. If the peripheral came with software, run the setup program for it. Try a different port. There could be a problem with the peripheral's driver, especially if you didn't follow the installation instructions. You can start over by disconnecting the device from your system and uninstalling the driver. To remove a driver in Windows, right-click the peripheral in Device Manager, select Properties, switch to the Driver tab, and click Uninstall.



NOTE If a mouse is dirty, the pointer may stutter or jump around on-screen as you try to use it; remove any dirt or hair from around the sensor on the bottom of the mouse if this occurs. On a trackball, remove the ball and clean out any debris from underneath it.

If it's a cordless peripheral, make sure it has fresh batteries, that it's turned on

https://t.me/learningnets

(if it has a switch), and that the corresponding transceiver is connected to an appropriate port on the PC. Run the setup utility, try a different port, and try different batteries. Make sure the batteries are installed correctly.

For a local printer attached with a cable, check the snugness of the cable connection at both ends. Make sure the printer is turned on and that lights (or a screen) on the printer indicate it is working. If Windows doesn't automatically detect the printer, something is wrong; it should *detect* it even if it can't automatically install the needed driver for it without running the setup utility that came with the printer. Try a different cable. Look in the printer's manual for the procedure to print a test page, and print one to ensure the printer itself works.



NOTE Windows might not automatically detect a network-capable printer that connects directly to a LAN's switch. Open Devices and Printers from the Control Panel and choose Add Printer to run the Add Printer Wizard, which will search local ports and the network for printers.

Getting Help

Thanks to the Internet, you can get help for most computer problems. If someone has solved a similar problem to the one you face, you can find an article about it online. The following sections review the many places to look for help with your computer difficulties.



EXAM TIP You should able to list several sources of help and the pros and cons of each. Make sure you understand the difference between manufacturer documentation, manufacturer web sites, technical community groups, Internet search results, and technical support.

Manufacturer Documentation and Web Sites

Any hardware or software you buy comes with documentation. It could be a printed booklet in the box, a document file on the installation media, or a downloadable file from the company's web site. The original documentation

https://t.me/learningnets

should explain how the item works and may also provide some basic troubleshooting information. Documentation quality and detail varies widely, from nicely formatted 100-page manuals to a few vaguely English sentences on a half-sheet of paper. The manufacturer documentation (including additional documentation on a manufacturer-maintained web site) is the most authoritative source of information about the device or software.

If you've misplaced the original printed documentation, you can probably find it online, either at the manufacturer web site or at a third-party site. There are web sites that specialize in providing PDFs of product manuals, for example. Manufacturers also build documentation into the application in the form of a help file. Look on the menu bar or Ribbon for a Help command. More and more manufacturers save money by including documentation only in electronic form, rather than providing a printed manual.

Manufacturer web sites can provide excellent information. Depending on the size of the company, the Support section of the web site may integrate with the main site, or it may be a separate host like http://support.microsoft.com. On a manufacturer's web site you might find any of the following:

- Downloadable updates and patches
- Downloadable product manuals and setup utilities
- A customer support message board, with help both from company representatives and from other customers
- Press releases regarding new versions
- Existing-customer discounts for upgrading to new versions
- Product registration forms
- Warranty claim information
- Information about known problems and conflicts with certain hardware or software
- Contact information for technical support and customer service

---



NOTE *Technical support* provides help for operating the product; if the product isn't working as expected, you contact technical support. *Customer service* helps with financial and authentication matters, such as creating a user account, placing or canceling orders, and getting refunds. *Sales* is normally just for new sales, not billing or cancellations.

https://t.me/learningnets

Some support web sites request the exact model number or serial number of your computing device to customize the information presented. The Dell Product Support site shown in Figure 13-3, for example, identifies the exact model number of my laptop and offers to diagnose problems I might be having.

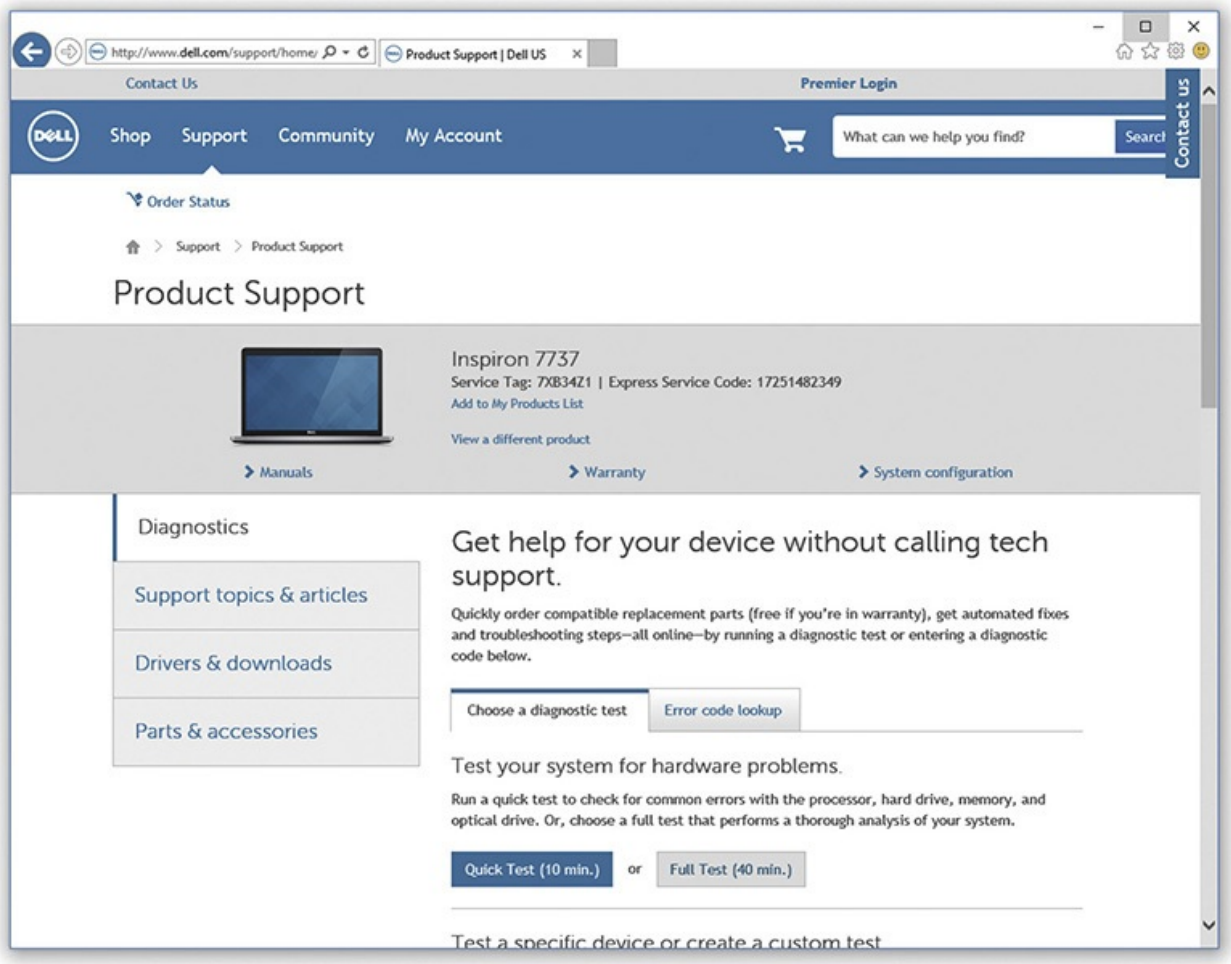


Figure 13-3 Dell's product support web site for my Inspiron 7737 laptop

Technical Support

The best way to get technical support for a product is usually via the web site. Technical support web sites can help you diagnose problems, update drivers and firmware, get product enhancements, and more. Your problem may appear in the Frequently Asked Questions (FAQ) section of the web site. If not, you can send an e-mail message asking for help.

https://t.me/learningnets



NOTE Sometimes the FAQ is just a document with common questions; some companies use a *knowledge base*, which is a little like a cross between the FAQ and a support forum. A knowledge base typically highlights the most common questions but also includes less frequently asked questions.

The Contact us link on a tech support web site usually leads to a form you can use to submit a support request. This is usually your best bet if you don't need an immediate answer. You might have to wait 24 hours for a response (usually via e-mail), but that's 24 hours where you can be doing something else. With phone support, you might get an answer after being tortured for an hour with low-quality elevator music and automatic reassurances about "how much your call matters" and how "we are experiencing unusually high call volume" and how "your call will be answered in the order it was received."



NOTE With luck, you'll be able to use some of the more compassionate support improvements pioneered in recent years, such as the ability to chat with a support person in your browser or to go about your business and receive a callback when a representative is available.

A phone call to the company's technical support line is usually a last resort. Some companies make it really easy to find the tech support phone number on the web site; others bury it in the fine print, hoping you won't be able to locate it. They do this because phone support costs a lot to provide, so don't be surprised if finding the phone number is only the first hurdle. Telephone support systems commonly include long automated menus crafted to avoid connecting you to a living, breathing human.

Internet Searches and Community Groups

If the manufacturer's web site and tech support department let you down, the next step is to see what the Internet at large has to offer. Use one of the popular search engines, such as Google or Bing, to see what's out there for your particular model number or product name. Keep in mind that the results of such searches aren't authoritative, so take what you find with a grain of salt. For

https://t.me/learningnets

example, one person might write about some complicated system file hack he used to solve a similar problem to yours, but don't assume that it is safe to try on your system.

Internet searches can connect you to user posts that mirror or match the trouble you have. Sometimes, an Internet search points you to that perfect solution. Implement it and you're on your way. Other times you might discover that you simply can't solve the current problem directly. You might find out, for example, that it's a known problem that your game won't run on systems with a certain type of video card or that you can circumvent a particular error by making a BIOS/UEFI setting change.



CAUTION Don't download anything from an untrusted site. Don't download a driver for your display adapter that is supposed to be "better than" the one that the manufacturer provides, for example, and be wary of free antivirus, system repair, and disk cleaner tools. A lot of them are malware disguised as helpful programs.

If you're lucky, you'll find a technical community group (such as a support message board or chat room) specifically for the device or software that's causing problems for you. You may also be able to find computer user groups that meet regularly in your town. (Yes, actual people in a room together physically! Such wonders still exist.)

Chapter Review

This chapter provided some advice for situations where a computer, mobile device, peripheral, or application isn't working properly.

If the computer or device seems dead, it's probably disconnected or not getting power. If your device gets wet, don't turn it on until it's bone-dry. Take it apart to let it air out if possible. You can also put it in a bag of rice to dry it out. If a device stops working after you drop it, check to make sure no cables inside have come unplugged; it's easy enough to open up a desktop and look, but mobile and portable devices may need to go to a specialist. For a cracked screen, you'll need to take it to a repair shop.

If the computer starts performing poorly after an update or system change,

https://t.me/learningnets

use System Restore or the Windows Recovery Environment. If a certain app won't run, try uninstalling and reinstalling it. You can also try the Program Compatibility Troubleshooter. If a peripheral isn't working, check the connection, cord, and batteries.

Some places you can get help include manufacturer documentation, manufacturer web sites, technical support, Internet searches, and community groups, both online and in-person.

Questions

1. Which of these could *not* be the cause of a computer appearing completely dead?
   - **A.** Hibernate mode
   - **B.** Bad power cable
   - **C.** Disconnected power cable
   - **D.** Bad keyboard
2. Which of these is the most hazardous to a desktop computer or mobile device?
   - **A.** Dropping it
   - **B.** Leaving it in a hot car in the summer
   - **C.** Getting it wet
   - **D.** Leaving it in an unheated building in winter
3. What Windows utility returns the computer's system files to previously saved versions?
   - **A.** Control Panel
   - **B.** Compatibility Mode
   - **C.** File Explorer
   - **D.** System Restore
4. Which of these might correct a problem with an application not running correctly?
   - **A.** Delete your data files.
   - **B.** Clean the display screen.
   - **C.** Uninstall and reinstall the application.

https://t.me/learningnets

D. Create a shortcut to the application on the desktop.

5. Suppose you have a wireless mouse that doesn't work at all. Which of these is *not* likely to be the cause?

A. The mouse is dirty.

B. The power switch on the mouse is turned off.

C. The transceiver is not connected to the computer.

D. The batteries are dead.

6. You have a printer that connects to your computer via USB cable. The printer can print a test page successfully from its own controls, but the computer doesn't see it. Which of these should you try?

A. Use a different printer cable.

B. Replace the ink cartridges.

C. Turn the printer off and then back on again.

D. Use a different kind of paper in the printer.

7. Which is the most authoritative source of information about a device?

A. Friend and relatives

B. Internet search

C. Community user groups

D. Manufacturer's web site

8. What is the FAQ?

A. The main page of a manufacturer's support web site

B. A web page containing frequently asked questions and their answers

C. An index of all help topics on a web site

D. A utility that identifies your product's model number

9. If you need to cancel an online subscription, what department of the company do you need to contact?

A. Customer service

B. Technical support

C. Service

D. Sales

10. Which of these would likely be found on a manufacturer's support web site?

https://t.me/learningnets

A. Downloadable product manuals

B. New versions of the device's drivers

C. Troubleshooting information

D. All of the above

Answers

1. **D**. A bad keyboard would not prevent the computer from starting up, although you might see an error message.
2. **C**. Water is the most serious hazard to computers.
3. **D**. System Restore allows you to return system files to earlier versions.
4. **C**. Uninstalling and reinstalling an application sometimes corrects problems with the application's performance.
5. **A**. A dirty mouse would not appear completely dead, although it might result in an erratically moving pointer on-screen.
6. **A**. A different printer cable might allow the computer to see the printer. All the other solutions would not be likely to help since the printer has already proven to be working.
7. **D**. The manufacturer web site is the most authoritative source of information.
8. **B**. FAQ stands for Frequently Asked Questions. It is a web page commonly found on a manufacturer's support web site.
9. **A**. Customer service handles financial matters relating to existing accounts.
10. **D**. All of these items are commonly found on a manufacturer's support web site.

https://t.me/learningnets

PART IV

Databases and Software Development

- **Chapter 14** Understanding Databases
- **Chapter 15** Software Development and Implementation

https://t.me/learningnets

CHAPTER 14

Understanding Databases

In this chapter, you will learn how to

- Explain database concepts
- Structure a database
- Create and manage databases

Databases store data. They can be used to store banking records, grocery store inventory lists, income tax filings, smartphone app configuration settings—databases are everywhere! Database storage is *persistent*, meaning the data will still be there even if you reboot the database server.

The CompTIA IT Fundamentals exam will test you on your database knowledge, and as an IT professional, database knowledge is essential. This chapter first covers database concepts and then describes database structures; finally, it explains how to manipulate data.

Database Concepts

Databases are used to store data in an organized manner for quick searching and retrieval. Compare this to simply writing information directly into a text file. Extracting meaningful data from a text file compared to a database can be difficult because there is no detailed structure as to how individual pieces of data are stored. Simple data storage, such as in a text file, is referred to as *flat-file* storage.

As an example, imagine you are the owner of a musical instrument store. When making a sale, you need to store customer information along with items purchased, which must also be removed from inventory. Databases make storing, retrieving, and reporting on this type of related information easy compared to simply blasting the information into a big text file. Think of a database as a container within which *tables* are used to store *records*, also called *rows*. Figure

https://t.me/learningnets

14-1 shows a subset of tables contained in the Microsoft AdventureWorks 2012 sample database. Each row in a table consists of *fields*, or *columns*, that store small pieces of data such as first name, last name, date of birth, and so on. Each column can have a maximum length such as ten characters, a requirement for data entry, a data type such as int (integer) or char (character), and other properties.

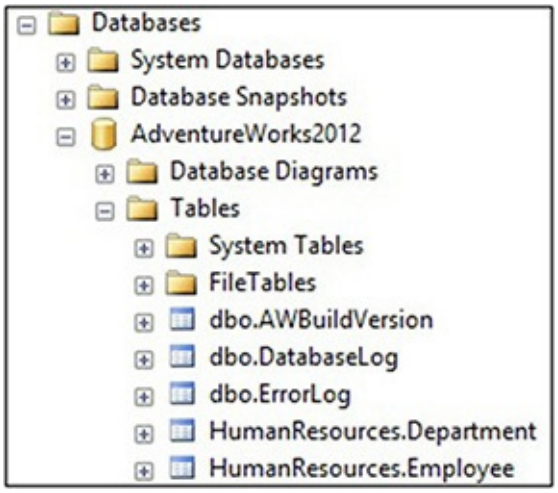


Figure 14-1 Microsoft SQL Server database tables

Database Table Structure

Designing a table structure must account for how you need to manipulate and query (ask questions about) the data. You can populate database tables by importing data from a local file or over a network, by executing a script, or by manually inputting data.

Let's say you anticipate needing to search for specific musical instrument makes and models in your music store endeavor. Instead of storing all musical instrument details together in a single field in the database as shown in Table 14-1, you could break it up into multiple fields as shown in Table 14-2.

Field Name	Sample Data
Musical Instrument	Guitar Gibson A456-899 Cobalt Burst 899.99 1999.00 2018 gabc123 4 Hfx12

Table 14-1 Musical Instrument Details Stored in One Field

https://t.me/learningnets

Field Name	Sample Data
Category	Guitar
Make	Gibson
Model	A456-899
Color	Cobalt Burst
Wholesale Cost	899.99
Selling Price	1999.99
Year Manufactured	2018
Inventory ID	Gabc123
Quantity In Stock	4
Store Code	Hfx12

Table 14-2 Musical Instrument Details Stored in Separate Fields

Breaking a record into fields means searching your database will be quicker. Figure 14-2 shows a sample table definition. In our example, searching for Gibson guitars will be easy, and the search (or query) will execute quickly since it only has to search through the Make field and not the others.

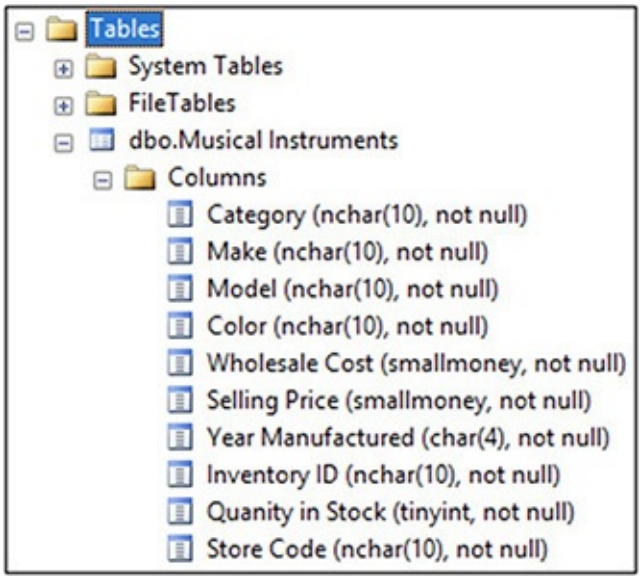


Figure 14-2 Sample table with column definitions

https://t.me/learningnets



EXAM TIP Breaking data down into its smallest units helps database queries perform better. Indexes are normally built on one or more fields to speed up ordering and searching.

Database Scalability

Scaling a database means making sure it can accommodate current and future storage requirements as well as provide the best possible performance for data reads and writes. Database solutions run on a physical or virtual machine, and the power of that machine relates directly to database performance.

You can install and configure operating system and database software manually, or you can provision databases quickly without having to install anything. The latter is common in cloud computing and is called a *managed service*. Managed services make provisioning resources such as databases quick and easy, thus allowing database builders to focus on solving business problems instead of on the underlying technology.

Compute Power

There is a limit to how much RAM and CPUs you can stuff into a single physical or virtual machine. If your database needs it, more power is always better, but what happens when you max out the horsepower? The answer: scale out.

Scaling out, also called *scaling horizontally*, means adding compute nodes or database replicas to support a busy computing environment. This can be done manually or automatically in response to preconfigured thresholds (autoscaling). Increasing the underlying computer horsepower is called *scaling up* or *vertical scaling.* Bear in mind that databases are designed to support many concurrent users. Database compute nodes can work together to provide high availability and improved performance.

Database Storage Performance

A great thing about cloud computing is its rapid elasticity. You can provision additional cloud storage at a moment’s notice with the click of a mouse. Compare this with the traditional method of purchasing disks, installing them

https://t.me/learningnets

into servers, and then partitioning and formatting them. You might never use all of the space either; obviously this is time-consuming and potentially wasteful.

Not only should you consider storage space for databases, both on-premises and in the cloud, but you should consider the nature of how the database will be used. Will it be used more for reading (querying) or for writing data, or a combination of both? For example, you might have a single writable database replica and multiple read replicas to support intensive querying.

Input and output operations per second (IOPS) is a unit of measurement related to storage devices. More IOPS is better, but more IOPS means more cost. Like storage capacity, this is easily configured with cloud database solutions, as you can see in Figure 14-3. It's a bit trickier and takes longer to increase database IOPS in a traditional on-premises environment.

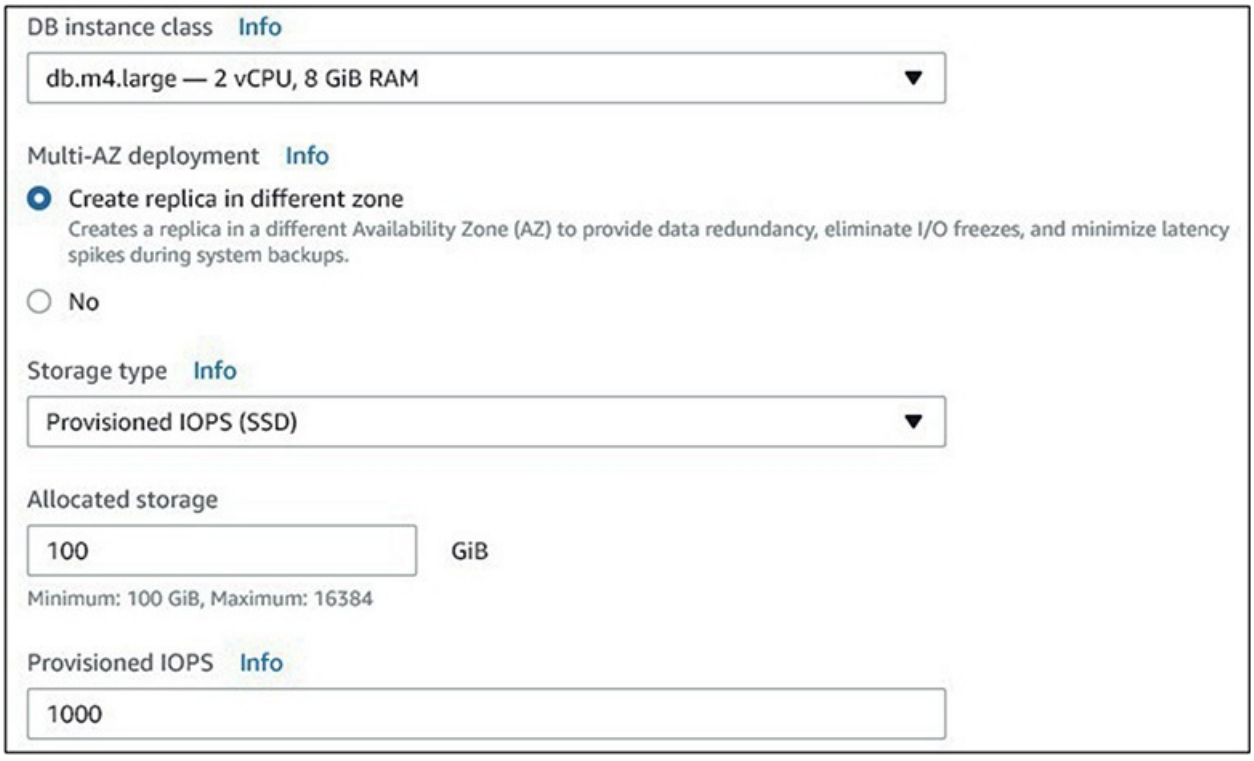


Figure 14-3 Amazon Web Services database replica and IOPS settings

Database Persistence

For high-volume database transactions, there are in-memory cache solutions such as Redis and Oracle In-Memory Database (IMDB) cache. These solutions can be configured on-premises, but setting them up through public cloud providers like Amazon Web Services or Microsoft Azure is much simpler and

https://t.me/learningnets

takes only a matter of minutes.

Reading and writing data from and to RAM (volatile memory) is many times faster than reading and writing even to the fastest disk storage. When your application needs the quickest possible database access time, consider in-memory caching.

Storing database data on disk is referred to as *persistent storage* because the data hangs around even between system reboots. When the data is in a memory cache, it is referred to as *nonpersistent storage*.

Database Structures

Using the best database solution that fits your needs is crucial. There is no one-size-fits-all for this type of thing, and configurations will vary from one business to the next. Here are some factors to consider when choosing a database solution:

- **Type of database** Relational or NoSQL
- **Location** On-premises or in the cloud
- **Security** The ability to encrypt data at rest and in transit
- **Isolation** Deployed into its own network
- **Vertical scaling** CPUs, RAM, disk IOPS
- **Horizontal scaling** Additional database servers or replicas

Relational Databases

Relational databases have been around for a long time. This type of solution uses a structured *schema*, or blueprint, of how data should be stored through column (or field) definitions. With a structured schema, all rows (records) within the table follow the same rules for what type of data can be stored, as in the following example:

- Lastname: Jones
- Firstname: James
- Date of birth: 5/12/1965
- Street number: 564
- Street name: Maple Street
- City: Halifax

https://t.me/learningnets

- Province: Nova Scotia
- Country: Canada
- Postal Code: B2R 4E9

The world *relational* is used because related tables can be linked together. For instance, a Customers table might be linked to a Transactions table in a query; this way you can view transaction data and customer data at the same time.

Related database tables are joined using some kind of unique identifier called a *foreign key*, which is a combination of one or more fields (columns) in both tables. In our example, such a field might be called CustID, and it would exist in both the Customers and Transactions tables. A unique identifier within one table is called a *primary key*. In Figure 14-4, the primary key shows up with a small key icon to the left of the field name.

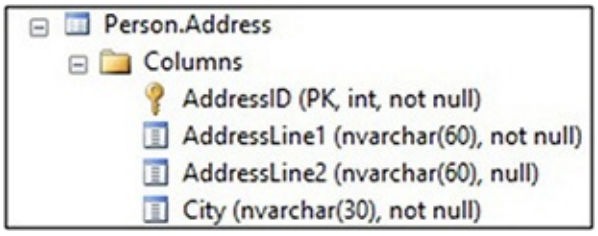


Figure 14-4 Sample table definition in Microsoft SQL Server

Constraints such as *referential* integrity can prevent the addition of rows unless there is a corresponding foreign key in a parent table. For example, the addition of a transaction in the Transactions table might be disallowed if a corresponding CustID does not exist in the Customers table.

Examples of common relational databases include the following:

- Oracle Database
- Microsoft SQL Server
- MySQL
- PostgreSQL



EXAM TIP Make sure you understand the importance of foreign keys and

https://t.me/learningnets

how they apply to relational DATABASES. NoSQL databases are different in that they are not designed based on table relationships but instead are based on the queries that will be run.

NoSQL Databases

Unlike relational databases, NoSQL is not as rigid about the definition (schema) of how data will be stored. Depending on the specific product, there might be a semistructured schema or no schema at all! If that's the case, then what is the benefit of a NoSQL database compared to a relational database? Easy: scalability and performance.

There is so much existing data as well as new data being generated daily (big data) that a solution designed to handle this massive scale of changing information is needed, and that solution is NoSQL. An emphasis on "changing" is important here, not just changes in the data itself but also in the data structure. This wouldn't work well with a relational database using a rigid schema that must define the specific data that will be stored. Think of the constantly changing world of online gaming or social media and the content that goes along with it. Think of storing text files, multimedia files, e-mail messages, office productivity files—the contents of these files will almost always vary and are therefore perfect for unstructured data sources such as NoSQL.

Common NoSQL Database Types

Key-value databases are simple in that a key (also called an *attribute*), such as SiteURL, is stored along with its value, such as https://www.acmesocialmedia.com. What's interesting about this is that a single NoSQL data store might contain rows that have different types of data, unlike a relational database. The simplicity of this design lends itself to less resource consumption on a database server, which results in better performance.

Document databases are generally more complex than key-value databases. Multiple key-value pairs or even nested documents can exist within a single document. A *document* is conceptually similar to a row or record in a relational database. Documents can be standard user files such as Microsoft Excel files, XML files, JSON files, and so on. Each document in the database can have a completely different structure, which is why NoSQL databases are often called *schema-less*. A group of documents is referred to as a *collection* and is used to work with subsets of data.

Examples of common NoSQL databases include

https://t.me/learningnets

- Oracle NoSQL
- MongoDB
- CouchDB
- IBM Domino

Database Creation and Management

Whether you plan on using a relational or NoSQL database, the creation methods are pretty much the same.

- **Manual** You can use commands such as the Microsoft SQL Server CREATE DATABASE command, or you can use graphical user interface (GUI) tools.
- **Scripted** You can create or acquire a script that will create the database and even populate it with data.
- **Template** Cloud providers such as Microsoft Azure support resource deployment (including databases) using Azure Resource Manager (ARM) templates, which also support parameters for reusability. The equivalent solution available through Amazon Web Services (AWS) uses CloudFormation templates.
- **Virtual machine image** You can use an image that already includes the database engine; this is prevalent in the cloud (see Figure 14-5).

https://t.me/learningnets

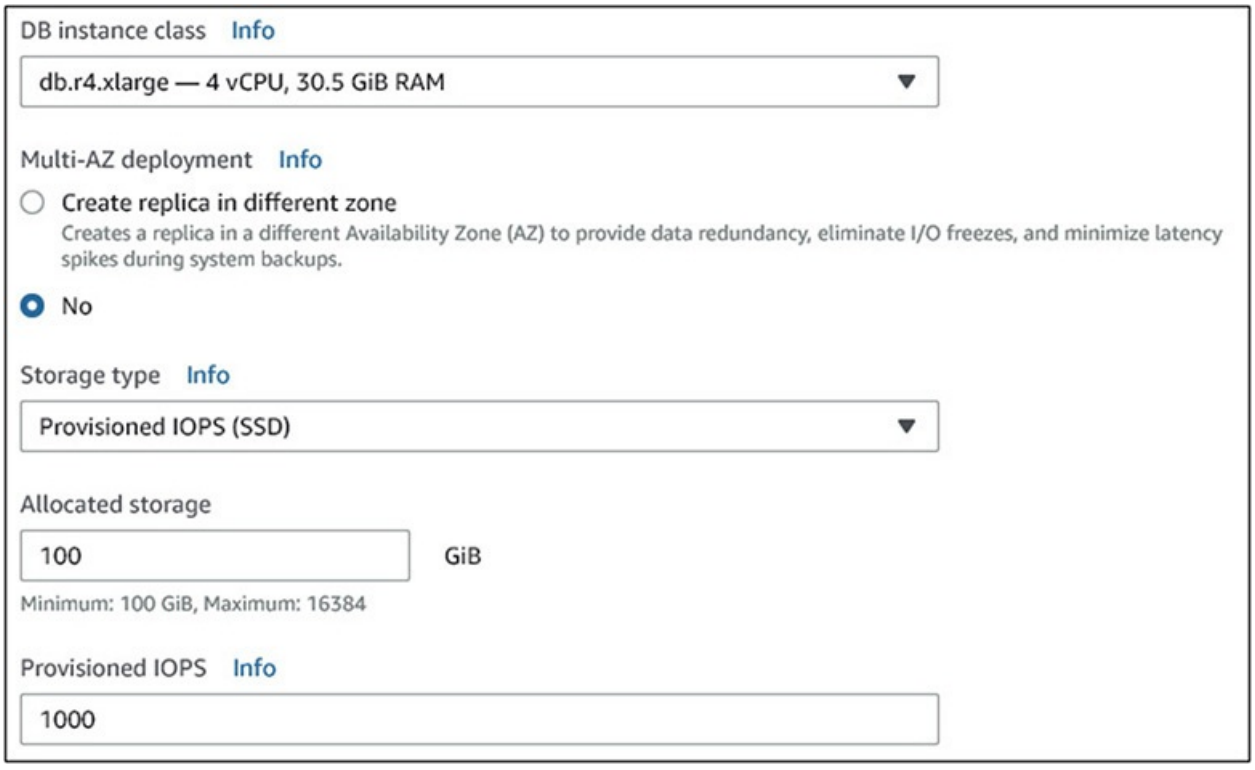


Figure 14-5 Cloud MySQL deployment options available using the Amazon Web Services GUI

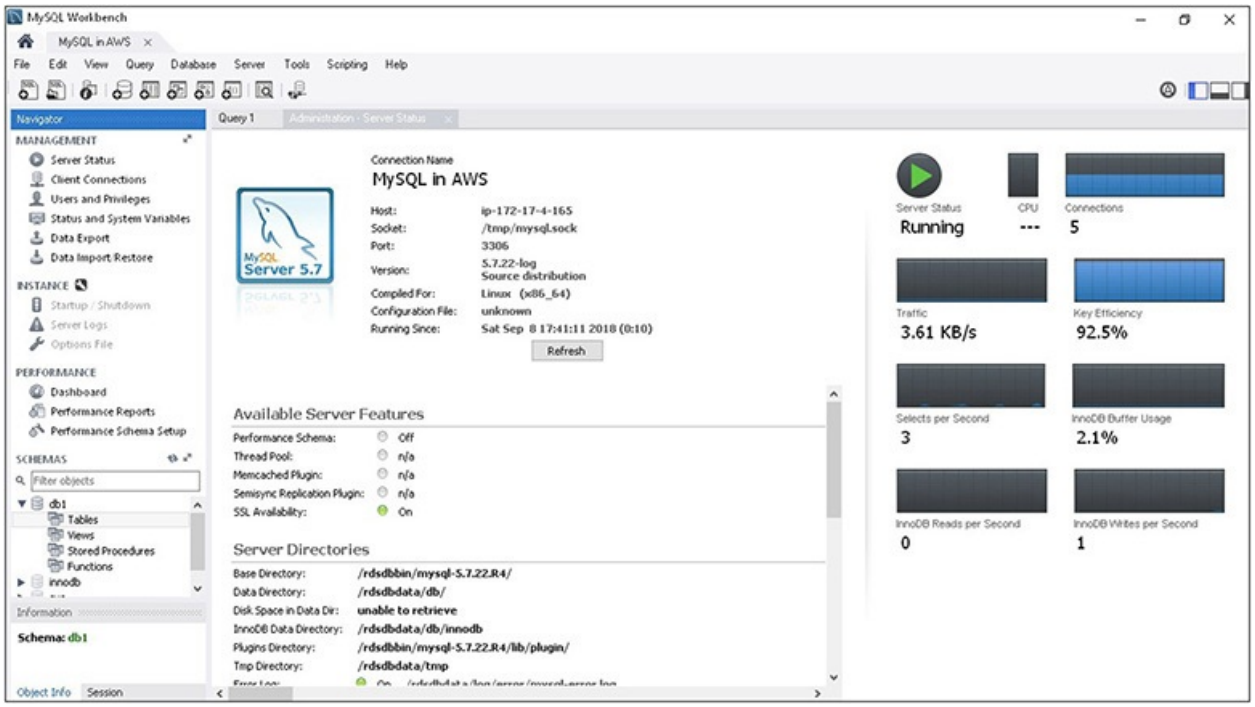


Figure 14-6 The MySQL Workbench utility

https://t.me/learningnets

Aside from creation, other common database administration activities include applying updates and setting permissions. CRUD is a term often used to refer to create, read, update and delete database actions. Technicians can use command-line and GUI tools to perform the tasks listed in Table 14-3.

Task	Description
Alter	Modifies the design of an existing relational database or table
Drop	Deletes an existing database or table
Grant/revoke	Adds or removes permissions for database objects

Table 14-3 Common Database Management Tasks

Database Connectivity

Database engines run on physical or virtual servers and listen on a port number, much like radio receivers listen on a specific frequency. Users and technicians can connect to database objects and rows using a variety of methods, as shown in Table 14-4.

Database Access Method	Description

Manual/direct	Users connect to the database directly without a separate front end. Using database solutions such as MySQL allows users to design and use database objects directly through the command line, depending on their permissions.
	The following MySQL commands log in as user1, connect to the employeesdatabase1 database, and finally return all rows from the employeestable1 table.
	`mysql -u user1 -p`
	`show databases;`
	`use employeesdatabase1;`
	`select * from employeestable1;`

Programmatic	Developers write custom code to access database objects. The following PHP code makes a programmatic connection to a MySQL server:
	`<?php`
	`$servername = "dbserver1";`
	`$username = "user1";`
	`$password = "Passw0rd";`
	`$connection = new mysqli($servername, $username, $password);`
	`?>`

User interface/utility	Users access database objects through a front-end GUI such as a web site connected to a back-end database or utilities such as MySQL Workbench, as shown in Figure 14-6.

Table 14-4 Database Access Methods

https://t.me/learningnets

By default, Microsoft SQL Server listens on TCP port 1433, and MySQL listens on TCP port 3306. Firewalls need to allow this inbound traffic for a successful connection.

Database Security

Hardening a database server involves changing default configuration settings, applying OS and database updates, enabling anti-malware solutions, and adhering to the principle of least privilege (PoLP). The PoLP states that only the permissions required to complete a task should be granted and nothing more.

Database network transmissions can be protected through the use of encrypted virtual private network (VPN) tunnels or Secure Sockets Layer/Transport Layer Security (SSL/TLS) security certificates. Protecting stored data (data at rest) is achieved in many ways. Microsoft SQL Server, for example, supports Transparent Data Encryption (TDE).

Just like with operating systems, setting user account permissions and password settings determines which users have access to database objects. Figure 14-7 shows Microsoft SQL Server roles that can be assigned to users so you can grant permissions.

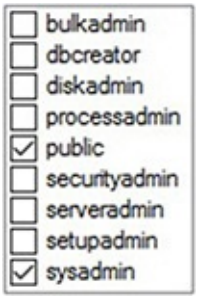


Figure 14-7 Microsoft SQL Server roles

Manipulating Data

Most databases provide not only command-line tools for data manipulation but also GUI tools. Custom solutions (such as web sites that talk to databases) are also common.

Modern web apps often consist of a front-end web GUI tier that reads and writes to a separate database tier, which is often on its own isolated network and protected by a firewall.

https://t.me/learningnets

Getting Data Into Databases

Databases are useful only when they contain relevant data. Database designers will often build field validation rules to control what can be stored in a field.

For example, a Canadian postal code field might have an input mask that allows only LNL-NLN (where *L* is a placeholder for *letter* and *N* is a placeholder for *number*). An example would be B4C-2G4. This rule is honored regardless of how data comes into the system. Common data insertion and modification methods include

- Manual data entry
- Importing a supported file such as a CSV file or backup file
- Programmatically from another app component locally or over the network
- INSERT INTO relational database command
- UPDATE relational database command
- Update queries

Querying and Removing Data

Over time data is no longer required and can be either deleted or archived for long-term storage. Archive settings are often dictated by regulations. Another reason data eventually gets removed from a database is because it can slow down database actions such as updates and queries.

Getting data out of databases is also achieved by running queries. Queries are used to filter data for viewing or, in some cases, for modification or deletion. Relational databases can use the SELECT command to filter data. Consider the following example that extracts specific table fields containing specific values and sorts (ordering) by a specific field:

```
SELECT field1, field2 from tablename WHERE field1=value AND
field2=value ORDER BY field1
```

Common data removal and backup methods include

- Manual data deletion
- Automated archiving
- Delete queries
- Exporting a database dump to a file

https://t.me/learningnets

- Database local or cloud backup



NOTE Many production databases have automated maintenance tasks to migrate infrequently accessed data to another storage tier, such as for archiving.

Query and Report Builder Tools

Most databases provide query and report building tools that are GUI based. This allows extracting relevant data (via a query) to base a report on. Figure 14-8 shows a query builder screen for Microsoft Access 2013.

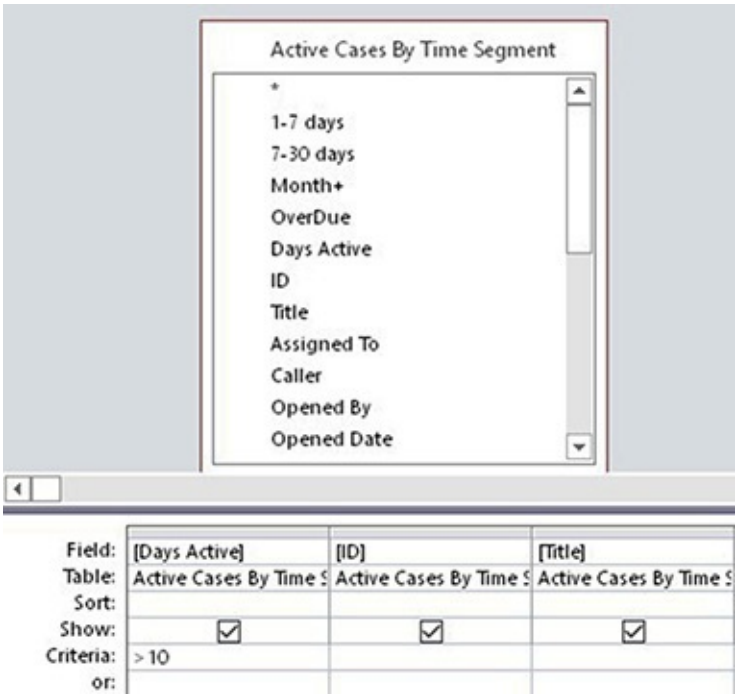


Figure 14-8 Simple query in Microsoft Access

Most databases come with preconfigured reports, but sometimes you'll have specific needs not addressed by existing reports. For example, you might want to include the company logo at the top, control text formatting, include specific data with numeric totals, and so on.

Luckily, there are plenty of report building tools for a wide variety of databases. Figure 14-9 shows a report designer in Microsoft Access 2013.

https://t.me/learningnets



Figure 14-9 Microsoft Access report designer

Chapter Review

This chapter provided insight into what databases are and why they're important.

Flat files do not allow you to join multiple related tables using a foreign key. A foreign key is a unique identifier consisting of one or more fields (columns).

Databases contain tables that in turn contain fields, or columns. For relational databases, this is a rigid design in that all table records, or rows, share the same underlying design. The opposite is true with NoSQL databases; each row can have a different structure.

Increasing the CPUs, RAM, and disk IOPS is called *scaling up*. Adding compute nodes is called *scaling out* and can be automated with autoscaling. Both types of scaling (up and out) can support a larger database user base and increase performance.

You can optimize the disk subsystem for your database by ensuring there is adequate storage space and that the disk IOPS is as high as possible. Adding database read replicas can offload data reads from a primary replica that supports writing.

Relational databases use a rigid schema, or blueprint, that describes what type of data will be stored. NoSQL databases use either a semistructure or no structure when it comes to the database schema; this allows NoSQL databases to grow on a massive scale while maintaining optimal database performance.

The relational database CREATE DATABASE command creates database objects. The ALTER command modifies the design of an existing object. DROP

https://t.me/learningnets

is used to remove objects such as tables. The GRANT and REVOKE commands are used for database permissions management.

Database connectivity is achieved manually by users or programmatically. Microsoft SQL Server listens on port 1433, and MySQL listens on port 3306. Database security is achieved with network and local database encryption in addition to adhering to the principle of least privilege.

You can populate a database by entering the data manually, by importing files locally or over network, or by using the relational INSERT INTO command. Data modifications are achieved manually, programmatically, or through update queries. Data deletions are achieved manually, programmatically, or through delete queries.

Databases backup targets can exist on-premises or in the cloud. Data exports, such as database dumps, can be used to recover the database in case of disaster.

The relational SELECT statement is used in standard queries to extract data from database tables. Query builders provide a GUI to facilitate the creation of queries that can then be used as a basis for creating reports.

Questions

1. What is another term used to refer to a field?
   - **A.** Row
   - **B.** Collection
   - **C.** Column
   - **D.** Foreign key
2. Your database has grown over time, and you need to improve query performance. What should you do? (Choose two.)
   - **A.** Perform a database dump
   - **B.** Remove infrequently accessed data
   - **C.** Create an index for queried data
   - **D.** Create a foreign key
3. You have increased the amount of RAM available for your cloud-based database instance. Which term describes this action?
   - **A.** Scaling in
   - **B.** Scaling down

https://t.me/learningnets

C. Scaling out

D. Scaling up

4. You have increased the number of compute nodes for your cloud-based database instance. Which term describes this action?

A. Scaling in

B. Scaling down

C. Scaling out

D. Scaling up

5. You have configured a database in the headquarters office located in Houston, Texas. Your company has office in major cities across Canada and the United States. Users in Eastern Canada complain about slow query access to the database, while Texas users enjoy fast performance. What should you do?

A. Place a read replica in Eastern Canada

B. Create an index

C. Place a writeable replica in Eastern Canada

D. Create a foreign key

6. Which unit of measurement relates to disk throughput?

A. MHz

B. GHz

C. IOPS

D. Uptime

7. Which type of database does not use a rigid schema?

A. Relational

B. On-premises

C. Cloud

D. NoSQL

8. Which type of database uses a rigid schema?

A. Relational

B. On-premises

C. Cloud

D. NoSQL

https://t.me/learningnets

9. What statement regarding NoSQL databases is correct? (Choose two.)
   - **A.** Each row must store the same type of data.
   - **B.** They are less scalable than relational databases.
   - **C.** Each row can store different types of data.
   - **D.** They are more scalable than relational databases.
10. Which of the following is a NoSQL database?
   - **A.** Microsoft SQL Server
   - **B.** MongoDB
   - **C.** Oracle Database
   - **D.** MySQL

Answers

1. **D**. *Column* is synonymous with *field* when it comes to database structure terminology.
2. **B**, **C**. Indexing orders field values and thus speeds up queries (searches). Reducing the amount of data also speeds up searching.
3. **D.** Scaling up refers to increasing compute characteristics such as the number of CPUs, the amount of RAM, and the number of disk IOPS.
4. **C**. Adding compute nodes to support a busy IT workload is called *scaling out*.
5. **A**. Placing a database read replica physically near users will reduce network latency.
6. **C**. Input and output operations per second (IOPS) is a unit of measurement related to disk performance; more IOPS means better performance.
7. **D**. NoSQL databases are used to store large amounts of unstructured data and as such do not use a rigid schema to define what type of data will be stored.
8. **A**. Relational databases use a rigid schema to define what type of data will be stored.
9. **C**, **D**. NoSQL databases do not use a rigid schema, which means different rows could contain completely different types of data. Because of the simple structure for NoSQL storage, NoSQL databases scale much better than a relational database.

https://t.me/learningnets

10. **B**. MongoDB is a NoSQL database.

https://t.me/learningnets

CHAPTER 15

Developing and Implementing Software

In this chapter, you will learn how to

- Plan software solutions
- Choose a programming language
- Pick the right data type
- Use constants and variables
- Control program flow
- Reuse code with functions

We are all exposed to many different types of software during the course of a day. Using your smartphone operating system, checking the weather via an app, checking your bank account, submitting work travel expenses, booking a hotel—software is everywhere!

Not only must creators of software understand how to code in a given programming language, but they must also be able to determine the problem the software will address and the requirements necessary to make it all happen. Writing code requires knowing how to pick the right data type, how to create and call functions, and how to control program flow. In this chapter, we'll cover these topics and more!

Software Development Life Cycle

The software development life cycle (SDLC) is a six-step structured framework (see Figure 15-1) used by software developers to create and maintain software solutions. The SDLC is also referred to as the *systems development life cycle*. One factor that is consistent throughout all SDLC phases is security; this is something that should not be left as an afterthought.

https://t.me/learningnets

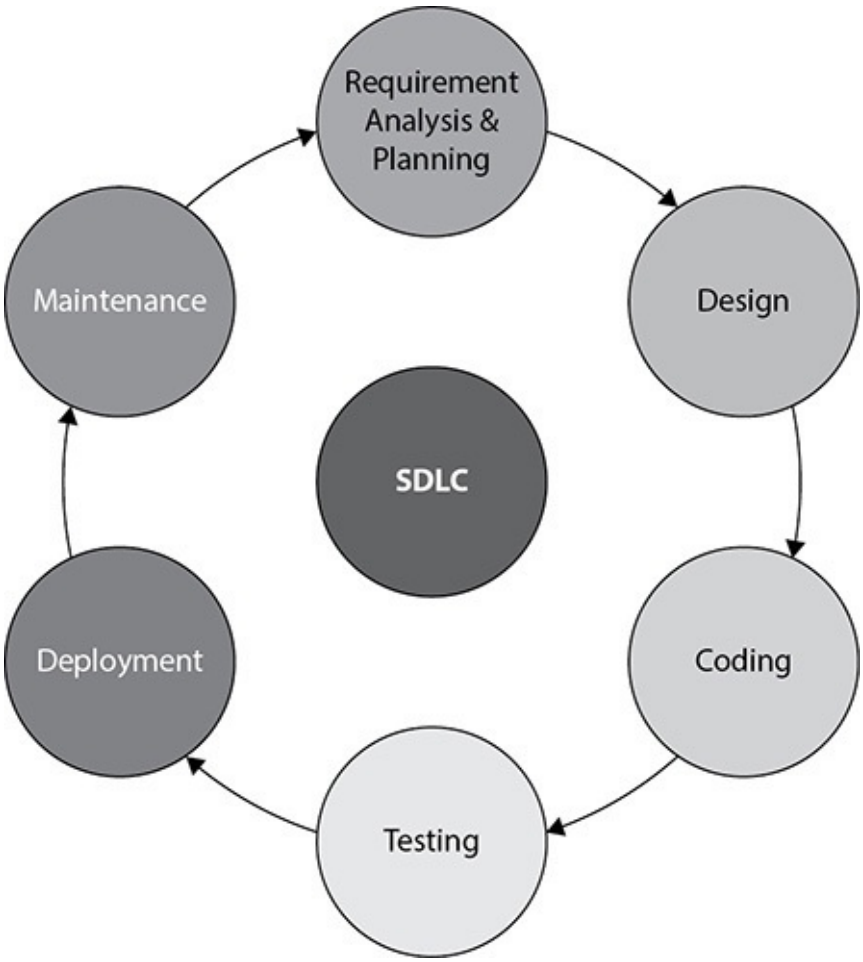


Figure 15-1 The six stages of the software development life cycle

You've probably, at some time, experienced software deficiencies such as software crashing or security vulnerabilities. Security fixes and updates are created to address these issues. Software developers use the SDLC not only for the initial creation of software but also for its continuous improvement.

Software can run within a server, desktop, laptop, smartphone, or specialized device operating system environment. Software can be an entire operating system, a stand-alone application, a web browser plug-in, or even software embedded within a chip (firmware). Regardless of the software type and how it will be used, the SDLC provides a structured approach for creating and maintaining the solution.



NOTE Using a scripting language such as Linux bash or Microsoft

https://t.me/learningnets

PowerShell to create quick automated solutions doesn’t require going through the SDLC.

Requirement Analysis and Planning

Software is created to entertain people or solve problems; it includes games, music-streaming apps, customer relationship tracking programs, patient medical statistics programs, and so on. In the business world, software is used to automated business processes. When planning a software solution, a number of factors must be considered:

- Users of the solution
- Overall purpose of the solution
- Data inputs and outputs
- Legal and regulatory compliance
- Encryption of data at rest and in transit
- Allocation of human and financial resources
- Project scheduling

All of these factors are combined into a document called a *requirement specification document*, which is used as a blueprint for further SDLC phases. All stakeholders affected by the development of the solution, such as end users, should be involved in voicing opinions about what the software will do and how it will do it.

Design

In this SDLC phase, using the requirement specification document from the first phase as a guideline, software developers can map how inputs and outputs will be consumed and generated by the solution; this is often done using a series of flowcharts. Figure 15-2 shows a partial sample flowchart.

https://t.me/learningnets

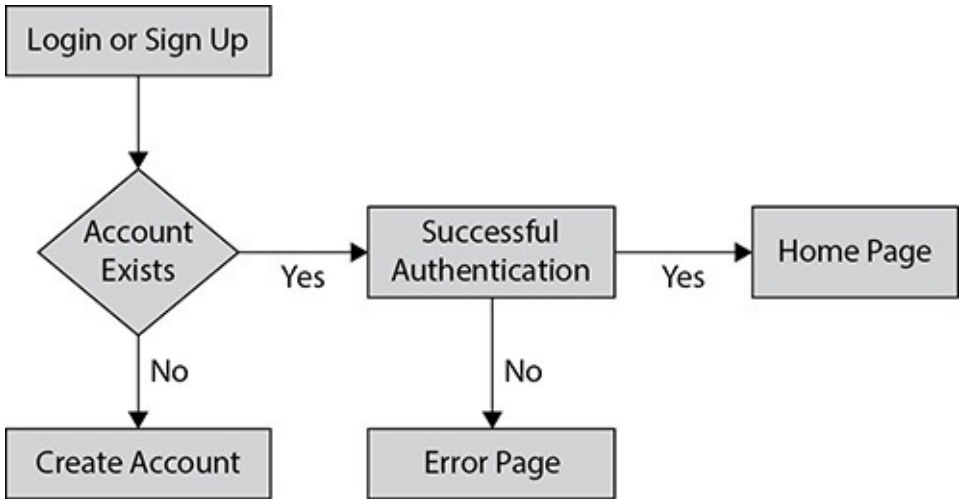


Figure 15-2 Partial sample application flowchart

Hardware Requirements

Software runs on hardware in the form of physical computing devices such as servers, desktops, laptops, tablets, and smartphones. Designers must take into account which type of device the software solution will run on and be accessible from. The amount of CPU power, RAM, disk space, and even graphics capabilities must be considered.

On the client side, supported devices must be determined along with the required hardware such as processor speed, amount of RAM, storage space, and network connectivity whether through a wired network connection, WiFi, or Bluetooth.

Software Requirements

Depending on the type of software being developed, there could be external dependencies on other software. This holds true even when creating software that will be embedded within a chip; there might be additional external software components that must also be embedded within the chip for proper functionality. External software requirements could include the following:

- A specific version of an operating system, such as iOS 11.4.1 on an Apple iPhone, to run certain apps
- Modular software components, such as a web browser plug-in that must be installed before using a web application
- Application programming interfaces (APIs) that expose functionality, such as allowing developers to call functions that will allocate cloud

https://t.me/learningnets

storage

- A specific identity provider, such as Microsoft Active Directory, Google, or Facebook

Coding

Project planners allocate code development tasks to developers or development teams, and in turn, software developers write code using a programming language. A modular, or *microservice*, approach is often employed where code chunks, or *modules*, are created, each with their own specific functionality. This means a software app could consist of many microservices. Changes, failures, and maintenance for specific microservice code does not directly affect any other microservices. The old method of creating a single large program is called a *monolithic* application.

The coding phase is the longest of all SDLC phases because it's where the core of the solution is built. There are plenty of available programming languages; the specific project environment, preference of the developer, or tools already in use will dictate which language is used.

Developers can use scripting languages such as Bash shell scripting (commonly used in Linux) or Microsoft PowerShell (commonly used in Windows). These are called *interpreted* languages because the code is not compiled to a program file; instead, it is run in an environment that supports the scripted statements.

Scripted solutions are often created by IT administrators to automate administrative tasks, as in the following PowerShell example that lists running Windows services:

```
Get-Service | Where-Object{$_.status –eq “Running”}
```

Get-Service is the name of a PowerShell command (cmdlet), and the vertical bar is a pipe symbol that passes data resulting from the command on the left to the command on the right. The Where-Object cmdlet filters output. $_ is a temporary placeholder for processing all returned items one at a time (in this case, all listed services), and finally the command is checking the status property for a value of Running.

Compiled programming languages, unlike interpreted languages, use a compiler program that results in a program file to run the software. Compilers render high-level, easy-to-read source code to machine code; however, compiling is unnecessary for the assembly programming language since it is

https://t.me/learningnets

already machine code.



EXAM TIP Make sure you know the difference between scripted versus compiled code. Scripting is normally used by IT administrators to automate repetitive administrative tasks, whereas compiled programs are more formal, larger programs that solve more complex problems.

Imagine that a developer uses the C programming language to create an app that runs on the Windows desktop platform. After compiling the code, the result will include at least one file, which is an executable (EXE) file that runs the program. Once the code is compiled, you can’t see the actual programming that makes the code work. Table 15-1 lists common programming languages.

https://t.me/learningnets

Language	Interpreted or Compiled?	Description
Assembly	Already in machine code	• Low-level; talks directly to hardware instruction sets; useful for small programs or tools that need to talk directly to hardware. • The following sets the focus on memory address 4440H and then moves data in that location: register B: lxi h, 4440H; mov b, m;

C	Compiled	• Case-sensitive, general-purpose programming language. Many operating systems, including Windows, are written in C or a derivative such as C++.
		• Includes the standard input and output library of functions.
		• The following creates a main function that displays the text "Hello Everyone" on the screen:
		#include <stdio.h>
		int main()
		{
		printf("Hello Everyone\n");
		return 0;
		}

Java	Compiled	• Case-sensitive; cross-platform, which means the same code will run on Windows, Linux, and macOS; requires a Java virtual machine (JVM) as an executable environment to run the code; useful when the same program should run on multiple platforms.
		• The following creates a Java class that displays the text "Hello Everyone" on the screen:
		public class HelloEveryone {
		public static void main(String[] args) {
		System.out.println("Hello Everyone");
		}
		}

Python	Interpreted	• Case-sensitive, general-purpose programming language; used often in Windows, Unix, and Linux environments as well as for server-side web app code; requires a Python engine to run the code. • The following displays "Hello Everyone" on the screen: print("Hello Everyone")

https://t.me/learningnets

JavaScript	Interpreted	• General-purpose scripting language that runs on the client side within a web browser. • The following displays "Hello Everyone" on a web page using the <script> HTML tag: <!DOCTYPE HTML> <html> <body> <script> alert('Hello, everyone!'); </script> </body> </html>
HTML	Interpreted	• Hypertext Markup Language; uses tags to format web pages that are rendered in a client-side web browser. • The following displays "Hello everyone" on a web page in large bold letters (heading 2, or h2) with an underline (horizontal rule, or hr): <html> <body> Hello everyone <hr> </body> </html>
XML	Interpreted	• Extensible Markup Language; uses tags to describe (and not format) data; often used to exchange data between dissimilar systems over a network or through file importing and exporting. • The following shows basic data related to an e-mail message: <message> <to>Amy</to> <from>Bob</from> <subject>2019 Budget Due</subject> <body>Please submit by end of day Friday, thanks. </body> </message>
SQL	Interpreted	• Structured Query Language; used to ask questions about and retrieve data from relational databases. • The following retrieves all rows from a table: SELECT * FROM Customers; • The following retrieves only specific columns from a table: SELECT LName, FName, City FROM Customers; • The following retrieves only those customer transactions over $500: SELECT * FROM Transactions WHERE Amount > 500;

https://t.me/learningnets

Graph API	Compiled	• Can be used to read and write data to systems such as Microsoft Azure and Facebook; commonly used by software developers building mobile device apps.
		• Given a unique item or node ID, the following reads social media–posted data using a GET statement; the return result is also listed for a single item:
		GET https://graph.facebook.com/820314001277881/feed
		{
		"data": [
		{
		"created_time": "2018-11-08T01:08:21+0000",
		"message": "FakeCo provided excellent service, I would definitely return here!",
		"id": "820314001277881_1805993182846942"
		},
		]
		}

Table 15-1 Common Software Programming Languages

Programmers will often write pseudocode to plan the actual code, which will follow. For example, “Retrieve username from user input” is pseudocode, whereas the following is the corresponding actual code in the Python programming language:

```
username = raw_input("Enter username: >> ")
```

A second pseudocode example is “Retrieve social media–posted items,” and the actual Graph API code would look something like this:

```
GET https://graph.facebook.com/820314001277881/feed
```

Regardless of the programming language in use, larger projects will involve multiple software developers. A code repository such as GitHub (Figure 15-3) can be used to track changes to code as well as to allow code to be downloaded on a developer’s workstation. Some tools such as Microsoft Visual Studio Team Foundation Server allow developers to “check out” code so that they can make changes but others don’t. Checked-out code is readable but not writable by other developers.

https://t.me/learningnets

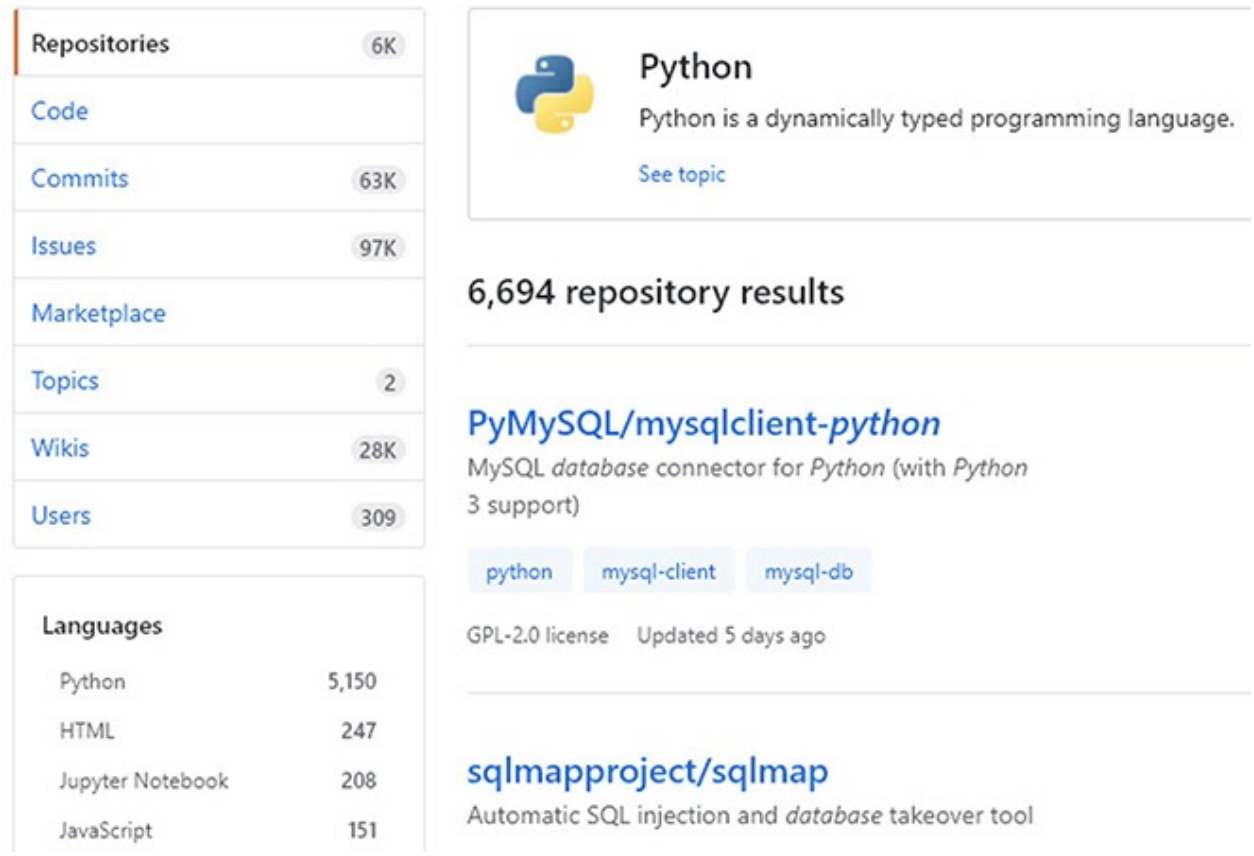


Figure 15-3 Python code available through GitHub

Testing

During initial software development and then as updates are created over time, code needs to be thoroughly tested to ensure it is stable, it is secure, and it performs the required functions. Testing can be manual, automated, or a hybrid of both.

Many software developers will deploy test (sandbox) environments consisting of virtual machines hosting web servers, authentication servers, database servers, mobile device simulators, and so on, in a cloud computing environment because of the speed of deployment and low cost compared to acquiring physical hardware on-premises. This type of environment can be completely isolated from other networks. Debugging is then used to verify the proper functionality of chunks of code in alignment with requirements from the first phase of the SDLC.



https://t.me/learningnets

NOTE Although not covered in this chapter, in reality building software solutions includes creating error-trapping code to gracefully exit the program when unanticipated events occur.

Common Types of Testing

When code changes are required, different types of testing can be used. In larger development environments, a developer checks out a chunk (module) of code for modification so that other developers cannot modify it. The code can then be tested, and upon successful testing the compilation and deployment of the changes can occur manually or in an automated fashion.

Unit testing is applied not to the entire software solution but to modules or chunks of code. This allows other code modules to remain functional or to be modified by other developers. *Regression testing* is used to make sure new code changes haven't broken code that worked previously. You've probably experienced installing some kind of update only to realize you're now worse off for having installed it! *Acceptance testing* ensures that users of the system are satisfied with the solution and that it solves problems outlined in the requirements phase.

Deployment

This shortest of the SDLC phases kicks in after successful testing, and it can be manual or automated. In this phase, the software moves from development and testing into a production environment, and if you're not responsible for software maintenance, then this is the last SDLC phase for you.

Deployment includes making the software available for downloading on a web site, available in a mobile device app store, or publishing it on an internal software distribution server on a corporate network, as shown in Figure 15-4. Yet another aspect of deployment is ensuring documentation and training are available for users of the solution.

https://t.me/learningnets

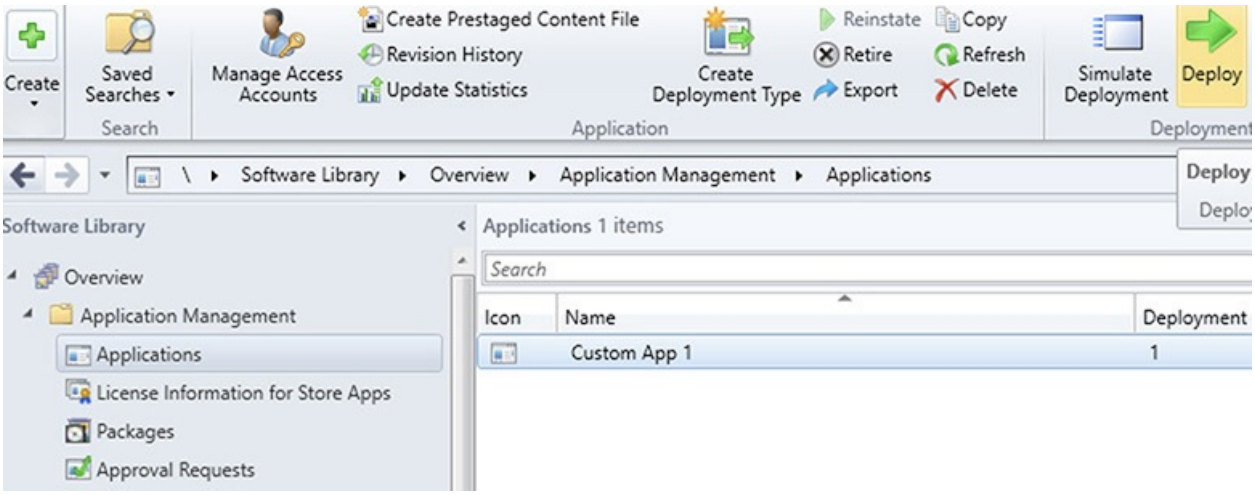


Figure 15-4 Deploying software using Microsoft System Center Configuration Manager 2016

Maintenance

If applicable, software support mechanisms and communications channels should be made known to users during the deployment phase. This not only allows product support but also provides a way for users to submit postdeployment reviews and product enhancement requests, all of which fall under the maintenance phase.

As product enhancements and bug fixes are created, they are implemented as part of software maintenance through updates posted on web sites, in app stores, or via updates pulled down to user systems such as with Windows updates downloaded to the user machine or Sony smart TV updates being pulled down to the TV.

In a corporate network environment, IT administrators can configure update servers that pull updates from the Internet and then push approved updates to managed devices on a scheduled basis, as shown in Figure 15-5. This way, on a busy network, you won't have hundreds of computers pulling down the same updates at the same time, which can cause unnecessary network congestion.

https://t.me/learningnets

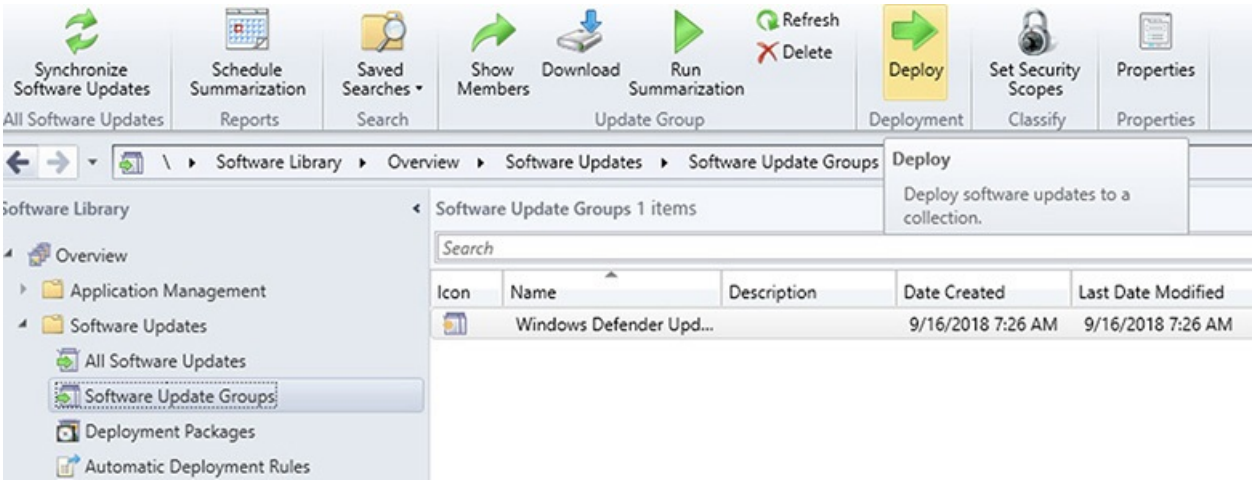


Figure 15-5 Deploying software updates using Microsoft System Center Configuration Manager 2016

Because the IT security threat landscape is constantly changing, applying security patches has become the norm. After the software solution is operational in a production environment, security best practices and documentation can be updated and relayed to users.

Maintenance also includes tracking software performance levels. Developers will often build metric-tracking features into an app that are then sent to a central server for analysis. Depending on the specific software, users may have the choice to participate or not participate in this feature.

Data Types

When coding software solutions, software developers will work with a variety of data types. Writing code that deals with customer names and addresses means working with text data (strings or characters), whereas working with all aspects of a running service is a bit more complex because the running service is an *object* with properties (more on this later).

The name of a specific data type will vary depending on the programming language you're using just as the specific syntax for typing in the code will vary. These are only details that can be easily learned; software development is really about building efficient software solutions to problems—in other words, having great ideas. Table 15-2 describes common data types.

https://t.me/learningnets

Data Type	Description	Example
Char	A single character.	The letter *g* or the number 6
String	A collection of characters.	The name Smith or a textual description such as "Golden yellow with black stripes"
Byte	A small numeric data type whose details vary between programming languages. Java has a byte data type, but C does not.	-128 to +127
Int	Integer; a whole number. Some languages support short and long integers with varying lower and upper limits. Unsigned integers are positive values, and signed integers can be either positive or negative.	-2,147,483,648 to 2,147,483,647
Float	Floating point; this data type can have decimal points.	143.95
DateTime	Stores date and time details as offset from a starting point that varies between languages. In Microsoft Excel, the date 5/5/2018 (May 5, 2018) is stored as numeric value 43,225, which is the number of days since January 1, 1900.	43225
Boolean	True or false; represented in many different ways.	1 or 0, true or false, $true or $false
Array	Container that stores items of the same type. Used often to store related items together for processing individually or through a loop. Some languages such as R use the term *vector* instead of array. Whereas in many languages the first array element starts at 0, in R it starts at 1.	• City names such as Halifax, Toronto, or Vancouver, or numbers such as 46, 67, or 981 • In Microsoft PowerShell, an array variable containing stock codes can be created as follows: $stock_codes="MSFT", "APPL", "GOOGL" • The following retrieves the first array item, which returns MSFT: $stock_codes[0]
Vector	An array type of var.	

Table 15-2 Common Software Development Data Types



EXAM TIP Make sure you know when to use specific data types for a given

https://t.me/learningnets

scenario. For example, if you need a variable to determine true or false, use Boolean as the data type.

Constants

To facilitate programming, software developers will often use custom names for unchanging values (*constants*) throughout their code if the programming or scripting language supports it.

For example, imagine you are writing code for a payroll application. Instead of referring to an hourly wage of $17.99 over and over again throughout your code, you could instead declare a constant named something like hourly_wage with a value of 17.99 at the beginning of your code. Not only does this make your code more readable, but down the road if the hourly wage changes, you have only a single update to make. Consider the following Microsoft PowerShell example, which sets a constant by creating a read-only variable:

```
Set-Variable -Name hourly_wage -Value 17.99 -Option ReadOnly
```

Variables

To facilitate programming, software developers will often use custom names for changing values (*variables*) throughout their code. This is really the only way to work with items that are unknown when coding, such as files, user accounts, services, or whatever it is your code is accessing. The alternative is to hard-code names and values into your software solution, which is generally considered a bad idea.

Imagine that you are writing a script that will list only running services on a Windows computer. If you need to use that list of running services over and over again in your code, it's much more efficient to get the list of services only once, store it in a variable, and then reuse the variable instead of continuously getting the list of services each time it's needed in your code. The following Microsoft PowerShell example stores only running services in a variable named running_svcs; note that the built-in placeholder variable $_ is also being used:

```
$running_svcs = Get-Service | Where{$_.status -eq "Running"}
```

Whenever you need to list running services, you can simply refer to the $running_svcs variable name. Then if, for example, you needed to count the number of running services, you could use the existing variable, as shown in Figure 15-6.

https://t.me/learningnets

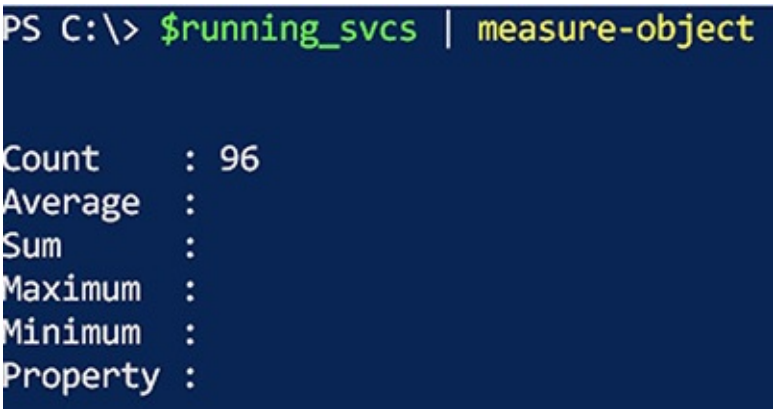


Figure 15-6 Counting the number of objects in a variable using Microsoft PowerShell

Object-Oriented Programming

The data types discussed so far are called *scalar data types,* which means they store single items or a range of items (arrays). Objects, on the other hand, are much more complex and contain many different types of data. Consider the following examples:

- **Scalar** String data type such as “Jones”
- **Object** All information related to a running Windows service, including the service name, status, dependencies, and actions (methods) such as start, stop, pause, and so on

An object can be anything, such as a Windows service, a cloud storage account, a database table, a user account, a Linux file system folder—you get the picture. What’s consistent about objects is that they consist of *properties* and *methods*.

Properties

Properties contain descriptive information, otherwise called *attributes.* As an example, a file object would have many properties, including the following:

- Name
- Path
- Hidden or not
- Read-only or not

https://t.me/learningnets

- Metadata tags such as Department or Location
- Creation date and time
- Modification date and time
- User permissions

Each property has one or more *values*. So, the name property for a file might have a value of eastern_region_budget.xlsx. When writing code, software developers separate the object from a property using a period. Consider the following Microsoft PowerShell example, which returns the values of the name and length (file size in bytes) properties, where the values are eastern_region_budget.xlsx and whatever the size of the file is. Notice the property references (name and length) follow the object reference ($file_variable) and a period:

```
$file_variable = Get-ChildItem c:\budgets\eastern_region_budget.xlsx
$file_variable.name
$file_variable.length
```

Some languages allow you to discover which properties are available for a specific object type. In Microsoft PowerShell, the following code returns properties related to file system objects where the Get-member cmdlet lists all available properties for the specific object $file_variable:

```
$file_variable | Get-Member -Type Property
```

Methods

Objects have actions that can be run against them, such as deleting a file object, creating a new user account object, or starting a Windows service object. These actions are called *methods.* Just like with properties, when writing code, software developers call methods by separating the object and method using a period.

Consider the following Microsoft PowerShell example, which calls the delete() method to remove a file:

```
$file_variable = Get-ChildItem c:\budgets\eastern_region_budget.xlsx
$file_variable.delete()
```

Some methods, such as the previously listed delete() method, do not require additional data (arguments), and you can call the method with empty parentheses. Other methods might require you to specify information within the parentheses; it just depends on the specific method being called upon.

https://t.me/learningnets

Some languages allow you to discover which properties are available for a specific object type. In Microsoft PowerShell, the following code returns methods related to file system objects:

```
$file_variable | Get-Member -Type Method
```

Program Flow

Just like in real life, within your code, sometimes decisions need to be made. Your code might validate that user input from a web application is acceptable, and if it isn't, then the code does not write the data to a database but instead returns an error message. Controlling program flow based on conditions can be achieved in numerous ways.

Conditional Execution

Most languages have some way of conditionally running code, normally through an if statement where a condition is tested. The general format of an if statement looks like this:

```
If <condition_to_test>, <code to run if true>, <code to run if false>
```

The specific syntax varies between languages; if you're using Python, it would look something like this:

```
age = raw_input("Enter age: >> ")
if age < 16:
    print "A driver's license cannot be applied for."
else :
    print "Submission has been accepted."
```

When you're testing a variable for multiple values, you could also use a select case or switch statement, such as in this C language example, which tests the value of the city variable:

https://t.me/learningnets

```
switch(city)
{
    case 'Halifax':
        printf("The country is Canada.");
        break;
    case 'Los Angeles':
        printf("The country is the United States of America.");
        break;
    case 'Munich':
        printf("The country is Germany.");
        break;
}
```

Getting Loopy

Loops execute a series of programming statements zero or more times depending on how they are coded. Sometimes you'll know how many times you need to run the same code, such as processing ten input fields on a web page; you could run validation code ten times. Other times you won't know how many times you need to run the same code, such as when processing however many files might exist in a subdirectory. Luckily, most languages provide a multitude of looping options.

Developers will often write pseudocode as they plan loops such as "Process all files in a directory; if a sensitive file is found, encrypt it." After the solution is planned via pseudocode, it can become reality using one of many possible programming languages. If a certain condition is met within a loop, the code can *branch out*, or go to, a different section of code to continue execution, as shown in the flowchart for Figure 15-7.

https://t.me/learningnets

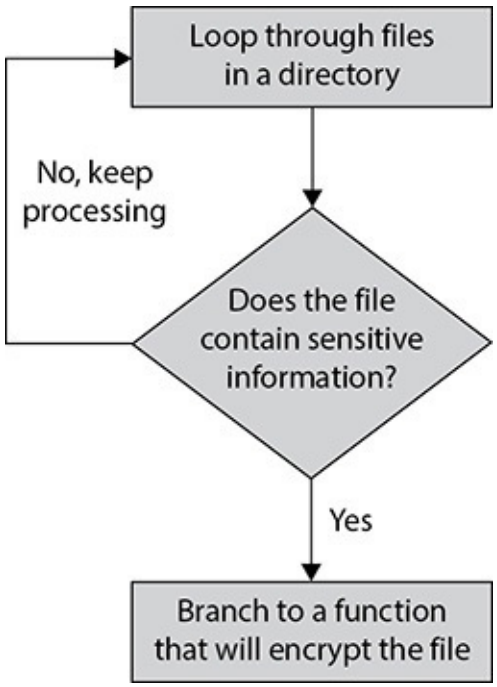


Figure 15-7 Flowchart depicting branching out of a loop when a condition is met

Loop Types

One common type of loop is a *for* loop. You can specify any type of variable or condition that determines how many times the code within the loop executes. The following Java language example uses an integer (int) variable named *x* whose value starts at 1, and while x is less than 10, it is incremented (x++) by a value of 1 each time through the loop. The code within the curly braces executes each time the loop runs. In this case, the code simple displays the value of x, but the code could do anything.

```
for(int x=1; x<10; x++)
{
              System.out.println("The value of x is: "+x);
}
```

Another common loop type is a while loop that tests a condition, and while the condition is true, the code within the loop executes. The following Microsoft PowerShell example displays a menu of options to the user until the user presses 4 (“Exit this menu”). Note that in some scripting and programming languages, “not equal to” is expressed as != or <>, but PowerShell uses –ne (not equal). The switch statement is used to test what the user entered (stored in the

https://t.me/learningnets

$user_entered_choice variable).

```
$user_entered_choice=1
while($user_entered_choice -ne 4)
{
    write-host "Utilities Menu"
    write-host "----------------------"
    write-host
    write-host "1 - List Active Directory user accounts"
    write-host "2 - List Active Directory computer accounts"
    write-host "3—View system log errors from all servers"
    write-host "4 - Exit this menu"
    write-host
    $user_entered_choice=read-host "Enter choice"
    switch($user_entered_choice)
    {
        1{write-host;stale_users;read-host}
        2{list_adcomputers;read-host}
        3{list_dcs_errors;read-host}
        4{cls;break}
    }
    cls
}
```

Functions

Over time software developers end up writing the same chunks of code multiple times. This is where functions come in. A *function* uses a name to refer to a chunk of code, and it lends itself nicely to code reusability. Suppose you create a function called create_user_account, which adds a user account to a server. You can simply call the function by name (create_user_account) to execute the code within the function definition. Most functions return a value, whether it is an object referring to a newly created user account or simply a status code such as a value of 1 to indicate success.

Just like methods, some functions accept arguments, and some do not. The following is an example of using the C programming language to declare a function called *largest*, which accepts two integer (int) values, x and y, and returns the largest number of the two. Note on the first line that the function definition begins with *int,* which means the return data type of the function is an integer.

https://t.me/learningnets

```
int largest(int x, int y)
{
    if (x > y)
      return x;
    else
      return y;
} `
```

After functions are defined as in the previous example, they must be called upon in order to be executed, as in the following example that sets two integer variables (firstnumber and secondnumber) that are passed as arguments to the largest function:

```
int firstnumber = 5, secondnumber = 6;
int returnvaluevariable = largest(firstnumber, secondnumber);
```

Chapter Review

This chapter provided insight into what is involved in software design and implementation, whether a simple script or a larger complex solution.

The software development life cycle is a structured approach to building software solutions. The SDLC consists of six steps:

1. Requirement analysis and planning
2. Design
3. Coding
4. Testing
5. Deployment
6. Maintenance

Microservices are code modules that together form a larger application. A microservice architecture allows module management and execution independently of other modules; it also allows for code reusability.

Scripting languages such as Linux bash and Microsoft PowerShell are interpreted by a runtime environment that understands the script commands. Compiled languages such as C use a compiler program to render the source code to machine language. Assembly language is already machine code and does not need to be compiled.

During the SDLC design phase, software developers will often plan the code

https://t.me/learningnets

first using pseudocode, which is human readable and can later be converted to actual syntax for the chosen scripting or programming language. During the SDLC testing phase, unit testing is run against modules of code, and regression testing ensures that code changes have not negatively affected other code that worked well previously.

Common data types used in coding include the following:

- Char
- String
- Byte
- Int
- Float
- DateTime
- Boolean
- Array
- Vector

These scalar, or simple, data types can be used with unchanging values (constants) or changing values (variables) within code. Objects are complex programming entities that contain properties and methods. *Properties* are descriptive attributes, such as the name of a Windows service or its status, whereas *methods* are actions, such as deleting a file or stopping a Windows service.

Controlling the code sequence and branching to pieces of code is achieved with condition statements, loops, and functions. The if, select case, and switch statements test a condition to determine what code should executed when the condition is true or false. Loops repeatedly execute code segments based on a specific number of times (for loop) or until a condition is reached (while loop).

Functions are smaller reusable chunks of code that can return a value. Some functions accept arguments, while others do not. After being defined, functions must be called upon for the code within the function to execute.

Questions

1. Which of the following programming languages requires a compiler?
   A. Assembly

https://t.me/learningnets

B. Linux bash

C. Microsoft PowerShell

D. C

2. Which SDLC phase involves the use of flowcharts?

A. Deployment

B. Maintenance

C. Coding

D. Design

3. You are creating a function that must return either true or false. Which data type should the function return?

A. Boolean

B. Integer

C. Character

D. String

4. Which term describes running an action against an object variable?

A. Property

B. Method

C. Debugging

D. Boolean

5. You are working with file system objects in your code. You need to determine the modification timestamp for a file. What should you reference?

A. Property

B. Method

C. Constant

D. Variable

6. You are using the C programming language to create a software solution. A single variable must be tested for multiple possible values. Which programming construct should you use to achieve this?

A. If

B. Select case

C. While

https://t.me/learningnets

D. Switch

7. Your code needs to execute the same code for each month of the year, so 12 times. Which type of loop is best suited for this?
   A. Switch
   B. If
   C. For
   D. Assembly
8. Which of the SDLC phases is the shortest in duration?
   A. Coding
   B. Design
   C. Deployment
   D. Requirement analysis and planning
9. Which SDLC phase is the longest in duration?
   A. Coding
   B. Design
   C. Deployment
   D. Requirement analysis and planning
10. Which type of coding practice uses smaller code modules working together to support an application?
    A. Monolithic
    B. Interpreted
    C. Microservices
    D. Compiled

Answers

1. **D**. Before the code can be executed, the C programming language requires a compiler.
2. **D**. The SDLC design phase uses flowcharts to design program flow.
3. **A.** The Boolean data type is used for true or false values.
4. **B**. Methods are actions run against objects, such as start, stop, delete, connect, and so on.

https://t.me/learningnets

5. **A**. Properties are descriptive attributes such as modification timestamps, names, and so on.
6. **D**. In the C programming language, the switch statement is best suited for testing a single variable for multiple values.
7. **C**. When you know how many times a loop should execute, use a for loop.
8. **C**. The deployment phase is the shortest of SDLC phases.
9. **A**. The coding phase is the longest of SDLC phases.
10. **C**. Microservices are independent code modules that together form a larger application.

https://t.me/learningnets

PART V

Appendixes

- **Appendix A** Exam Objective Reference
- **Appendix B** About the Online Content

https://t.me/learningnets

APPENDIX A

Exam Objective Reference

CompTIA IT Fundamentals+

The commercial version of the CompTIA IT Fundamentals+ exam is designed to show that the successful candidate has the knowledge to discuss basic computer components and put together a personal computer (PC). The candidate can install software for productivity, connect the computer to a network, and explain basic security. The candidate can communicate essentials of safety and maintenance. This test is intended for candidates who want to understand modern technology to function well in our increasingly digital world and for those considering becoming a tech.



NOTE The lists under each objective are not exhaustive. Even though they are not included in this document, other examples of technologies, processes, or tasks pertaining to each objective may also be included on the exam.

https://t.me/learningnets

Domain	Percent of Examination
1.0 IT Concepts and Terminology	17%
2.0 Infrastructure	22%
3.0 Applications and Software	18%
4.0 Software Development	12%
5.0 Database Fundamentals	11%
6.0 Security	20%
Total	100%

Topic	Chapter No.	Page No.
1.0 IT Concepts and Terminology		
1.1 Compare and contrast notational systems.		
Binary	4	89
Hexadecimal	2	42
Decimal	2	42

https://t.me/learningnets

ASCII	Glossary	
Unicode	Glossary	
1.2 Compare and contrast fundamental data types and their characteristics.		
Char	15	377
String	15	377
Integer	15	377
Float	15	377
Boolean	15	377
1.3 Illustrate the basics of computing and processing.		
Input	1	18
Output	1	18
Processing	1	8
Storage	1	8
1.4 Explain the value of data and information.		
Data and information as assets	1	8
Importance of investing in security	11	279
Relationship of data to creating information	1	8
Trademarks	Glossary	
Copyrights	1	8
Patents	1	8
Data capture and collection	11	307
Data correlation	Glossary	
Meaningful reporting	14	361
1.5 Compare and contrast common units of measure.		
Bit	4	89
Byte	4	89
KB	4	89
MB	4	90
GB	4	90
TB	4	90
PB	4	90
bps	4	89
Kbps	4	89
Mbps	4	89

https://t.me/learningnets

Gbps	4	89
Tbps	4	89
MHz	4	89
GHz	4	89
1.6 Explain the troubleshooting methodology.		
Identify the problem	13	336
Research knowledge base/Internet, if applicable	13	336
Establish a theory of probable cause	13	336
Test the theory to determine the cause	13	336
Establish a plan of action to resolve the problem and identify potential effects	13	336
Implement the solution or escalate as necessary	13	336
Verify full system functionality and, if applicable, implement preventive measures	13	336
Document findings/lessons learned, actions and outcomes	13	336
2.0 Infrastructure		
2.1 Classify common types of input/output device interfaces.		
Telephone connector (RJ-11)	3	61
Ethernet connector (RJ-45)	3	61
Bluetooth	3	78
NFC	11	281
USB	4	96
Thunderbolt	4	96
RF	3	75
VGA	3	71
DVI	3	70
HDMI	3	70
DisplayPort	3	73
Mini-DisplayPort	3	64
2.2 Given a scenario, set up and install common peripheral devices to a laptop/PC.		
Printer	3	81
Scanner	3	79
Keyboard	3	76
Mouse	3	76

https://t.me/learningnets

Camera	3	80
External hard drive	3	65
Speakers	3	78
Display	3	66
Plug-and-play vs. driver installation	5	128
Other required steps	5	128
IP-based peripherals	6	147
Web-based configuration steps	6	147
2.3 Explain the purpose of common internal computing components.		
Motherboard/system board	2	40
Firmware/BIOS	2	51
RAM	2	47
CPU – ARM	2	40
CPU – Mobile Phone	2	40
CPU - Tablet	2	40
CPU - 32-bit, 64-bit	2	42
CPU – Laptop, workstation, server	2	40
CPU – Cooling	2	44
NIC - wired	3	61
NIC - wireless	3	61
NIC - onboard	3	61
NIC - add-on card	3	61
2.4 Compare and contrast common Internet service types.		
Fiber optic	10	261
Cable	10	261
DSL	10	261
Wireless - radio frequency	10	274
Wireless - satellite	10	274
Wireless - Cellular	10	274
2.5 Compare and contrast storage types.		
Volatile vs. non-volatile	14	355
RAM	2	47
HDD	4	90
SSD	4	93

https://t.me/learningnets

Optical	4	92
Flash drive	4	93
NAS	4	97
File server	4	97
Cloud storage	4	99
2.6 Compare and contrast common computing devices and their purposes.		
Mobile phone	7	154
Tablet	7	154
Laptop	1	11
Workstation	1	11
Server	1	26
Gaming console	1	25
IoT – Home appliances	1	7
IoT – Home automation devices	1	7
IoT – Modern cars, IP cameras, Streaming media devices, Medical devices	1	7
2.7 Explain basic networking concepts.		
Basic of packet transmission	11	300
DNS	11	301
LAN vs. WAN	10	244
IP address	10	250
MAC address	Glossary	
HTTP/S	11	303
POP3	7	171
IMAP	7	171
SMTP	7	171
Modem	3	61
Router	10	250
Switch	10	248
Access point	10	260
Firewall	11	312
2.8 Given a scenario, install, configure a secure a basic wireless network.		
802.11a/b/g/n/ac	10	249
Change SSID	10	255
Change default password	10	253

https://t.me/learningnets

Captive portal	Glossary	
WEP	10	255
WPA/WPA2	10	256
3.0 Applications and Software		
3.1 Manage applications and software		
Interface between applications and hardware	5	127
Disk management	14	354
Process management/scheduling	13	340
Application management	9	219
Memory management	2	47
Device management	5	128
Access control/protection	9	212
Type of OS	5	107
3.2 Compare and contrast components of an operating system.		
NTFS	8	187
FAT32	Glossary	
EXT4	8	187
HFS	8	187
Compression	8	188
Encryption	8	188
Permissions	8	200
Journaling	8	188
Naming rules	8	182
File management	8	183
Services	5	126
Processes	13	340
Task scheduling utilities	5	125
CLI	5	107
GUI	5	107
3.3 Explain the purpose and proper use of software.		
Productivity software	9	225
Collaboration software	9	226
Business software	9	227

https://t.me/learningnets

3.4 Explain methods of application architecture and delivery models.		
Locally installed	9	234
Local network hosted	9	215
Cloud hosted	9	215
Application architecture models	9	207
3.5 Given a scenario, configure and use web browsers.		
Caching/clearing cache	11	309
Deactivate client-side scripting	11	308
Browser add-ons/extensions	11	312
Private browsing	11	302
Proxy settings	Glossary	
Certificates	11	304
Popup blockers	11	310
Script blockers	11	308
Compatible browser for application(s)	9	225
3.6 Compare and contrast general application concepts and uses.		
Single-platform software	9	224
Cross-platform software	9	224
Licensing	9	234
Software installation best practices	9	215
4.0 Software Development Concepts		
4.1 Compare and contrast programming language categories.		
Interpreted	15	372
Compiled programming languages	15	372
Query languages	15	372
Assembly language	15	372
4.2 Given a scenario, use programming organizational techniques and interpret logic.		
Pseudocode concepts	15	373
Flowchart concepts	15	369
Branching	15	381
Looping	15	381
4.3 Explain the purpose and use of programming concepts.		
Variables, constants	15	377, 378
Arrays, vectors	15	377

https://t.me/learningnets

Functions	15	382
Objects	15	383
5.0 Database Fundamentals		
5.1 Explain database concepts and the purpose of a database.		
Usage of database	14	351
Flat file vs. database	14	351
Records	14	351
Data persistence	14	355
5.2 Compare and contrast various database structures		
Structured vs. semi-structured	14	355
Schema	14	355
Tables	14	351
Non-relational databases	14	356
5.3 Summarize methods used to interface with databases.		
Data manipulation	14	358
Data definition	14	355
Database access methods	14	359
Export/import	14	360
6.0 Security		
6.1 Summarize confidentiality, integrity, and availability concerns.		
Snooping, eavesdropping, wiretapping	11	303, 300
Social engineering	11	293
Dumpster diving	11	278
Man-in-the-middle, replay attack, impersonation	11	301
Availability concerns	10	261
6.2 Explain methods to secure devices and best practices.		
Antivirus/antimalware	11	298
Host firewall	11	312
Secure passwords	11	286
Safe browsing practices	11	303
Patching/updates	11	308
Software sources	11	304
Removal of unwanted/unecessary/malicous software	11	291

https://t.me/learningnets

6.3 Summarize behavioral security concepts.		
Internet privacy	11	302
Mobile application privacy	11	303
Desktop/business software	11	280
Corporate network	11	301
Written policies and procedures	11	285
Handling of confidential information	11	307
6.4 Compare and contrast authentication, authorization, accounting, and non-repudiation concepts.		
Single factor authentication	11	284
Multi factor authentication	11	284
Authentication factors	11	284
Single sign-on	11	286
Authorization	11	278
Non-repudiation	11	283
6.5 Explain password best practices.		
Password length	11	285
Password complexity	11	285
Password history	11	286
Password expiration	11	286
Password reuse across sites	11	286
Password managers	11	285
Password reset process	11	285
6.6 Explain common uses of encryption.		
Plain text vs. cipher text	11	283
Data at rest	11	282
Data in transit	11	283
6.7 Explain business continuity concepts.		
Replication	8	202
Redundancy	8	202
Backup considerations	8	202
Data location	8	203
Contingency plan	12	331
Disaster recovery	12	331

https://t.me/learningnets

APPENDIX B

About the Online Content

This book comes complete with:

- TotalTester Online customizable practice exam software with more than 130 practice exam questions
- More than an hour of video training episodes from Mike Meyers' CompTIA IT Fundamentals+ Certification series

System Requirements

The current and previous major versions of the following desktop Web browsers are recommended and supported: Chrome, Edge, Firefox, and Safari. These browsers update frequently and sometimes an update may cause compatibility issues with the TotalTester Online or other content hosted on the Training Hub. If you run into a problem using one of these browsers, please try using a different Web browser until the problem is resolved.

Your Total Seminars Training Hub Account

In order to get access to the online content, you will need to create an account on the Total Seminars Training Hub. Registration is free and you will be able to track all your online content using your account.

Single User License Terms and Conditions

Online access to the digital content included with this book is governed by the McGraw-Hill Education License Agreement outlined next. By using this digital content you agree to the terms of that license.

Access To register and activate your Total Seminars Training Hub account, simply follow these easy steps.

https://t.me/learningnets

1. Go to **hub.totalsem.com/mheclaim**.
2. To register and create a new Training Hub account, enter your email address, name, and password. No further information (such as credit card number) is required to create an account.



NOTE If you already have a Total Seminars Training Hub account, select **Log in** and enter your email and password.

3. Enter your Product Key: **`c0n7-c0g2-2w0w`**.
4. Click to accept the user license terms.
5. Select or deselect the Send special offers option.
6. Click **Register and Claim** to create your account. You will be taken to the Training Hub and have access to the content for this book.

Duration of License Access to your online content through the Total Seminars Training Hub will expire one year from the date the publisher declares the book out of print.

Your purchase of this McGraw-Hill Education product, including its access code, through a retail store is subject to the refund policy of that store.

The Content is a copyrighted work of McGraw-Hill Education and McGraw-Hill Education reserves all rights in and to the Content. The Work is © 2019 by McGraw-Hill Education, LLC.

Restrictions on Transfer The user is receiving only a limited right to use the Content for user's own internal and personal use, dependent on purchase and continued ownership of this book. The user may not reproduce, forward, modify, create derivative works based upon, transmit, distribute, disseminate, sell, publish, or sublicense the Content or in any way commingle the Content with other third-party content, without McGraw-Hill Education's consent.

Limited Warranty The McGraw-Hill Education Content is provided on an "as is" basis. Neither McGraw-Hill Education nor its licensors make any guarantees or warranties of any kind, either express or implied, including, but not limited to, implied warranties of merchantability or fitness for a particular purpose or use as to any McGraw-Hill Education Content or the information therein or any

https://t.me/learningnets

warranties as to the accuracy, completeness, correctness, or results to be obtained from, accessing or using the McGraw-Hill Education content, or any material referenced in such content or any information entered into licensee's product by users or other persons and/or any material available on or that can be accessed through the licensee's product (including via any hyperlink or otherwise) or as to non-infringement of third-party rights. Any warranties of any kind, whether express or implied, are disclaimed. Any material or data obtained through use of the McGraw-Hill Education content is at your own discretion and risk and user understands that it will be solely responsible for any resulting damage to its computer system or loss of data.

Neither McGraw-Hill Education nor its licensors shall be liable to any subscriber or to any user or anyone else for any inaccuracy, delay, interruption in service, error or omission, regardless of cause, or for any damage resulting therefrom.

In no event will McGraw-Hill Education or its licensors be liable for any indirect, special or consequential damages, including but not limited to, lost time, lost money, lost profits or good will, whether in contract, tort, strict liability or otherwise, and whether or not such damages are foreseen or unforeseen with respect to any use of the McGraw-Hill Education content.

TotalTester Online

TotalTester Online provides you with a simulation of the CompTIA IT Fundamentals+ exam. Exams can be taken in Practice Mode or Exam Mode. Practice Mode provides an assistance window with hints, references to the book, explanations of the correct and incorrect answers, and the option to check your answer as you take the test. Exam Mode provides a simulation of the actual exam. The number of questions, the types of questions, and the time allowed are intended to be an accurate representation of the exam environment. The option to customize your quiz allows you to create custom exams from selected domains or chapters, and you can further customize the number of questions and time allowed.

To take a test, follow the instructions provided in the previous section to register and activate your Total Seminars Training Hub account. When you register you will be taken to the Total Seminars Training Hub. From the Training Hub Home page, select IT Fundamentals+ FC0-U61 from the list of "Your Topics" on the Home page. Click the TotalTester tab. You can then select the option to customize your quiz and begin testing yourself in Practice Mode or Exam Mode. All exams provide an overall grade and a grade broken down by

https://t.me/learningnets

domain.

Mike’s Video Training

The training videos, starring Mike Meyers, are available for free for the first four chapters of the book. Select IT Fundamentals+ FC0-U61 from the list of “Your Topics” on the Home page. Click the TotalVideos tab. Along with access to the videos from the first four chapters of the book, you’ll find an option to purchase Mike’s complete video training series.

Technical Support

For questions regarding the Total Tester software or operation of the Training Hub, visit **www.totalsem.com** or e-mail **support@totalsem.com**.

For questions regarding book content, e-mail **hep_customer-service@mheducation.com**. For customers outside the United States, e-mail **international_cs@mheducation.com**.

https://t.me/learningnets

GLOSSARY

3-D graphics Video technology that attempts to create images with the same depth and texture as objects seen in the real world.

4G Most popularly implemented as Long Term Evolution (LTE), a wireless data standard with theoretical download speeds of 300 Mbps and upload speeds of 75 Mbps.

7.1 speaker system Speaker setup consisting of six satellite speakers (two front, two side, two rear) plus a center speaker and a subwoofer.

64-bit processing A type of processing that can run a compatible 64-bit operating system, such as Windows 7, 8, 8.1, or 10, and 64-bit applications. 64-bit PCs have a 64-bit-wide address bus, enabling them to use more than 4 GB of RAM.

8.3 naming system Filenaming convention that specified a maximum of eight characters for a filename, followed by a three-character file extension. Has been replaced by LFN (long filename) support.

80-wire ribbon cable PATA cable used to attach fast EIDE devices (such as ATA/100 hard drives) or ATAPI devices (such as optical drives) to a system. (*See also* parallel ATA [PATA].)

802.11a Wireless networking standard that operates in the 5 GHz band with a theoretical maximum throughput of 54 Mbps.

802.11ac Wireless networking standard that operates in the 5 GHz band and uses multiple in/multiple out (MIMO) and multi-user MIMO (MU-MIMO) to achieve a theoretical maximum throughput of 1 Gbps.

802.11b Wireless networking standard that operates in the 2.4 GHz band with a theoretical maximum throughput of 11 Mbps.

https://t.me/learningnets

802.11g Wireless networking standard that operates in the 2.4 GHz band with a theoretical maximum throughput of 54 Mbps and is backward compatible with 802.11b.

802.11n Wireless networking standard that can operate in both the 2.4 GHz and 5 GHz bands and uses multiple in/multiple out (MIMO) to achieve a theoretical maximum throughput of 100+ Mbps.

AC (alternating current) Type of electricity in which the flow of electrons alternates direction, back and forth, in a circuit.

accelerometer Feature in smartphones and tablets that rotates the screen when the device is physically rotated.

acceptance testing Ensuring that the users of an IT solution are satisfied with the solution functionality.

access control Security concept using physical security, authentication, users and groups, and security policies.

access control list (ACL) A clearly defined list of permissions that specifies what actions an authenticated user may perform on a shared resource.

Action Center A one-page aggregation of event messages, warnings, and maintenance messages in the Windows operating system.

activation Process of confirming that an installed copy of a Microsoft product (most commonly Windows or a Microsoft Office application) is legitimate. Usually done at the end of software installation.

active cooling System designed to remove heat from a processor by using some electrically powered mechanical parts, such as a fan.

ad hoc mode Decentralized wireless network mode, otherwise known as *peer-to-peer mode*, where each wireless node is in meshed contact with every other node.

Add or Remove Programs Applet allowing users to add or remove a program manually to or from a Windows system.

https://t.me/learningnets

add-on A small program used within a web browser to add functionality, such as reading PDF files; also called a browser *extension* or *plug-in*.

Administrative Tools Group of Control Panel applets, including Computer Management, Event Viewer, and Reliability and Performance Monitor.

administrator account User account, created when the OS is first installed, that is allowed complete, unfettered access to the system without restriction.

Administrators group List of members with complete administrator privileges.

ADSL (asymmetric digital subscriber line) Fully digital, dedicated connection to the telephone system that provides average download speeds of 3 Mbps to 15 Mbps and upload speeds of 384 Kbps to 15 Mbps. *Asymmetric* identifies that upload and download speeds are different, with download usually being significantly faster than upload.

Advanced Encryption Standard (AES) A block cipher created in the late 1990s that uses a 128-bit block size and a 128-, 192-, or 256-bit key size. Practically uncrackable.

Advanced Startup Options menu Menu that can be reached during the boot process that offers advanced OS startup options, such as to boot to Safe Mode or boot into Last Known Good Configuration.

adware Type of malicious program that downloads ads to a user's computer, generating undesirable network traffic.

Aero The Windows Vista/7 desktop environment. Aero adds some interesting aesthetic effects such as window transparency and Flip 3D.

airplane mode Mode for mobile devices that disables all wireless and cellular communication for use on airplanes.

algorithm Set of rules for solving a problem in a given number of steps.

AMD (Advanced Micro Devices) CPU and chipset manufacturer that competes with Intel. It produces FX, A-Series, Phenom II, Athlon, Sempron, and Opteron CPUs and APUs. It also produces video card processors under its ATI

https://t.me/learningnets

brand.

amperes (amps or A) Unit of measure for amperage, or electrical current.

analog Device that uses a physical quantity, such as length or voltage, to represent the value of a number. By contrast, digital storage relies on a coding system of numeric units.

Android Smartphone and tablet OS created by Google.

Android application package (APK) Installation software for Android apps.

antistatic bag Bag made of antistatic plastic into which electronics are placed for temporary or long-term storage. It is used to protect components from electrostatic discharge.

antistatic mat Special surface on which to lay electronics. These mats come with a grounding connection designed to equalize electrical potential between a workbench and one or more electronic devices. It is used to prevent electrostatic discharge.

antistatic wrist strap Special device worn around the wrist with a grounding connection designed to equalize electrical potential between a technician and an electronic device. It is used to prevent electrostatic discharge.

antivirus program Software designed to combat viruses by either seeking out and destroying them or passively guarding against them.

API (application programming interface) Software definition that describes operating system calls for application software; conventions defining how a service is invoked.

app A program for a tablet or smartphone; also, a program written for the Windows Modern interface.

App Store Apple’s mobile software storefront, where you can purchase apps for your smartphone, tablet, or other Apple products.

applet Generic term for a program in the Windows Control Panel.

https://t.me/learningnets

Applications Name of the tab in Task Manager that lists running applications.

apt-get Linux command for installing or updating a program using the advanced packaging tool.

archive To copy programs and data onto a relatively inexpensive storage medium (drive, tape, etc.) for long-term retention.

archive attribute Attribute of a file that shows whether the file has been backed up since the last change. Each time a file is opened, changed, or saved, the archive bit is turned on. Some types of backups turn off this archive bit to indicate that a good backup of the file exists on tape.

ARM Energy-efficient processor design frequently used in mobile devices.

ARP (Address Resolution Protocol) Protocol in the TCP/IP suite used with the command-line utility of the same name (arp) to determine the MAC address that corresponds to a particular IP address.

array Computer programming data type used to store multiple items of the same type, such as an array of integers values.

ASCII (American Standard Code for Information Interchange) Industry-standard 8-bit characters used to define text characters, consisting of 96 upper- and lowercase letters, plus 32 nonprinting control characters, each of which is numbered. These numbers were designed to achieve uniformity among computer devices for printing and the exchange of simple text documents.

aspect ratio Ratio of width to height of an object. Standard television has a 4:3 aspect ratio. High-definition television is 16:9. Desktop computer monitors tend to be either 16:9 or 16:10.

assembly language A low-level computer programming language that talks directly to hardware instruction sets.

ATA (AT Attachment) Type of hard drive and controller designed to replace the earlier ST506 and ESDI drives without requiring replacement of the AT BIOS—hence, AT attachment. These drives are more popularly known as IDE drives. (*See also* integrated drive electronics [IDE].) The ATA/33 standard has drive transfer speeds up to 33 MBps; the ATA/66 up to 66 MBps; the ATA/100

https://t.me/learningnets

up to 100 MBps; and the ATA/133 up to 133 MBps. (*See also* Ultra DMA.)

ATM An automated teller machine; a variation of a point-of-service terminal, designed for banking transactions.

ATM (Asynchronous Transfer Mode) A network technology that runs at speeds between 25 and 622 Mbps using fiber-optic cabling or CAT 5 or better UTP.

attack surface A term that references the potential for security breaches; for example, a patched server reduces the attack surface.

attenuation Signal degradation over distance.

attributes Values in a file that determine the hidden, read-only, system, and archive status of the file.

ATX (Advanced Technology Extended) Popular motherboard form factor that generally replaced the AT form factor.

audio interface High-end external sound device used by audio engineers and recording artists.

authentication Any method a computer uses to determine who or what can access it.

authorization Any method a computer uses to determine what an authenticated user can do.

Automatic Updates Feature allowing updates to Windows to be retrieved automatically over the Internet.

availability Ensuring that IT systems or data are accessible.

backlight One of three main components used in LCDs to illuminate an image.

backplate A piece of metal that fits into an opening in the back of a desktop PC so you can access the expansion card's port (or ports).

Backup or Restore Wizard Older Windows utility that enables users to create

https://t.me/learningnets

system backups and set system restore points.

bandwidth Piece of the spectrum occupied by some form of signal, such as television, voice, or fax data. Signals require a certain size and location of bandwidth to be transmitted. The higher the bandwidth, the faster the signal transmission, allowing for a more complex signal such as audio or video. Because bandwidth is a limited space, when one user is occupying it, others must wait their turn. Bandwidth is also the capacity of a network to transmit a given amount of data during a given period.

BD-R (Blu-ray Disc-Recordable) Blu-ray Disc format that enables writing data to blank discs. (*See also* Blu-ray Disc [BD].)

BD-RE (Blu-ray Disc-Rewritable) Blu-ray Disc equivalent of the rewritable DVD, allows writing and rewriting several times on the same BD. (*See also* Blu-ray Disc [BD].)

BD-ROM (Blu-ray Disc-Read Only Media) Blu-ray Disc equivalent of a DVD-ROM or CD-ROM. (*See also* Blu-ray Disc [BD].)

binary numbers Number system with a base of 2, unlike the number systems most of us use that have bases of 10 (decimal numbers), 12 (measurement in feet and inches), and 60 (time). Binary numbers are preferred for computers for precision and economy. An electronic circuit that can detect the difference between two states (on–off, 0–1) is easier and more inexpensive to build than one that could detect the differences among ten states (0–9).

biometric device Hardware device used to support authentication; works by scanning and remembering a unique aspect of a user's various body parts (e.g., retina, iris, face, or fingerprint) by using some form of sensing device such as a retinal scanner.

BIOS (basic input/output services or basic input/output system) Classically, software routines burned onto the system ROM of a PC. More commonly, this is seen as any software that directly controls a particular piece of hardware. It is a set of programs encoded in read-only memory (ROM) on computers. These programs handle startup operations and low-level control of hardware such as disk drives, the keyboard, and the monitor.

bit Single binary digit; also, any device that can be in an on or off state.

https://t.me/learningnets

bit depth Number of colors a video card is capable of producing. Common bit depths are 16-bit and 32-bit, representing 65,536 colors and 16.7 million colors (plus an 8-bit alpha channel for transparency levels), respectively.

BitLocker Drive Encryption Drive encryption software offered in high-end versions of Windows. BitLocker requires a special chip to validate hardware status and to ensure that the computer hasn't been hacked.

bloatware Additional software that a user does not want; normally packaged with other software that a user does want.

Bluetooth Wireless technology designed to create small wireless networks preconfigured to do specific jobs but not meant to replace full-function networks or Wi-Fi.

Blu-ray Disc (BD) Optical disc format that stores 25 or 50 GB of data, designed to be the replacement media for DVD. This competed with HD DVD and won.

Boolean Computer programming data type used for true or false testing.

boot To initiate an automatic routine that clears the memory, loads the operating system, and prepares the computer for use. The term is derived from "pull yourself up by your bootstraps." PCs must do that because RAM doesn't retain program instructions when power is turned off. A cold boot occurs when the PC is physically switched on. A warm boot loads a fresh OS without turning off the computer, lessening the strain on the electronic circuitry. To do a warm boot, press the ctrl-alt-delete keys twice in rapid succession (the three-fingered salute).

Boot Camp Apple tool used to install and boot to versions of Windows on a macOS computer.

boot sector First sector on a PC hard drive, track 0. This is the bootup software in ROM tells the computer to load whatever program is found there. If a system disk is read, the program in the boot record directs the computer to the root directory to load the operating system.

boot sequence List containing information telling the bootstrap loader in which order to check the available storage devices for an OS. This is configurable in

https://t.me/learningnets

CMOS setup.

bootable disk Disk that contains a functional operating system; can also be a USB thumb drive or optical disc.

bps (bits per second) Measurement of how fast data is moved from one place to another. A 56K modem can move ~56,000 bits per second.

bridge A device that connects two networks and passes traffic between them based only on the node address so that traffic between nodes on one network does not appear on the other network. For example, an Ethernet bridge looks only at the MAC address. Bridges filter and forward packets based on MAC addresses and operate at level 2 (Data Link layer) of the OSI seven-layer model.

broadband Commonly understood as a reference to high-speed, always-on communication links that can move large files much more quickly than a regular network connection.

broadcast A network transmission addressed for every node on the network.

browser Program specifically designed to retrieve, interpret, and display web pages.

bug Programming error that causes a program or a computer system to perform erratically, produce incorrect results, or crash. The term was coined when a real bug was found in one of the circuits of one of the first ENIAC computers.

burn Process of writing data to a writable optical disc, such as a DVD-R.

bus Series of wires connecting two or more separate electronic devices, enabling those devices to communicate at a given rate (bus speed). Also, a network topology where computers all connect to a main line called a *bus cable*.

bus topology Network configuration wherein all computers connect to the network via a central bus cable.

BYOD (bring your own device) An arrangement in some companies' IT departments where employees are permitted to use their own phones or other mobile devices instead of company-issued ones. Also, a feature of some wireless carriers where you can buy an unsubsidized device and use it to get cheaper

https://t.me/learningnets

wireless rates.

byte Unit of 8 bits; fundamental data unit of personal computers. Storing the equivalent of one character, the byte is also the basic unit of measurement for computer storage. In computer programming, it is a small numeric data type.

cache (disk) Special area of RAM that stores the data most frequently accessed from the hard drive. Cache memory can optimize the use of your systems.

cache (L1, L2, L3, etc.) Special section of fast memory, usually built into the CPU, used by the onboard logic to store information most frequently accessed by the CPU.

calibration Process of matching the print output of a printer to the visual output of a monitor. Alternatively, this is a method used to define the active or touchable area of a touchscreen monitor or phone; it's primarily found on older, resistive touchscreen devices.

capacitive touchscreen Type of touchscreen that uses electrical current in your body to determine movement of your fingers across the screen.

CAPTCHA (Completely Automated Public Turing Test to tell Computers and Humans Apart) Authentication challenge using images, videos, sounds, or other media to be identified by a user. Computers have a much more difficult time discerning the content of these tests than humans, making the challenge useful in determining whether a human or a computer is attempting access.

Captive Portal Web page used to authenticate a user before providing network access.

card reader Device with which you can read data from one of several types of flash memory.

Cascading Style Sheet CSS; a web design document that centrally controls web page formatting.

case fan This is used to cool off the interior of the computer,

cathode ray tube (CRT) Uses electron guns to activate phosphors behind the screen, causing each pixel on the monitor to generate red, green, or blue.

https://t.me/learningnets

cd (chdir) Shorthand for “change directory.” The command enables you to change the focus of the command prompt from one directory to another.

CD (compact disc) Originally designed as the replacement for vinyl records; has become the primary method of long-term storage of music and data.

CD quality Audio quality that has a sample rate of 44.4 KHz and a bit rate of 128 bits.

CD-R (CD-recordable) CD technology that accepts a single “burn” but cannot be erased after that one burn.

CD-ROM (compact disc/read-only memory) Read-only compact storage disc for audio or video data. CD-ROMs are read by using CD-ROM drives and optical drives with backward compatibility, such as DVD and Blu-ray Disc drives.

CD-RW (CD-rewritable) CD technology that accepts multiple reads/writes like a hard drive.

cellular wireless networks Networks that enable cell phones, smartphones, and other mobile devices to connect to the Internet.

CGI Computer-generated imagery (CGI) effects for movies.

char A computer programming data type consisting of a single character.

charms In Windows 8 and 8.1, tools located in the hidden Charms bar, such as a search function, a sharing tool, a settings tool, and more.

Charms bar The location in Windows 8 and 8.1 of the charms tools. Accessed by moving the cursor to the upper-right corner of the screen.

chattr Linux command that can be used to encrypt files.

chipset One or more programmed chips working together to serve a functions, such as a video chipset.

Chrome OS A Linux variant operating system designed by Google for thin client systems for Internet usage.

https://t.me/learningnets

CIFS (Common Internet File System) The protocol that NetBIOS used to share folders and printers. It is still common, even on UNIX/Linux systems.

cipher text Scrambled data resulting from feeding plain text through an encryption cipher along with an encryption key.

clean installation Installing an operating system on a fresh drive, following a reformat of that drive. Often it's the only way to correct a problem with a system when many of the crucial operating system files have become corrupted.

client Computer program that uses the services of another computer program. It is also software that extracts information from a server; your auto-dial phone is a client, and the phone company is its server. It is also a machine that accesses shared resources on a server.

client-server Relationship in which client software obtains services from a server on behalf of a person.

client-server network Network that has dedicated server machines and client machines.

closed source Software that is solely controlled by its creator or distributor.

cloud computing A model for enabling and accessing computing storage and other shared (or not shared) resources on-demand. The "cloud" is based on servicing models that include IaaS, PaaS, and SaaS, or hybrid mixtures of these services.

cluster Basic unit of storage on a hard disk. Multiple sectors are contained in a cluster. When Windows stores a file on a disk, it writes those files into dozens or even hundreds of contiguous clusters. If there aren't enough contiguous open clusters available, the operating system finds the next open cluster and writes there, continuing this process until the entire file is saved. The FAT or MFT tracks how the files are distributed among the clusters on the disk.

code Set of symbols representing characters (e.g., ASCII code) or instructions in a computer program (a programmer writes source code, which must be translated into executable or machine code for the computer to use).

codebook A collection of CPU commands; also referred to as an instruction

https://t.me/learningnets

set.

codec (compressor/decompressor) Software that compresses or decompresses media streams.

cold cathode fluorescent lamps (CCFLs) An older type of display backlights that is efficient and long-lasting.

collaborative applications Enables multiple people to work on the same data simultaneously and instantly see each other's changes.

color depth Term to define a scanner's ability to produce color, hue, and shade.

COM port(s) Serial communications ports available on a computer. COM*x* is used to designate a uniquely numbered COM port such as COM1, COM2, etc.

command A request, typed from a terminal or embedded in a file, to perform an operation or to execute a particular program.

command-line interface User interface for an OS devoid of all graphical trappings.

command prompt Text prompt for entering commands.

CompactFlash (CF) One of the older but still popular flash media formats. Its interface uses a simplified PC Card bus, so it also supports I/O devices.

compression Process of squeezing data to eliminate redundancies, allowing files to use less space when stored or transmitted.

computer A sophisticated machine, also called a *computing device*, that you can use to create work, play games, and so on. Computers have processing and input/output hardware, an operating system, and application software.

Computer Management Applet in Windows' Administrative Tools that contains several useful snap-ins, such as Device Manager and Disk Management.

Computing Technology Industry Association (CompTIA) Nonprofit IT trade association that administers the CompTIA A+ and CompTIA IT Fundamentals+

https://t.me/learningnets

exams, and many other vendor-neutral IT certification exams.

connectors Small receptacles used to attach cables to a system. Common types of connectors include USB, PS/2, DB-25, RJ-45, HDMI, DVI, HD15, DisplayPort, and Thunderbolt.

consumables Materials used up by printers, including paper, ink, ribbons, and toner cartridges.

context menu Small menu brought up by right-clicking objects in Windows.

Control Panel Collection of Windows applets, or small programs, that can be used to configure various pieces of hardware and software in a system.

controller card Card adapter that connects devices, such as a drive, to the main computer bus/motherboard.

cookie A small web browser file that contains site information including web site session details, preferences (such as language) and so on. A *first-party cookie* comes from the web site you are actually visiting. First-party cookies can be helpful. A *third-party cookie* comes from another source, such as an advertisement on the web page.

copy backup Type of backup similar to a normal or full backup, in that all selected files on a system are backed up. This type of backup does not change the archive bit of the files being backed up.

copy command Command in the command-line interface for making a copy of a file and pasting it in another location.

copyright Rights given to the owner of an artistic creative work such as music or literature.

CPU (central processing unit) "Brain" of the computer. Microprocessor that handles primary calculations for the computer. CPUs are known by names such as Core i5 and Phenom II.

crossover cable Specially wired network cable that reverses receive and transmit wires at the opposite end of a cable.

https://t.me/learningnets

CRUD Create, read, update, delete; common database transactions.

daily backup Backup of all files that have been changed on that day without changing the archive bits of those files. Also called *daily copy backup*.

data correlation Examines the relationship between data items; often used to test web applications by re-submitting web server values during load testing.

data at rest Data that is stored on any type of storage media on-premises or in the cloud.

data loss prevention DLP; controls put in place to protect sensitive data or intellectual property.

data manipulation language Computer programming language used to perform database CRUD operations. (*See also* CRUD.)

data storage Saving a permanent copy of your work so that you can return to it later.

data definition language DDL; a schema used to define database storage structures.

DC (direct current) Type of electricity in which the flow of electrons is in a complete circle in one direction.

DDOS (distributed denial of service) An attack on a computer or network device in which multiple computers send data and requests to the device in an attempt to overwhelm it so that it cannot perform normal operations.

DDR (double data rate) Shortened reference to memory technology, such as DDR SDRAM. Similarly, DDR2 can refer to DDR2 SDRAM, DDR3 to DDR3 SDRAM, and so on.

DDR RAM (double data rate SDRAM) Shortened reference to memory technology, such as DDR SDRAM.

debug To detect, trace, and eliminate errors in computer programs.

dedicated server Machine that is not used for any client functions, only server

https://t.me/learningnets

functions.

default gateway In a TCP/IP network, the nearest router to a particular host. This router's IP address is part of the necessary TCP/IP configuration for communicating with multiple networks using IP.

definition file List of virus signatures that an antivirus program can recognize.

del (erase) Command in the command-line interface used to delete/erase files.

desktop User's primary interface to the Windows operating system.

desktop computer Full-sized nonmobile high-powered computing device found in most office environments.

desktop environment Different Linux distros have their own user interface known as a desktop environment (DE).

device driver Program used by the operating system to control communications between the computer and peripherals.

device hardening Actions to make a computing device as difficult as possible for unauthorized people to access.

Device Manager Utility that enables techs to examine and configure all the hardware and drivers in a Windows PC.

DHCP (Dynamic Host Configuration Protocol) Protocol that enables client hosts to request and receive TCP/IP settings automatically from an appropriately configured server.

digital certificate Form in which a public key is sent from a web server to a web browser so that the browser can decrypt the data sent by the server.

DIMM (dual inline memory module) 32- or 64-bit type of DRAM packaging with the distinction that each side of each tab inserted into the system performs a separate function. DIMMs come in a variety of sizes, with 184-, 240-, and 288-pin being the most common on desktop computers.

dir Command used in the command-line interface to display the entire contents

https://t.me/learningnets

of the current working directory.

directory Another name for a folder.

disk duplexing Type of disk mirroring using two separate controllers rather than one; faster than traditional mirroring.

disk initialization A process that places special information on every hard drive installed in a Windows system.

Disk Management Snap-in available with the Microsoft Management Console that enables techs to configure the various disks installed in a system; available in the Computer Management Administrative Tool.

disk mirroring Process by which data is written simultaneously to two or more disk drives. Read and write speed is decreased, but redundancy in case of catastrophe is increased.

display adapter Handles all the communication between the CPU and the monitor. This is also known as a *video card*.

Display applet Tool in Windows XP and Windows 7 used to adjust display settings, including resolution, refresh rate, driver information, and color depth.

DisplayPort Digital video connector used by Apple Mac desktop models and some PCs, notably from Dell. Designed by VESA as a royalty-free connector to replace VGA and DVI.

distribution (distro) A specific variant of Linux.

DNS (domain name service or domain name server) TCP/IP name resolution system that translates a host name into an IP address.

DNS domain Specific branch of the DNS name space. First-level DNS domains include .com, .gov, and .edu.

Documents folder Windows folder for storing user-created files.

domain Groupings of users, computers, or networks. In Microsoft networking, a domain is a group of computers and users that share a common account

https://t.me/learningnets

database and a common security policy. On the Internet, a domain is a group of computers that share a common element in their hierarchical name. Other types of domains exist—e.g., broadcast domain, etc.

domain-based network Network that eliminates the need for logging on to multiple servers by using domain controllers to hold the security database for all systems.

DoS (denial of service) An attack on a computer resource that prevents it from performing its normal operations, usually by overwhelming it with large numbers of requests in an effort to monopolize its resources.

dot-matrix printer Printer that creates each character from an array of dots. Pins striking a ribbon against the paper, one pin for each dot position, form the dots. This may be a serial printer (printing one character at a time) or a line printer.

double data rate (DDR) RAM Memory that can send or receive data twice for each clock tick on the motherboard.

drawing pad Used with a stylus pen for data input.

drive letter A letter designating a specific drive or partition in the Windows operating system.

driver signing Digital signature for drivers used by Windows to protect against potentially bad drivers.

DSL (digital subscriber line) High-speed Internet connection technology that uses a regular telephone line for connectivity. DSL comes in several varieties, including asynchronous (ADSL) and synchronous (SDSL), and many speeds. Typical home-user DSL connections are ADSL with faster download speeds than upload speeds.

dual boot Refers to a computer with two operating systems installed, enabling users to choose which operating system to load on boot. Can also refer to kicking a device a second time just in case the first time didn’t work.

dual-core CPUs that have two execution units on the same physical chip but share caches and RAM.

https://t.me/learningnets

dual voltage Refers to power supplies that work with either 110–120 VAC (United States, Canada) or 220–240 VAC (most other parts of the world).

dumb terminal A keyboard and monitor connected to a device that had no processing power, just network connection points.

dumpster diving To go through someone's trash in search of information.

DVD (digital versatile disc) Optical disc format that provides for 4 GB to 17 GB of video or data storage.

DVD-RAM A type of writable DVD disc that is used primarily in camcorders and personal video recorders.

DVD-ROM DVD equivalent of the standard CD-ROM.

DVD-RW/DVD+RW Incompatible rewritable DVD media formats.

DVD-Video DVD format used exclusively to store digital video; capable of storing over two hours of high-quality video on a single DVD.

DVI (Digital Visual Interface) Special video connector designed for digital-to-digital connections; most commonly seen on PC video cards and LCD monitors. Some versions also support analog signals with a special adapter.

dynamic disks Special feature of Windows that enables users to span a single volume across two or more drives. Dynamic disks do not have partitions; they have volumes. Dynamic disks can be striped, mirrored, and striped or mirrored with parity.

dynamic RAM Standard system memory that must be constantly refreshed because it can retain data only while powered.

eavesdropping A method of capturing network communications not intended for the capturer similar to wiretapping phone lines; often performed using a packet capturing tool such as Wireshark.

e-book reader E-book readers (such as Amazon Kindle or Barnes & Noble Nook), which are basically tablets specialized for reading e-books.

https://t.me/learningnets

EFS (encrypting file system) Storage organization and management service, such as NTFS, that has the capability of applying a cipher process to the stored data.

electromagnetic interference (EMI) Electrical interference from one device to another, resulting in poor performance of the device being interfered with. Examples are static on your TV while running a blow dryer and placing two monitors too close together and getting a “shaky” screen.

electrostatic discharge (ESD) Uncontrolled rush of electrons from one object to another. This is a real menace to PCs, as it can cause permanent damage to semiconductors.

e-mail (electronic mail) Messages, usually text, sent from one person to another via computer. Can also be sent automatically to a group of addresses (mailing list).

encryption Making data unreadable by those who do not possess a key or password.

e-reader Mobile electronic device used for reading e-books.

ergonomics The study of how humans and equipment interact.

eSATA (external SATA) Serial ATA-based connector for external hard drives and optical drives.

escalate Process used when person assigned to repair a problem is not able to get the job done, such as sending the problem to someone with more expertise.

establish a plan of action and implement the solution After establishing and testing a theory about a particular problem, techs solve the problem. This is step 4 of 6 in the CompTIA troubleshooting theory. (*See also* troublehooting theory.)

establish a theory of probable cause After identifying a problem, techs question the obvious to determine what might be the source of the problem. This is step 2 of 6 in the CompTIA troubleshooting theory. (*See also* troublehooting theory.)

Ethernet Name coined by Xerox for the first standard of network cabling and

https://t.me/learningnets

protocols. Based on a bus topology.

EULA (end-user license agreement) Agreement that accompanies a piece of software, to which the user must agree before using the software. This outlines the terms of use for the software and also lists any actions on the part of the user that violate the agreement.

Event Viewer Utility made available in Windows as an MMC snap-in that enables users to monitor various system events, including network bandwidth usage and CPU utilization.

e-wallet A software utility that remembers your many screen names, passwords, and credit-card numbers to make online purchases easier and faster.

expansion bus Set of wires going to the CPU, governed by the expansion bus crystal, directly connected to expansion slots of varying types (PCI, PCIe, etc.).

expansion card Electrical circuit board that can add capabilities to a computer.

expansion slots Connectors on a motherboard that enable users to add optional components to a system. (*See also* PCI [Peripheral Component Interconnect]; PCIe [PCI Express].)

ext4 A Linux file system type that supports journaling.

Extensible Authentication Protocol (EAP) Authentication wrapper that EAP-compliant applications can use to accept one of many types of authentication. While EAP is a general-purpose authentication wrapper, its only substantial use is in wireless networks.

extension Letters that follow a filename and identify the type of file. Some common file extensions are .zip, .exe, .doc, .java, and .xhtml.

face lock Technology that enables use of facial features to unlock a mobile device or personal computer.

FAT (file allocation table) Hidden table that records how files on a hard disk are stored in distinct clusters; the only way DOS knows where to access files. Address of first cluster of a file is stored in the directory file. FAT entry for the first cluster is the address of the second cluster used to store that file. In the entry

https://t.me/learningnets

for the second cluster for that file is the address for the third cluster, and so on, until the final cluster, which gets a special end-of-file code. There are two FATs, mirror images of each other, in case one is destroyed or damaged. This also refers to the 16-bit file allocation table when used by Windows 2000 and later NT-based operating systems.

FAT32 File allocation table; a file system type that uses 32 bits to address and index file clusters. This is commonly used with USB flash-media drives and older versions of Windows.

fax machine Scans a hard copy of a document and then converts it to digital data and transmits it across telephone lines using a built-in modem to another fax machine.

fiber-optic cable High-speed cable for transmitting data, made of high-purity glass sealed within an opaque tube. This is much faster than conventional copper wire such as coaxial cable.

field A database definition element specifying the type of data to be stored along with size limits, allowed input values and so on; this is also called a *column*.

file Collection of any form of data that is stored beyond the time of execution of a single job. A file may contain program instructions or data, which may be numerical, textual, or graphical information.

File Explorer A tool in Windows 8/8.1/10 that enables users to browse files and folders.

file format How information is encoded in a file. Two primary types are binary (pictures) and ASCII (text), but within those are many formats, such as BMP and GIF for pictures. This is commonly represented by a suffix at the end of the filename, for example, .txt for a text file or .exe for an executable.

file server Computer designated to store software, courseware, administrative tools, and other data on a LAN or WAN. It “serves” this information to other computers via the network when users enter their personal access codes.

file system Scheme that directs how an OS stores and retrieves data on and off a drive; FAT32 and NTFS are both file systems. Used interchangeably with the

https://t.me/learningnets

term *data structure*.

filename Name assigned to a file when the file is first written on a disk. Every file on a disk within the same folder must have a unique name. Filenames can contain any character (including spaces), except the following: \ / : * ? “< > |

Finder The file and folder browser in macOS.

fingerprint lock Type of biometric device that enables a user to unlock a mobile device using a fingerprint.

firewall Device that restricts traffic between a local network and the Internet.

FireWire (IEEE 1394) Interconnection standard to send wide-band signals over a serialized, physically thin connector system. Serial bus developed by Apple and Texas Instruments; enables connection of 63 devices at speeds up to 800 Mbps.

firmware Embedded programs or code stored on a ROM chip. This is generally OS-independent, thus allowing devices to operate in a wide variety of circumstances without direct OS support. The system BIOS is firmware.

firmware upgrade Process by which the BIOS/UEFI of a motherboard can be updated to reflect patched bugs and added features. This is performed, usually, through CMOS, though some motherboard manufacturers provide a Windows program for performing a firmware upgrade.

flash drive *See* USB thumb drive.

flatbed scanner Most popular form of consumer scanner; runs a bright light along the length of the tray to capture an image.

flat file Simple data storage, such as in a text file; is referred to as *flat-file* storage.

flat panel display A display that is thin (many are thinner than a half-inch), is lightweight, and has very little power.

float Computer programming numeric data type that can have decimal points.

https://t.me/learningnets

foreign key Some kind of unique identifier that joins related data tables; a combination of one or more fields (columns) in both tables.

form factor Standard for the physical organization of motherboard components and motherboard size. Most common form factors are ATX, microATX, and Mini-ITX.

format Command in the command-line interface used to format a storage device.

formatting Magnetically mapping a disk to provide a structure for storing data; can be done to any type of disk, including a hard disk, or other type of removable disk.

frame A data unit transferred across a network. Frames consist of several parts, such as the sending and receiving MAC addresses, the data being sent, and the frame check sequence.

freeware Software that is distributed for free, with no license fee.

front-view projector Shoots the image out the front and counts on you to put a screen in front at the proper distance.

FTP (File Transfer Protocol) Rules that enable two computers to talk to one another during a file transfer. This is the protocol used when you transfer a file from one computer to another across the Internet. FTP uses port numbers 20 and 21.

FTPS (File Transfer Protocol over SSL) An extension to FTP that uses the Secure Sockets Layer (SSL) or Transport Layer Security (TLS) cryptographic protocol.

fully qualified domain name (FQDN) A complete, bottom-to-top label of a DNS host going from the specific host to the top-level domain that holds it and all of the intervening domain layers, with each layer being separated by a dot. FQDNs are entered into browser bars and other utilities in formats like *mail.totalseminars.com*.

function In computer programming, a chunk of code that performs a specific task and lends itself nicely to code reusability.

https://t.me/learningnets

function key Keys commonly found on a laptop keyboard with an *F* prefix (F1, F2, F3 and so on) that provide alternate functionality such as enabling airplane mode or controlling screen brightness.

geotracking Feature in cellular phones that enables the cell phone companies and government agencies to use the ID or MAC address to pinpoint where a phone is at any given time.

gesture-based interaction Various actions using one or more fingers to input on a touchscreen, like on a tablet or smartphone.

giga- Prefix for the quantity 1,073,741,824 (2^{30}) or for 1 billion. One gigabyte would be 1,073,741,824 bytes, except with hard drive labeling, where it means 1 billion bytes. One gigahertz is 1 billion hertz. Commonly used for GB (gigabyte), Gb (gigabit), and GHz (gigahertz).

Global Positioning System (GPS) Technology that enables a mobile device to determine where you are on a map.

GPU (graphics processing unit) Specialized processor that helps the CPU by taking over all of the 3-D rendering duties.

group Collection of user accounts that share the same access capabilities.

GSM (Global System for Mobile Communications) Wireless data standard for mobile devices.

GUI (graphical user interface) Interface that enables user to interact with computer graphically, by using a mouse or other pointing device to manipulate icons that represent programs or documents, instead of using only text as in early interfaces. It is pronounced as “gooey.”

gyroscope Device that can detect the position of the tablet or phone in 3-D space.

hacker A term for talented experts driven to expand, extend, improve, overcome, and repurpose existing hardware, software, and systems. Also used to refer to malicious IT users or attackers.

hard drive Data-recording system using solid disks of magnetic material

https://t.me/learningnets

turning at high speeds to store and retrieve programs and data in a computer. It is abbreviated as HDD when used for *hard disk drive*.

hardening Reducing the attack surface through methods such as applying patches, disabling unnecessary software, etc.

hardware Physical computer equipment such as electrical, electronic, magnetic, and mechanical devices. Anything in the computer world that you can hold in your hand. A hard drive is hardware; Microsoft Word is not.

hardware protocol Defines many aspects of a network, from the packet type to the cabling and connectors used.

HDD (hard disk drive) *See* hard drive.

HDMI (High Definition Multimedia Interface) Single multimedia connection that includes both high-definition video and audio. One of the best connections for outputting to television. It also contains copy protection features.

heat sink A block of heat-conductive metal such as aluminum affixed to a chip with some heat-conductive *thermal paste*. The heat sink has spikes or baffles that increase its surface area. Heat wicks away from the chip into the heat sink and dissipates into the air.

hertz A unit of measurement related to the number of changes in an electrical signal within one second. Commonly expressed in millions (megahertz) or billions (gigahertz).

hex (hexadecimal) Base-16 numbering system using ten digits (0 through 9) and six letters (A through F). In the computer world, shorthand way to write binary numbers by substituting one hex digit for a four-digit binary number (e.g., hex 9 = binary 1001).

HFS Hierarchical file system; file system used on macOS.

hibernation Power management setting in which all data from RAM is written to the hard drive before the system goes into Sleep mode. Upon waking up, all information is retrieved from the hard drive and returned to RAM.

hidden attribute File attribute that, when used, does not allow the dir

https://t.me/learningnets

command to show a file.

hierarchical directory tree Method by which Windows organizes files into a series of folders, called *directories,* under the root directory.

HomeGroup A Windows 7 and later feature that connects a group of computers using a common password—no special usernames required. Each computer can be a member of only one homegroup at a time. Homegroups enable simple sharing of documents and printers between computers.

host On a TCP/IP network, single device that has an IP address—any device (usually a computer) that can be the source or destination of a data packet. In the mainframe world, this is computer that is made available for use by multiple people simultaneously. Also, in virtualization, this is a computer running one or more virtual operating systems.

hostname Windows command for displaying the name of a computer.

hotspot Feature that enables a mobile device connected to a mobile data network to be used as a wireless access point (WAP) for other devices. Often these are stand-alone devices, though many cellular phones and data-connected tablets can be set up to act as hotspots.

hot-swappable Any hardware that may be attached to or removed from a PC without interrupting the PC's normal processing.

HTML (Hypertext Markup Language) ASCII-based, script-like language for creating hypertext documents such as those on the World Wide Web.

HTTP (Hypertext Transfer Protocol) Extremely fast protocol used for network file transfers in the WWW environment. It uses port 80.

HTTPS (HTTP over Secure Sockets Layer) Secure form of HTTP used commonly for Internet business transactions or any time when a secure connection is required. It uses port 443. (*See also* HTTP [Hypertext Transfer Protocol].)

hub Electronic device that sits at the center of a star topology network, providing a common point for the connection of network devices. Hubs repeat all information out to all ports and have been replaced by switches, although the

https://t.me/learningnets

term *hub* is still commonly used.

hybrid A network topology that combines features from multiple other topologies, such as the star-bus topology.

hyperthreading CPU feature that enables a single pipeline to run more than one thread at once.

hypervisor Software that enables a single computer to run multiple virtualized operating systems simultaneously.

I/O (input/output) General term for reading and writing data to a computer. *Input* includes data entered from a keyboard, identified by a pointing device (such as a mouse), or loaded from a disk. *Output* includes writing information to a disk, viewing it on a monitor, or printing it to a printer.

iCloud Apple cloud-based storage. iCloud enables a user to back up all iPhone or iPad data and makes that data accessible from anywhere. This includes any media purchased through iTunes and calendars, contacts, reminders, and so forth.

identify the problem To question the user and find out what has been changed recently or is no longer working properly. This is step 1 of 6 in the CompTIA troubleshooting theory. (*See also* troublehooting theory.)

IEEE (Institute of Electronic and Electrical Engineers) Leading standards-setting group in the United States.

IEEE 1284 IEEE standard governing parallel communication.

IEEE 1394 IEEE standard governing FireWire communication. (*See also* FireWire [IEEE 1394].)

IEEE 1394a FireWire standard that runs at 400 Mbps.

IEEE 1394b FireWire standard that runs at 800 Mbps.

IEEE 802.11 Wireless Ethernet standard more commonly known as Wi-Fi.

imaging software Create an image of a physical or virtual hard drive that is

https://t.me/learningnets

stored as an image file. The image file can then be restored to a physical or virtual disk in the event of a disk problem.

IMAP4 (Internet Message Access Protocol version 4) An alternative to POP3 that retrieves e-mail from an e-mail server, like POP3; IMAP uses TCP port 143.

impact printer Uses pins and inked ribbons to print text or images on a piece of paper.

incremental backup Backs up all files that have their archive bits turned on, meaning that they have been changed since the last backup. Turns the archive bits off after the files have been backed up.

infrastructure mode Wireless networking mode that uses one or more WAPs to connect the wireless network nodes to a wired network segment.

ink cartridge Small container of ink for inkjet printers.

inkjet printer Uses liquid ink, sprayed through a series of tiny jets, to print text or images on a piece of paper.

installation disc Typically a CD-ROM or DVD that holds all the necessary device drivers.

int Computer programming numeric data type; an integer; a whole number with no decimals.

integrated drive electronics (IDE) A controller that translates requests from the PC into action, telling the heads where to read or write.

intellectual property IP; a unique work that the creators has rights to.

Internet Global collection of interconnected networks.

Internet cache When you go to a web site, browsers store copies of the graphics and other items so the page will load more quickly the next time you access it. These are part of the *Internet cache.*

iOS The operating system of Apple mobile devices.

https://t.me/learningnets

IoT Internet of Things; consumer devices such as home environmental controls, baby monitors, smart cars, fridges, and so on, that communicate over the Internet.

IP (Internet Protocol) A set of rules used to identify and locate devices on networks; an essential component in the TCP/IP protocol suite, the communications rules that enable the Internet to function.

IP address Numeric address of a computer connected to the Internet. An IPv4 address consists of four octets of 8-bit binary numbers translated into their shorthand numeric values. An IPv6 address is 128 bits long. The IP address can be broken down into a network ID and a host ID. This is also called the *Internet address*.

IPv4 (Internet Protocol version 4) Internet standard protocol that provides a common layer over dissimilar networks; used to move packets among host computers and through gateways if necessary. It is part of the TCP/IP protocol suite. This uses the dotted-decimal format—*x.x.x.x*. Each *x* represents an eight-bit binary number, or 0 to 255. Here's an example: 192.168.4.1.

IPv6 (Internet Protocol version 6) Protocol in which addresses consist of eight sets of four hexadecimal numbers, each number being a value between 0000 and FFFF, using a colon to separate the numbers. Here's an example: FEDC:BA98:7654:3210:0800:200C:00CF:1234.

IR (infrared) Wireless short-range device communication technology.

IrDA (Infrared Data Association) protocol Protocol that enables communication through infrared devices, with speeds of up to 4 Mbps.

ISDN (integrated services digital network) CCITT (Comité Consultatif Internationale de Télégraphie et Téléphonie) standard that defines a digital method for communications to replace the current analog telephone system. ISDN is superior to POTS telephone lines because it supports a transfer rate of up to 128 Kbps for sending information from computer to computer. It also allows data and voice to share a common phone line. DSL reduced demand for ISDN substantially.

ISO file Complete copy (or image) of a storage media device, typically used for optical discs. ISO image files typically have a file extension of .iso.

https://t.me/learningnets

ISP (Internet service provider) Company that provides access to the Internet, usually for money.

ITX A family of motherboard form factors. Mini-ITX is the largest and the most popular of the ITX form factors but is still quite small.

jack (physical connection) Part of a connector into which a plug is inserted. Also referred to as a *port*.

journaling file system File system type (such as NTFS, ext4) that tracks file system writes not yet written to disk in a transaction log, or journal; useful for repairing file system problems resulting from improper disk volume dismounts.

kernel Core portion of program that resides in memory and performs the most essential operating system tasks.

keyboard Input device. Three common types of keyboards exist: those that use a mini-DIN (PS/2) connection, those that use a USB connection, and those that use wireless technology.

keylogger A hardware device or malware that records every keystroke entered.

kilo- Prefix that stands for the binary quantity 1,024 (2^{10}) or the decimal quantity of 1,000. One kilobyte is 1,024 bytes. One kilohertz, however, is a thousand hertz. This is commonly used for KB (kilobyte), Kb (kilobit), and KHz (kilohertz).

knowledge factor Related to authentication; possessing specific knowledge, such as a username or password.

LAN (local area network) Group of PCs connected via cabling, radio, or infrared that use this connectivity to share resources such as printers and mass storage.

laplet A device whose functionality is somewhere between laptop and tablet.

laptop Traditional clamshell portable computing device with built-in LCD monitor, keyboard, and trackpad.

laser printer Electro-photographic printer in which a laser is used as the light

https://t.me/learningnets

source.

launcher A part of the Chrome OS user interface where programs are started.

LED monitor LCD monitor that uses LEDs instead of CCFL tubes for backlighting, creating much higher contrast ratios and image quality.

level 1 (L1) cache First RAM cache accessed by the CPU, which stores only the absolute most-accessed programming and data used by currently running threads. This is always the smallest and fastest cache on the CPU.

level 2 (L2) cache Second RAM cache accessed by the CPU. This is much larger and often slower than the L1 cache and accessed only if the requested program/data is not in the L1 cache.

level 3 (L3) cache Third RAM cache accessed by the CPU. This is much larger and slower than the L1 and L2 caches and accessed only if the requested program/data is not in the L2 cache.

Library Feature in Windows 7 and later that aggregates folders from multiple locations and places them in a single, easy-to-find spot in Windows Explorer or File Explorer. Default libraries in Windows include Documents, Music, Pictures, and Videos.

light-emitting diode (LED) A type of display backlight that uses a grid of many tiny lightbulbs.

Lightning An eight-pin connector, proprietary to Apple, that can be inserted without regard to orientation. This is used to connect mobile devices to a power or data source.

Linux Open-source UNIX-clone operating system.

liquid cooling A method of cooling a PC that works by running some liquid—usually water—through a metal block that sits on top of the CPU, absorbing heat. The liquid gets heated by the block, runs out of the block and into something that cools the liquid, and is then pumped through the block again.

liquid crystal display (LCD) A type of display that has a backlit layer of liquid crystal molecules (called *subpixels*) sandwiched between polarizing filters.

https://t.me/learningnets

Live DVD The Windows installation media, which loads the Windows Preinstallation Environment (WinPE) directly from disc into memory and doesn't access or modify a hard drive or solid state drive.

local permissions Resource privileges applied only to a local resource as opposed to privileges applied over a network.

local storage Storage available to a device without transmitting over a network; also called *direct attached storage*.

local user account List of user names and their associated passwords with access to a system, contained in an encrypted database.

Local Users and Groups Tool enabling creation and changing of group memberships and accounts for users.

lossless compression Creates a file that retains the quality of the original file. Media producers use this kind of compression when file size doesn't really matter but quality does.

lossy compression Deletes some of data from the file to make the final file size smaller.

lumens Unit of measure for amount of brightness on a projector or other light source.

Mac Common name for Apple Computers' flagship operating system; also Macintosh. (*See also* macOS.)

MAC address filtering Method of limiting wireless network access based on the 48-bit hexadecimal address (MAC address) of the wireless NIC of a computing device.

machine language Binary instruction code that is understood by the CPU.

macOS Apple's flagship operating system; runs on Intel-based hardware. CompTIA refers to the operating system as *Mac OS*. The OS has gone through many names: Macintosh, Mac, Mac OS X, OS X, and macOS.

mainframe Large powerful computers used by government and large

https://t.me/learningnets

organizations for critical applications such as transaction processing or census results.

man-in-the-middle attack (MITM) An attacker impersonating one party of an active network conversation and replaying previous captured traffic that has been modified by the attacker; a type of replay attack.

md (mkdir) Command in the command-line interface used to create directories.

mega- Prefix that stands for the binary quantity 1,048,576 (2^{20}) or the decimal quantity of 1,000,000. One megabyte is 1,048,576 bytes. One megahertz, however, is a million hertz. Sometimes shortened to *meg*, as in "a 286 has an address space of 16 megs." It is commonly used for MB (megabyte), Mb (megabit), and MHz (megahertz).

megapixel Term used typically in reference to digital cameras and their ability to capture data.

memory Device or medium for temporary storage of programs and data during program execution. Synonymous with storage, although it most frequently refers to the internal storage of a computer that can be directly addressed by operating instructions. A computer's temporary storage capacity is measured in kilobytes (KB), megabytes (MB), or gigabytes (GB) of random-access memory (RAM). Long-term data storage on hard drives and solid-state drives is also measured in megabytes, gigabytes, and terabytes.

memory addressing Taking memory address from system RAM and using it to address nonsystem RAM or ROM so the CPU can access it.

metadata Additional information associated with an entity such as a file; metadata might include associated cost center, sensitivity level, etc.

Metro UI Name given to the Windows 8.*x* user interface.

Micro Secure Digital (MicroSD) The smallest form factor of the SD flash memory standard. It is often used in mobile devices.

micro USB USB connector commonly found on Android phones.

https://t.me/learningnets

microATX (µATX) Variation of the ATX form factor, which uses the ATX power supply. MicroATX motherboards are generally smaller than their ATX counterparts but retain all the same functionality.

microBTX Variation of the BTX form factor. MicroBTX motherboards are generally smaller than their BTX counterparts but retain all the same functionality.

microcomputer A computing device with moderate computing power, similar to the older and slower minicomputer.

microprocessor "Brain" of a computer. Primary computer chip that determines relative speed and capabilities of the computer. Also called CPU.

microservice A small reusable chunk of code that performs a specific function that is a part of a larger application.

MIDI (musical instrument digital interface) Interface between a computer and a device for simulating musical instruments. Rather than sending large sound samples, a computer can simply send "instructions" to the instrument describing pitch, tone, and duration of a sound. MIDI files are therefore efficient. Because a MIDI file consists of a set of instructions rather than a copy of the sound, modifying each component of the file is easy. Additionally, it is possible to program many channels, or "voices," of music to be played simultaneously, creating symphonic sound.

MIDI-enabled device External device that enables you to input digital sound information in the MIDI format; for example, a MIDI keyboard (the piano kind).

mini-audio connector A popular, 1/8-inch-diameter connector used to transmit two audio signals; perfect for stereo sound.

minicomputer A computer with moderate computing power; more than a mobile device but less than a server.

Mini-ITX The largest and the most popular of the three ITX form factors. At a miniscule 6.7 by 6.7 inches, Mini-ITX competes with microATX and proprietary small form factor (SFF) motherboards.

Mini-PCI Specialized form of PCI designed for use in laptops.

https://t.me/learningnets

Mini-PCIe Specialized form of PCIe designed for use in laptops.

mini power connector Connector used to provide power to floppy disk drives.

mobile app An application designed to run on a mobile computing device such as a smartphone.

modem (modulator/demodulator) Device that converts a digital bit stream into an analog signal (modulation) and converts incoming analog signals back into digital signals (demodulation). An analog communications channel is typically a telephone line, and analog signals are typically sounds.

Molex connector Computer power connector used by optical drives, hard drives, and case fans. Keyed to prevent it from being inserted into a power port improperly.

monitor Screen that displays data from a PC. Can use either a cathode ray tube (CRT) or a liquid crystal display (LCD) to display images.

monolithic application A single-tier application running on a single computer.

motherboard Flat piece of circuit board that resides inside your computer case and has a number of connectors on it. Every device in a PC connects directly or indirectly to the motherboard, including CPU, RAM, hard drives, optical drives, keyboard, mouse, and video cards. Also called a *system board*.

mouse Input device that enables users to manipulate a cursor on the screen to select items.

move Command in the command-line interface used to move a file from one location to another.

MP3 Short for MPEG Audio Layer 3, a type of compression used specifically for turning high-quality digital audio files into much smaller yet similar-sounding files.

MPA (Microsoft Product Activation) The process of providing a valid Microsoft software key to prove the authenticity of your software.

MPEG-2 Moving Pictures Experts Group Layer 2 standard of video and audio

https://t.me/learningnets

compression offering resolutions up to 1280 × 720 at 60 frames per second.

MPEG-4 Moving Pictures Experts Group Layer 4 standard of video and audio compression offering improved compression over MPEG-2.

multiboot A computer with multiple operating systems installed; the user can select which operating system upon machine startup.

multicore processing Using two or more execution cores on one CPU to divide up work independently of the OS.

multifactor authentication (MFA) An authentication schema requiring more than one unique authentication method. An example is a password and a fingerprint (inherence factors) or a username and password along with a token device (possession factor).

multifunction device (MFD) A printer with one or more other devices rolled in, such as scanner and copy machine; also called a *multifunction printer* (MFP).

multitouch Input method on many smartphones and tablets that enables you to use multiple fingers to do all sorts of fun things, such as using two fingers to scroll or swipe to another screen or desktop.

multiuser computer A computer allowing multiple users to perform computing tasks either locally or remotely.

mv The move command in Linux and macOS.

My Computer An applet that enables users to access a complete listing of all fixed and removable drives contained within a system and to view/manage configuration properties of the computer; also an aspect of Windows Explorer.

n-tier Multilevel applications having a front-end or user interface (UI) tier, such as a web site that runs on a web server, a middle-tier software component running on a different server, which in turn might read and write data to a back-end tier hosting database servers.

Nano-ITX A 4.7 inch by 4.7 inch variation of the ITX form factor.

network Collection of two or more computers interconnected by telephone

https://t.me/learningnets

lines, coaxial cables, satellite links, radio, and/or some other communication technique. Group of computers that are connected and that communicate with one another for a common purpose.

network attached storage (NAS) A device that attaches to a network for the sole purpose of storing and sharing files.

network storage Storage that appears local to the operating system but is accessed over a network.

NFC (near field communication) Mobile technology that enables short-range wireless communication between mobile devices. Now used for mobile payment technology such as Apple Pay and Google Wallet.

NIC (network interface card or controller) Expansion card or motherboard interface that enables a PC to connect to a network via a network cable. A *wireless NIC* enables connection via radio waves rather than a physical cable.

nonrepudiation The inability to deny that a specific transaction originated from a specific party. An example is a digital signature created by a private key that only the owner of that key has access to.

nonvolatile memory Memory whose contents is retained even when power is no longer present, such as with storage devices.

normal backup Full backup of every selected file on a system; turns off the archive bit after the backup.

NTFS (New Technology File System) Robust and secure file system introduced by Microsoft with Windows NT. NTFS provides an amazing array of configuration options for user access and security. Users can be granted access to data on a file-by-file basis. NTFS enables object-level security, long filename support, compression, and encryption.

NoSQL Uses a semistructured or completely unstructured (schema-less) data storage definition; useful for large amounts of varying types of data.

notebook A small computing device similar in size to a paper-based notebook; this term is often used interchangeably with laptop.

https://t.me/learningnets

numeric keypad Keypad on the right side of a full size keyboard with numbers; used for numeric data entry.

object System component that is given a set of characteristics and can be managed by the operating system as a single entity.

object-oriented programming Programmatic access to any type of item (file, folder, user account, cloud storage, running process, etc.); the item is called an *object*. The object has attributes (properties) and methods (functions). The object is separated from the property or method using a period.

OEM (original equipment manufacturer) Company that produces software or computer parts that other companies sell in their end products. Microsoft develops Windows OS, for example, that many companies sell with their PCs. Microsoft is the OEM for Windows. Alternatively, refers to companies that source parts from contract manufacturers but brand the end product as their own. Several Chinese companies make the circuit boards and screens used in Apple products, for example, but the final product is an Apple device. Apple is the OEM for the iPhone.

one-time password A uniquely generated password that is never reused.

online storage Storage that is accessible over the Internet; also referred to as *cloud storage* or *hosted storage*.

open source Software environment that is not controlled by a central creator or distributer.

operating system (OS) Software base that allows applications to use computer hardware.

optical disc/media Types of data discs (such as DVDs, CDs, BDs, etc.) that are read by a laser.

optical drive Drive used to read/write to optical discs, such as CDs or DVDs.

optical mouse Pointing device that uses light rather than electronic sensors (ball mouse) to determine movement and direction the mouse is being moved.

organic light-emitting diode (OLED) OLED uses organic compounds that

https://t.me/learningnets

naturally produce colored light rather than needing a backlight.

OS (operating system) Series of programs and code that creates an interface so users can interact with a system's hardware; for example, Windows, macOS, and Linux.

OS X Former name for the operating system on Apple Macintosh computers. (*See also* macOS.)

packet Basic component of communication over a network. Group of bits of fixed maximum size and well-defined format that is switched and transmitted as a single entity through a network. It contains source and destination address, data, and control information.

parallel ATA (PATA) Obsolete storage drive interface that used a 80-wire ribbon cable for data transfer.

partitioning Electronically subdividing a physical hard drive into groups called *partitions* (or *volumes*).

passcode lock Mobile device security feature that requires you to type in a series of letters, numbers, or motion patterns to unlock the mobile device each time you press the power button.

passive cooling System designed to remove heat from a processor without the use of power or mechanical parts; usually accomplished through a metal heat sink.

password cracking A technique for obtaining a password through rapid-fire trial and error, often by employing password-cracking software.

password manager A computer program that centrally and securely stores multiple passwords used by a variety of programs and services.

patch Small piece of software released by a software manufacturer to correct a flaw or problem with a particular piece of software.

patent Exclusive right given to owner of an invention.

PCI (Peripheral Component Interconnect) Design architecture for the

https://t.me/learningnets

expansion bus on the computer motherboard that enables system components to be added to the computer. It is the local bus standard, meaning that devices added to a computer through this port will use the processor at the motherboard's full speed (up to 33 MHz) rather than at the slower 8 MHz speed of the regular bus. PCI moves data 32 or 64 bits at a time rather than the 8 or 16 bits the older ISA buses supported.

PCIe (PCI Express) Serialized successor to PCI and AGP that uses the concept of individual data paths called *lanes*. This may use any number of lanes, although a single lane (×1) and 16 lanes (×16) are the most common on motherboards.

PCIe 6/8-pin power connector Connector on some power supplies for powering a dedicated graphics card.

PCI-X (PCI Extended) Enhanced version of PCI, 64 bits wide. Typically seen in servers and high-end systems.

peer-to-peer network Network in which each machine can act as both a client and a server.

peripheral Any device that connects to the system unit.

persistent storage Storing database data on disk is referred to as *persistent storage* because the data hangs around even between system reboots. When the data is in a memory cache, it is referred to as *nonpersistent storage*.

phablet Portmanteau of "phone" and "tablet." This is a colloquial term for a large phone.

phishing The act of trying to get people to give their usernames, passwords, or other security information by pretending to be someone else electronically.

PII (personally identifiable information) Any data or information that can identify a specific individual.

ping (packet Internet groper) Slang term for a small network message (ICMP ECHO) sent by a computer to check for the presence and aliveness of another. A ping is used to verify the presence of another system. This is also the command used at a prompt to ping a computer.

https://t.me/learningnets

plasma Displays that have their own method of lighting the screen with phosphorous cells instead of liquid crystals; the phosphors do not require backlighting.

platform The hardware on which an OS runs.

Play Store Storefront where Android users can purchase and download apps and digital media.

plug and play (PNP) An OS feature that automatically assigns hardware resources to devices when they are connected to the machine.

point-of-sale (POS) Terminals that process purchase transactions.

POP3 (Post Office Protocol 3) One of the two protocols that receive e-mail from SMTP servers. POP3 uses TCP port 110. While historically most e-mail clients use this protocol, the IMAP4 e-mail protocol is now more common.

port (networking) In networking, the number used to identify the requested service (such as SMTP or FTP) when connecting to a TCP/IP host. Examples include 80 (HTTP), 443, (HTTPS), 21 (FTP), 23 (Telnet), 25 (SMTP), 110 (POP3), 143 (IMAP), and 3389 (RDP).

power conditioner A device that enhances the features of a surge suppressor by storing extra voltage in a capacitor and then releasing it onto the power line to smooth out power sags.

power profile A collection of settings that determine how Windows manages power use.

power sag A reduction in the amount of voltage.

power supply unit (PSU) Provides the electrical power for a PC; converts standard AC power into various voltages of DC electricity in a PC.

PowerShell *See* Windows PowerShell.

ppm (pages per minute) Speed of a printer.

preboot execution environment (PXE) Technology that enables a PC to boot

https://t.me/learningnets

without any local storage by retrieving an OS from a server over a network.

primary key A unique identifier within a single database table.

printer Output device that can print text or illustrations on paper. Microsoft uses the term to refer to the software that controls the physical print device.

processes Running programs on a computer system. Each operating system has tools to view and kill processes.

product key Code used during installation to verify legitimacy of the software.

program/programming Series of binary electronic commands sent to a CPU to get work done.

programmer A person who writes applications or operating system software for computing devices.

Programs and Features Windows Control Panel applet; enables uninstalling or changing program options and altering Windows features.

projector Device for projecting video images from PCs or other video sources, usually for audience presentations. It is available in front- and rearview displays.

prompt A character or message provided by an operating system or program to indicate that it is ready to accept input.

proprietary Technology unique to a particular vendor.

protocol Agreement that governs the procedures used to exchange information between cooperating entities. Usually this includes how much information is to be sent, how often it is to be sent, how to recover from transmission errors, and who is to receive the information.

proxy server Device that fetches Internet resources for a client without exposing that client directly to the Internet. Usually accepts requests for HTTP, FTP, POP3, and SMTP resources. Often caches, or stores, a copy of the requested resource for later use. Common security feature in the corporate world. Proxy settings can be configured within applications such as web browsers.

https://t.me/learningnets

pseudocode A standard spoken or written human language method of planning programming code that will later use computer programming language–specific syntax.

queue Area where objects wait their turn to be processed. An example is the print queue, where print jobs wait until it is their turn to be printed.

QWERTY Name that comes from the first six letters on the top alphabetic row; there's typically a row of numbers above this row and a row of function keys above that.

RAID (redundant array of independent [or inexpensive] disks) Method for creating a fault-tolerant storage system. RAID uses multiple hard drives in various configurations to offer differing levels of speed/data redundancy.

RAM (random access memory) Memory that can be accessed at random; that is, memory that you can write to or read from without touching the preceding address. This term is often used to mean a computer's main memory.

ransomware Malware that prevents access to booting up a system or accessing malware-encrypted files unless a bitcoin ransom is paid. Paying the ransom does not guarantee a decryption key from the malicious user.

raster format Used for photos and digital paintings. It contains color information for each individual dot (pixel) in the entire image.

read-only memory ROM; nonvolatile memory that cannot be written to.

record A stored item within a database consisting of one or more fields (columns); also called a *row* or *document*.

Recycle Bin Location to which files are moved when they are deleted from a modern Windows system. To permanently remove files from a system, they must be emptied from the Recycle Bin.

regression testing Ensuring that software code changes have not indirectly caused problems elsewhere in the code.

relational database Uses a structured blueprint (schema) of how data will be stored through table column (field) definitions. Data in separate tables can be

https://t.me/learningnets

linked together via common values stored in both tables, such as a customer ID value linking a customers table to a purchases table.

Remote Assistance Feature of Windows that enables users to give anyone control of his or her desktop over the Internet.

Remote Desktop Windows tool used to enable a local system to graphically access the desktop of a remote system.

Remote Desktop Protocol Protocol used for Microsoft's Remote Desktop tool. It uses port 3389.

removable media Any storage on a computer that can be easily removed. Examples are optical discs, flash drives, or memory cards.

resistive screen Consists of two thin, flexible sheets of plastic, with a gap between them. When you touch the surface of one sheet, that sheet presses down onto the sheet below it, creating an electrical signal. A resistive screen works no matter what is pressing on it—a finger, a gloved finger, or a stylus.

resolution Measurement for monitors and printers expressed in horizontal and vertical dots or pixels. Higher resolutions provide sharper details and thus display better-looking images.

restore point System snapshot created by the System Restore utility that is used to restore a malfunctioning system.

requirement specification document Used as a blueprint for further SDLC phases.

RFI (radio frequency interference) Another form of electrical interference caused by radio wave–emitting devices, such as cell phones, wireless network cards, and microwave ovens.

RJ (registered jack) connector UTP cable connector, used for both telephone and network connections. RJ-11 is a connector for four-wire UTP; usually found in telephone connections. RJ-45 is a connector for eight-wire UTP; usually found in network connections.

RJ-11 *See* RJ (registered jack) connector.

https://t.me/learningnets

RJ-45 *See* RJ (registered jack) connector.

root folder Top level in the hierarchy of a file system.

rotation speed The speed at which hard disk platters spin. A higher rotation speed means better disk performance.

router Device connecting separate networks; forwards a packet from one network to another based on the network address for the protocol being used. For example, an IP router looks only at the IP network number. Routers operate at layer 3 (Network) of the OSI seven-layer model.

SaaS (software as a service) Cloud-based service to store, distribute, and update programs and applications. The SaaS model provides access to necessary applications wherever you have an Internet connection, often without having to carry data with you or regularly update software. At the enterprise level, the subscription model of many SaaS providers makes it easier to budget and keep hundreds or thousands of computers up-to-date.

SATA (serial ATA) Serialized version of the ATA standard that offers many advantages over PATA (parallel ATA) technology, including thinner cabling, keyed connectors, and lower power requirements.

scalar data type A simple data type storing a single item such as a character or a number; this is the opposite of a complex data type such as an object that contains properties and methods.

scaling Ability to adjust resources to support an IT solution. Vertical scaling increases or decreases the compute power for a physical or virtual machine. Horizontal scaling adds or removes compute nodes to support an application workload.

scientific calculator Calculating device or app that can perform different types of calculations using a variety of numbering systems such as decimal, binary, octal, and hexadecimal.

screen capture A digital image taken of a computer screen; also called a *screenshot*.

SD (Secure Digital) Popular format for flash media cards, such as SD cards;

https://t.me/learningnets

also supports I/O devices.

SDK (software development kit) Software that used to create custom applications or add features to existing applications on your mobile device.

security zone A group of settings that are applicable to a certain trust level for web sites.

separate video (S-Video) An interface for standard-definition video. It is a round plug with four pins.

server Computer that shares its resources, such as printers and files, with other computers on a network. An example is a network file system server that shares its disk space with a workstation that does not have a disk drive of its own.

service A program that runs in the background of a PC but displays no icons anywhere. You can view a list of services in the Windows Task Manager. Also, this is a program stored in a ROM chip.

service pack Collection of software patches released at one time by a software manufacturer.

Services Tab in Windows Task Manager that lists all running services on a system.

single-core A processor containing one processing core.

single factor authentication Possessing one category or authentication methods such as username and password (both are knowledge-based and thus constitute a single factor).

SFTP (Secure File Transfer Protocol) A reliable protocol used for copying and moving files over a network. It is more secure than FTP.

shortcut A special Windows file used to connect to a resource, such as a shortcut on the desktop that opens a file stored on a file server elsewhere.

shoulder surfing An attack technique whereby people spy on you from behind, watching what you type.

https://t.me/learningnets

SID (security identifier) Unique identifier for a security principal such as a user or a computer.

sidebar A part of the Windows Vista interface that displays Gadgets (small utility apps).

single data rate (SDR) RAM Now mostly obsolete, is synchronized with the motherboard's system timer so that it performs one operation per tick of that timer.

smartphone A cell phone enhanced to do things formerly reserved for fully grown PCs, such as web browsing, document viewing, and media consumption.

SMTP (Simple Mail Transport Protocol) Main protocol used to send electronic mail on the Internet. Uses port 25.

SNMP (Simple Network Management Protocol) A set of standards for communication with devices connected to a TCP/IP network. Examples of these devices include routers, hubs, and switches. It uses port 161.

social engineering Using or manipulating people inside the networking environment to gain access to that network from the outside.

SODIMM Small outline dual inline memory module; RAM chips used in laptops.

software Single group of programs designed to do a particular job; always stored on mass storage devices.

software development life cycle (SDLC) A six-step structured framework used by software developers to create and maintain software solutions.

SOHO (small office, home office) Designation for devices for personal use or in small businesses.

solid ink printers Printer that uses solid sticks of nontoxic "ink" that produce vibrant color documents with much less waste than color laser printers.

solid state A component with no moving parts but instead circuit boards and chips.

https://t.me/learningnets

sound card Expansion card that can produce audible tones when connected to a set of speakers.

spam Unsolicited e-mails from both legitimate businesses and scammers that account for a huge percentage of traffic on the Internet.

spyware Software that runs in the background of a user's PC, sending information about browsing habits back to the company that installed it onto the system.

SSD (solid-state drive) Data storage device that uses flash memory to store data.

SSH (Secure Shell) Terminal emulation program similar to Telnet, except that the entire connection is encrypted. It uses port 22.

SSID (service set identifier) Parameter used to define a wireless network; otherwise known as the *network name*.

SSL (Secure Sockets Layer) Security protocol that uses digital certificates to protect network communications; superseded by (Transport Layer Security (TLS).

SSO Single sign-on; allows users to access multiple network services without re-entering credentials for each one.

Start button Button on the Windows taskbar that enables access to the Start menu.

Start menu Menu that can be accessed by clicking the Start button on the Windows taskbar. Enables you to see all programs loaded on the system and to start them.

Start screen Windows 10 version of the Start menu, which functions as a combination of the traditional Start menu and Windows 8/8.1 Modern UI.

streaming media Broadcast of data that is played on your computer and immediately discarded.

string Computer programming data consisting of a collection of characters.

https://t.me/learningnets

strong password Password containing at least eight characters, including letters, numbers, and nonalphanumeric symbols.

subnet mask Value used in TCP/IP settings to divide the IP address of a host into its component parts: network ID and host ID.

subfolder A folder located inside another folder.

subnotebook A SMALL LAPTOP WITH LESS PROCESSING POWER THAN A LAPTOP.

subwoofer Powerful speaker capable of producing extremely low-frequency sounds.

supercomputer A computer with fast processing capabilities beyond standard commodity computers available to the public.

surge suppressor Inexpensive device that protects your computer from voltage spikes.

swipe Gesture for mobile devices where you hold your finger on the screen and slide it across the screen, either right to left or top to bottom, depending on the type of application.

swipe lock Mobile device feature that uses a swipe gesture to unlock the mobile device.

switch Device that filters and forwards traffic based on some criteria. A bridge and a router are both examples of switches. In the command-line interface, a switch is a function that modifies the behavior of a command.

sync The process of keeping files on mobile devices up-to-date with the versions on desktop PCs or over the Internet.

synchronize *See* sync.

synchronous replication An application does not receive notification that data has been written until *all* replicas have committed the data to disk. This normally requires a high-speed network. With asynchronous replication, after the primary, or first, replica has written the data, an application then receives notification that data has been written to disk; this can be used over slow network links.

https://t.me/learningnets

syntax The proper way to write a command-line command so that it functions and does what it's supposed to do.

system BIOS Primary set of BIOS stored on an EPROM or flash ROM chip on the motherboard. Defines the BIOS for all the assumed hardware on the motherboard, such as keyboard controller, floppy drive, basic video, and RAM.

table A database storage structure that defines how data is stored (for relational databases) through field (column) definitions. NoSQL tables do not use as rigid a definition, if at all.

tablet A mobile device consisting of a large touchscreen, enabling the user to browse the Web, view media, or even play games.

Tablet PC Small portable computer distinguished by the use of a touchscreen with stylus and handwriting recognition as the primary modes of input.

tailgating Form of infiltration and social engineering that involves following someone else through a door as if you belong in the building.

tap Touchscreen gesture where you press a spot on the screen to start an app or interact with a running app.

Task Manager Shows all running programs, including hidden ones, and is accessed by pressing ctrl-shift-esc. You can use the Task Manager to shut down an unresponsive application that refuses to close normally.

Task Scheduler Windows utility enabling users to set tasks to run automatically at certain times.

taskbar Contains the Start button, the notification area, the Quick Launch toolbar, and buttons for running applications. This is located by default at the bottom of the desktop.

tasklist A command-line version of the Task Manager.

tbps Terabits per second; 1,000 gigabytes per second.

TCP (Transmission Control Protocol) Rules used for transporting data over a network; part of the TCP/IP protocol suite, the communications rules that enable

https://t.me/learningnets

the Internet to function.

TCP/IP (Transmission Control Protocol/Internet Protocol) Communication protocols developed by the U.S. Department of Defense to enable dissimilar computers to share information over a network; default networking rules in most networks.

teleconference Teleconferencing means having a conference (meeting) via telephone, but the term has come to mean having a video-enabled remote business meeting.

telepresence Telepresence is a step up from teleconferencing; it uses sophisticated, high-quality video-conferencing equipment to create an immersive environment where the remote user feels almost present at the meeting.

test the theory Attempt to resolve the issue by either confirming the theory and learning what needs to be done to fix the problem or by not confirming the theory and forming a new one or escalating. This is step 3 of 6 in the CompTIA troubleshooting theory. (*See also* troublehooting theory.)

tethering The act of using a cellular network–connected mobile device as a mobile hotspot.

theory of probable cause One possible reason why something is not working; a guess.

thermal paste A heat conductive paste used to hold heat sinks to heat generating chips.

thermal printer Printer that uses heated printheads to create high-quality images on special or plain paper.

thick client CompTIA's name for a standard desktop computer. This runs desktop applications and meets recommended requirements for selected OS.

thin client A system designed to handle only basic applications with an absolute minimum amount of hardware required by the operating system. This meets minimum requirements for selected OS.

Thunderbolt An open standards connector interface that is primarily used to

https://t.me/learningnets

connect peripherals to devices, including mobile devices, if they have a corresponding port.

Time Machine The macOS full backup tool that enables you to recover some or all files in the event of a crash; it also enables you to restore deleted files and recover previous versions of files.

TKIP (Temporal Key Integrity Protocol) Deprecated encryption standard that provided a new encryption key for every sent packet.

token A multifactor authentication item (such as a unique code displayed in a hardware or software token device or app) in addition to other items (such as a username and password) used for authentication.

toner A fine powder made up of plastic particles bonded to iron particles, used to create the text and images on a laser printer. Also, this is a generic term for two devices used together—a tone generator and a tone locator (probe)—to trace cables by sending an electrical signal along a wire at a particular frequency. The tone locator then emits a sound when it distinguishes that frequency.

toner cartridge Object used to store the toner in a laser printer. (*See also* laser printer; toner.)

topology The way computers connect to each other in a network.

touch interface The primary user interface on modern mobile devices where keys are replaced with tactile interaction.

touchpad Flat, touch-sensitive pad that serves as a pointing device for most laptops.

touchscreen Monitor with a type of sensing device across its face that detects the location and duration of contact, usually by a finger or stylus.

traces Electrically conductive metal pathways embedded into the circuit board.

trackball A mouse with a ball atop the device where you can manipulate it with a finger to move the cursor.

trademark A unique design that identifies a product or company.

https://t.me/learningnets

transfer rate Rate of data transferred between two devices, especially over the expansion bus.

Trojan horse Program that does something other than what the user who runs the program thinks it will do. This is used to disguise malicious code.

troubleshooting theory Steps a technician uses to solve a problem. CompTIA A+ defines six steps: identify the problem; establish a theory of probable cause; test the theory to determine cause; establish a plan of action to resolve the problem and implement a solution; verify full system functionality and, if applicable, implement preventive measures; and document findings, actions, and outcomes.

UAC (User Account Control) Windows feature that enables standard accounts to do common tasks and provides a permissions dialog box when standard and administrator accounts do certain things that could potentially harm the computer (such as attempt to install a program).

UEFI (Unified Extensible Firmware Interface) Consortium of companies that established the UEFI standard that replaced the original EFI standard.

Ultra DMA Hard drive technology that enables drives to use direct memory addressing. Ultra DMA mode 3 drives—called ATA/33—have data transfer speeds up to 33 MBps. Mode 4 and 5 drives—called ATA/66 and ATA/100, respectively—transfer data at up to 66 MBps for mode 4 and 100 MBps for mode 5. Mode 6 pushed the transfer rate to 133 MBps. Modes 4, 5, and 6 require an 80-wire cable and a compatible controller to achieve these data transfer rates.

Ultrabook Thin, powerful laptop powered by Intel processors and built according to the Intel design specification. Competes directly with the Apple MacBook Air.

unattended installation A type of OS installation where special scripts perform all the OS setup duties without human intervention.

unauthorized access Anytime a person accesses resources in an unauthorized way. This access may or may not be malicious.

unbuffered RAM RAM without a buffer chip; in other words, normal, consumer-grade RAM.

https://t.me/learningnets

UNC (Universal Naming Convention) Describes any shared resource in a network using the convention \\<*server name*>\<*name of shared resource*>.

unicode A standard used to represent characters from most spoken languages on any computer platform.

unit testing The testing of a small portion of software code.

update Individual fixes for Windows that come out fairly often, on the order of once a week or so.

UPS (uninterruptible power supply) Device that supplies continuous clean power to a computer system the whole time the computer is on. Protects against power outages and sags.

URL (uniform resource locator) An address that defines the location of a resource on the Internet. URLs are used most often in conjunction with HTML and the World Wide Web.

USB (universal serial bus) General-purpose serial interconnect for keyboards, printers, joysticks, and many other devices. It enables the hot-swapping of devices.

USB host controller Integrated circuit that is usually built into the chipset and controls every USB device that connects to it.

USB hub Device that extends a single USB connection to two or more USB ports, almost always directly from one of the USB ports connected to the root hub.

USB thumb drive Flash memory device that uses the standard USB connection.

user account Container that identifies a user to an application, operating system, or network, including name, password, username, groups to which the user belongs, and other information based on the user and the OS being used. This usually defines the rights and roles a user plays on a system.

user interface Visual representation of the computer on the monitor that makes sense to the people using the computer, through which the user can interact with

https://t.me/learningnets

the computer. This can be a graphical user interface (GUI) like Windows 7 or a command-line interface like the Windows PowerShell or the Recovery Console.

variable Programmer-defined name for storing data during program execution.

vector Computer programming data type term with the same meaning as *array*. A vector format is used for line drawings. It uses math formulas to describe each line and curve in the image.

verify full system functionality Making sure that a problem has been resolved and will not return. This is step 5 of 6 in the CompTIA troubleshooting theory. (*See also* troublehooting theory.)

video card Expansion card that works with the CPU to produce the images displayed on your computer's display. This is also called a *display adapter*.

video display *See* monitor.

video graphics array (VGA) connector An older analog video connector; it has 15 pins, laid out in three rows of five.

virtual assistant Voice-activated technology that responds to user requests for information. Virtual assistants can be used to search the Internet, make reminders, do calculations, and launch apps.

virtual hard drive A file used by a virtual machine; the file serves as a storage device would to a physical computer.

virtual machine (VM) A complete environment for a guest operating system to function as though that operating system were installed on its own computer.

virtual machine manager (VMM) *See* hypervisor.

virtualization Presenting underlying physical network, storage, or compute hardware to be used by higher-level implementations such as virtual machines.

virus Program that can make a copy of itself without your necessarily being aware of it. Some viruses can destroy or damage files. The best protection is to back up files regularly.

https://t.me/learningnets

VoIP (Voice over Internet Protocol) Collection of protocols that makes voice calls over a data network possible.

volts (V) Measurement of the pressure of the electrons passing through a wire, or voltage.

VPN (Virtual Private Network) Encrypted connection over the Internet between a computer or remote network and a private network.

WAN (wide area network) Two or more LANs connected together; also referred to as a *remote network*.

WAP (wireless access point) Device that centrally connects wireless network nodes.

water block Liquid cooling systems attach heat sinks (sometimes called *water blocks*) to each of the chips that get hot in the PC.

wattage (watts or W) Measurement of the amps and volts needed for a particular device to function.

web browser Program designed to retrieve, interpret, and display web pages.

web server A computer that stores and shares the files that make up web sites.

webcam PC camera most commonly used for Internet video.

WEP (Wired Equivalent Privacy) Wireless security protocol that uses a standard 40-bit encryption to scramble data packets. It does not provide complete end-to-end encryption and is vulnerable to attack.

wide area network (WAN) A widespread group of computers connected using long-distance technologies.

WiFi Common name for the IEEE 802.11 wireless Ethernet standard.

WiFi Protected Setup (WPS) A standard included on many WAPs and clients to make secure connections easier to configure.

Windows Explorer Windows utility that enables you to manipulate files and

https://t.me/learningnets

folders stored on the drives in your computer. This has been rebranded as File Explorer in Windows 8, 8.1, and 10.

Windows PowerShell Command-line tool included with Windows. It offers a number of powerful scripting tools for automating changes both on local machines and over networks.

Windows Update Microsoft application used to keep Windows operating systems up-to-date with the latest patches or enhancements. (*See also* Automatic Updates.)

wireless local area network (WLAN) Small group of computers that connect via Wi-Fi.

wireless security A system of authentication for wireless clients that connect to a SOHO router. (*See also* WEP [Wired Equivalent Privacy]; WPA [Wi-Fi Protected Access]; WPA 2 [Wi-Fi Protected Access 2].)

workgroup A simple, decentralized network that Windows PCs are configured to use by default. The purpose is to organize networked Windows PCs similar to how folder are used to organize files on storage media.

worm Special form of virus. Unlike other viruses, a worm does not infect other files on the computer. Instead, it replicates by making copies of itself on other systems on a network by taking advantage of security weaknesses in networking protocols.

WPA (Wi-Fi Protected Access) Wireless security protocol that uses encryption key integrity-checking/TKIP and EAP and is designed to improve on WEP's weaknesses. This has been supplanted by WPA 2.

WPA 2 (Wi-Fi Protected Access 2) Wireless security protocol, also known as IEEE 802.11i. This uses the Advanced Encryption Standard (AES) and replaces WPA.

x64 Describes 64-bit operating systems and software.

x86 Describes 32-bit operating systems and software.

https://t.me/learningnets

INDEX

Please note that index links point to page beginnings from the print edition. Locations are approximate in e-readers, and you may need to page down one or more times after clicking a link to get to the indexed material.

Numbers

2.1 speaker system, 78–79
3G cellular networks, 164
3.5-mm audio
    audio devices, 77–78
    physical connections for desktop PC, 142
    ports/connectors, 65–66
4G cellular networks, 164
32-bit computing, 42, 110
64-bit computing, 42, 110
80-wire ribbon cable, hard drives, 95–96
802.11ac standard, wireless SOHO routers, 249

A

AC (alternating current), 52, 140–141
accelerometer, mobile device kinetics, 159
acceptance testing, 374
access control, mitigating physical security threats, 280
access methods, database, 359
access points. *See* WAPs (wireless access points)
accessibility options, operating systems, 130–131
account IDs, mobile devices, 162
accounts
    creating user, 149–150

https://t.me/learningnets

operating system setup, 145
using appropriate types of, 283–284
activation, of applications, 236
active cooling, CPU power/heat management, 45
active hours, changing in Windows Update, 297
ad hoc networks, 99, 248
Add Printer Wizard, 342
Administrator account
automating tasks, 370
User Account Control when signed in to, 287
using appropriate account types, 283
Advanced options, Windows Update, 297
Advanced Sharing dialog, sharing folders, 269–270
adware, 289–291
AES (Advanced Encryption Standard), SOHO router security, 256, 257
airplane mode, configuring mobile devices, 170–171
all-in-one printers. *See* MFDs (multifunction devices)
alternating current (AC), 52, 140–141
Amazon Kindle, e-book reader, 20
AMD (Advanced Micro Devices), 40, 51
Android
account IDs and passwords, 162
airplane mode, 171
categorizing smartphones by OS, 19
e-mail configuration, 171
enabling Wi-Fi on mobile devices, 168
finding/installing apps, 174–175
forcing frozen apps to exit on smartphones, 341
hard reset, 177
lost device security, 162–163
mobile device interface, 155–158
mobile device operating systems, 154
operating systems for mobile devices, 21
pairing via Bluetooth, 165
passcode, 160–161
removing apps, 175

https://t.me/learningnets

running applications on smartphones, 212–213
sharing cellular connections between mobile devices, 170
soft reset, 176
synchronizing devices, 172
synchronizing photos, 172–173
synchronizing with computer, 173
transferring data via Bluetooth, 167
anti-malware programs
malware prevention tips, 299
protection against malware, 298
removing adware with, 291
antistatic vacuums, cleaning inside PC, 328–329
antistatic wrist strap, avoiding ESD, 139, 327–328
antivirus program. *See* anti-malware programs
Apple
ID and passwords, 162
iOS. *See* iOS
Mac. *See* macOS
applications (apps)
audio and video formats, 230–232
business software, 226–227
collaboration software, 226
compression formats, 229–230
document formats, 233–234
executables, 228
executing, 125–126
exiting, 214
FaceTime as example of, 9
file types, 228
forms of programming, 7
image formats, 231–233
installing, 215
installing desktop application in macOS, 217
installing desktop application in Windows OS, 215–217
installing from online store, 217–218
installing to/removing from mobile devices, 174–175

https://t.me/learningnets

licensing, 234–236
mobile, 27
platforms and types, 224
product keys and activation, 236
productivity software, 225
removing Chrome, 224
removing in Windows OS, 221
removing Linux, 223
removing macOS, 221–222
removing Windows desktop, 220–221
resource sharing, 26
review answers, 239
review, chapter, 237
review questions, 237–238
running, 207–208
running in Chrome OS, 212
running in Linux OS, 211–212
running in macOS, 210–211
running in Windows OS, 208–210
running on smartphones, 212–213
saving your work, 213–214
specialized software, 228
switching between, 213
troubleshooting frozen, 340–341
updating, 219–220
utility software, 226–227
web, 27–29
web-based, 218–219
APs (access points). *See* WAPs (wireless access points)
archive files, compressed, 216, 229–230
arguments, functions and, 382
ARM (Azure Resource Manager) database templates, 357
aspect ratio, flat-panel displays, 68
assembly programming language, 371
associations, file extensions and, 192
ATMs (automated teller machines), 32

https://t.me/learningnets

attributes (flags). *See also* properties
advanced file, 187–188
basic file, 187
folder, 188
viewing/modifying properties, 189–191
attributes, object, 379
ATX, motherboard form factors, 50–51
audio
accessibility options, 130
devices, 77–79
formats, 230–232
operating system setup, 144
sound cards, 60
authentication
SOHO routers, 255–258
user, 284–286
Autocomplete section, Internet Explorer, 312
autofill, disabling forms, 312
automated teller machines (ATMs), 32
automation, of administrative tasks, 370
availability, Internet connectivity options for, 261
AWS (Amazon Web Services)
creating database with CloudFormation templates, 357
data replication services, 202
saving work to cloud, 214
Azure Resource Manager (ARM) database templates, 357

B

backups
overview of, 201
schedules and frequency, 202–203
storage media, 203
techniques, 201–202
verification and testing, 203
Balanced power plan, PC power management, 322–323

https://t.me/learningnets

ball mice, input devices, 77
banner ads, 306, 307
Barnes & Noble Nook, e-book reader, 20
Bash shell scripting language, Linux, 370
Basic Input Output System (BIOS), motherboard firmware, 51
batteries
    troubleshooting peripherals, 342
    troubleshooting physical damage, 338
    troubleshooting power, 337
BDs (Blu-ray Discs), 91–92
Better Business Bureau, trusted sites and, 303
big data, NoSQL databases for, 356–357
BIOS (Basic Input Output System), motherboard firmware, 51
birthdate, limiting online use of PII, 307
BitLocker, hardening hard drives, 282
bits, file and disk storage capacity, 89
BlackBerry
    operating systems for mobile devices, 22
    transferring data via Bluetooth, 167
blackouts, ensuring reliable AC power, 140
bloatware, uninstalling unneeded software, 148
blocking spam, with filters, 292
Blu-ray Discs (BDs), 91–92
Bluetooth sound connectivity
    ad hoc networks, 99
    pairing mobile devices, 165–167
    transferring data, 167–168
    Wi-Fi transmission range vs., 78
    wireless connectivity and, 164
book scanners, 79
botnets, DDoS attacks and, 301
branching out, of loops, 381
bricking devices, DoS attacks, 301
broadband box (cable or other), SOHO, 247–248, 250
broadband connection, SOHO networks, 247–248
browsers

https://t.me/learningnets

adjusting security settings, 308–309
clearing cookies, 309–310
clearing history and temporary Internet files, 311
disabling autofill forms and passwords, 312
disabling unneeded plug-ins, toolbars, and extensions, 312
updating, 307–308
browsing best practices
browser security/privacy settings, 308–312
firewalls, 312–313
limiting online use of PII, 307
recognizing invalid certificate warnings, 304
recognizing secure Web sites, 303
recognizing suspicious banner ads, 306–307
recognizing suspicious links, 304–306
recognizing untrusted source warnings, 304–305
risks of public workstations, 302–303
updating browsers and plug-ins, 307–308
bundled software, licensing and, 234
bus (clock) speed, motherboards, 41–42
business software, 226–227
bytes, file size/disk storage, 89–90

C

C programming language, 371
cables
routers sending communications via, 25
troubleshooting peripherals, 341
troubleshooting power, 337
cabling
ad hoc networks, 99
LANs, 23
managing, 143–144
cache, CPU memory, 43
CAD (computer-aided design), 228
capacitive screens, touchscreens, 74

https://t.me/learningnets

card readers, solid-state storage, 93
case fans, CPU power and heat management, 44–45
cathode ray tubes (CRTs), 68–69
CCFLs (cold cathode fluorescent lamps), 66
CDs (compact discs)
    installing applications from, 215
    optical storage media, 91–92
cellular networks
    Internet connectivity strengths/weaknesses, 259–263
    sharing connections between mobile devices, 170
    for smartphones and tablets, 259
    wireless connectivity and, 164
central processing units. *See* CPUs (central processing units)
certificates
    database security with SSL/TLS, 360
    recognizing invalid warnings on sites, 304
    recognizing untrusted source warnings, 304–305
CGI (computer generated imagery), supercomputers, 9
chairs, ergonomic, 138
Change plan settings, PC power plan, 322–323
chipsets, motherboard, 50
Chrome OS
    based on Linux, 17
    comparing OS interfaces, 121–124
    cross-referencing features, 124
    exiting applications, 214
    file management, 127
    hotkeys, 129
    overview of, 18
    removing apps, 224
    running applications in, 212
    screenshots, 130
    switching between applications, 213
CIR (committed information rate), satellites, 260
CLI (command line interface)
    interface options in OSs, 13–14

https://t.me/learningnets

OS as interface between user/machine, 107
running Linux applications, 211
client-server networks, 244–245
clients
network, 26
remote access and, 27
SOHO router connectivity for wireless, 258–259
types of devices for, 244
understanding, 244–246
Clipboard, moving/copying files and folders, 194
cloud computing
cloud storage, 99–100
creating databases with templates in, 357
database storage performance, 354
managed services for databases, 353
overview of, 28–29
platform types, 224
saving work to cloud, 213–214
synchronizing devices via, 172
web-based applications as, 218–219
CloudFormation database templates, AWS, 357
code repository, tracking changes in larger projects, 373–374
codebook, CPU preset commands as, 43
codecs (compressor-decompressor), audio/video formats, 230
coding phase, SDLC, 370–373
cold cathode fluorescent lamps (CCFLs), 66
collaboration
software, 29
via cloud-based services, 29
columns (fields)
building on fields to speed up searching, 353
database table structure, 352–353
database tables and, 351–352
command line interface. *See* CLI (command line interface)
commercial software, licensing and, 235
committed information rate (CIR), satellites, 260

https://t.me/learningnets

community groups, getting help from, 345
compact discs (CDs)
installing applications from, 215
optical storage media, 91–92
CompactFlash, memory card formats, 93
compiled programming languages, 370–373
complexity
operating system, 110
password, 285
component (RGB) video, 71–73
components, motherboard, 51
composite video, 71–72
compressed air, cleaning inside PC, 328
compressed archive files, 216, 229–230
compression formats, 229–230
compute power, database scalability and, 353–354
computer-aided design (CAD), 228
computer generated imagery (CGI), supercomputers, 9
computer maintenance and management
disaster recovery, 331
environmentally aware disposal, 330–331
overview of, 319
review answers, 334
review, chapter, 331–332
review questions, 332–333
computer maintenance and management, hardware
avoiding ESD, 327–328
cleaning inside, 328–329
cleaning inside desktop PC, 326–327
cleaning monitors and removable media, 326
proper cleaning materials, 325–326
ventilation, dust, and moisture control, 329–330
computer maintenance and management, power
choose energy-efficient devices, 320
choosing actions for power buttons/closing lid, 325
leaving PC running, 320

https://t.me/learningnets

low-power modes, 321–322
power plans, 322–324
shut down PC, 320–321
computers
cloud computing, 28–29
data assets, 8
data storage, 8
dedicated, 10–11
desktop and laptop, 11–13
features common to, 4–7
IoT devices, 7
mobile apps, 27
mobile devices, 18–20
multi-user, 9–10
networking, 23–25
OSs for desktops and laptops, 13–18
OSs for mobile devices, 21–23
overview of, 3–4
processors, 7
programming, 7
remote access, 27
resource sharing, 26
review answers, 36–37
review, chapter, 33–34
review questions, 34–36
servers, 26
software and apps, 8–9
specialized systems, 31–33
streaming media, 27
virtualization, 29–31
web apps, 27–29
concurrent license, 236
conditional execution, program flow, 380–381
confidentiality, password, 285–286
configuration utility, SOHO router, 250–252
connectivity

https://t.me/learningnets

database, 358–359
Internet. *See* Internet connectivity
Internet delay/latency, 262
setting up desktop PC, 142–143
setting up desktop PCs with physical, 142–143
wired. *See* wired connectivity
wireless. *See* wireless connectivity
constants, programming with, 376–378
Contact us link, tech support web site, 344
container files, video, 231
contingency plans, disaster recovery, 331
continuous improvement, SDLC, 367
Control Panel, checking for adware, 290–291
control, workgroups lack central, 266
cookies, clearing, 309–310
copying files, 192–194, 202
copyright protection, DRM, 231
CPUs (central processing units)
features, 42–43
motherboard features, 51
overview, 40
power and heat management, 43–46
speed of, 40–42
CREATE DATABASE, manually, 357
creation methods, database, 357–358
crossover cables, 99, 249
CRTs (cathode ray tubes), 68–69
CRUD (create, read, update, delete) database management, 358
cut-and-paste, moving/copying files/folders, 193–194
cycles, CPU speed and, 40

D

daemons (services), operating systems, 126–127
DAS (direct attached storage), 94
data

https://t.me/learningnets

built from 1s and 0s, 3
destruction, 279
manipulating in databases, 360–362
NoSQL database for big, 356–357
populating data tables with, 352
process of flow through computers, 39
recovering after hard reset, 177
replication, for backup, 202
transferring via Bluetooth, 167–168
data assets, 8
data storage
database scalability for current/future, 353–355
local storage, 94–97
magnetic storage, 90–91
managing file storage, 181
network storage, 97–99
online storage, 99–101
online storage for backups, 202
optical storage, 91–92
overview of, 8
review answers, 103–104
review, chapter, 101
review questions, 102–103
solid-state storage, 93–94
technologies, 89–90
via databases. *See* databases
data types, software development and, 376–378
databases
concepts, 351–352
connectivity, 358–359
creation methods, 357–358
getting data into, 360
NoSQL, 356–357
query and report builder tools, 361–362
querying and removing data, 361
relational, 355–356

https://t.me/learningnets

review answers, 365
review, chapter, 362–363
review questions, 363–365
scalability, 353–355
security, 360
structures, 355
table structure, 352–353
daylight savings, operating system setup, 144
DC (direct current), power supplies and, 52
DCs (domain controllers), Active Directory, 266
DDoS (distributed denial-of-service) attacks, 301
DDR (double data rate) RAM, 49, 51
DE (desktop environment), Linux OS, 17
dedicated computers, 10–11
defense, against spam, 292
definition file, malware prevention tips, 299
deleting
browsing history in Internet Explorer, 311
files and folders, 195–197
Dell plan, PC power management, 322–323
Dell Product Support site, 343–345
denatured alcohol, cleaning keyboards, 326
denial-of-service (DoS) attacks, 301
deployment phase, SDLC, 375
design phase, SDLC, 369–370
desk chair, ergonomics, 138
desktop applications. *See also* applications (apps)
installing in macOS, 217
installing in Windows OS, 215–217
removing in macOS, 221–222
removing in Windows OS, 220–221
desktop computers
operating systems, 13–18
overview of, 11–12
physical connections, 142–143
types of platforms, 224

https://t.me/learningnets

desktop environment (DE), Linux OS, 17
device hardening, mitigating physical security threats, 280–283
Devices and Printers applet, sharing local printer on LANs, 273
devices, types of client, 244
digital products, 8
digital rights management (DRM), copyright protection, 231
digital subscriber line (DSL), network communications via, 25
digital versatile discs (DVDs), 91–92, 215
Digital Video Interface (DVI)
    monitor connectors and ports, 70
    setting up desktop PC connections, 142
digitizer, touchscreens, 74
DIMMs (dual inline memory modules), and RAM, 47–49
direct attached storage (DAS), 94
direct current (DC), power supplies and, 52
direct link connection, 248–249
directories
    file and folder structure, 181
    operating system functions, 108
    root directory, 182
disaster recovery
    contingency plans, 331
    disaster recovery plans (DRP), 331
    incident response plans (IRPs), 331
disk drives
    hard drives. *See* hard drives
    measuring file and disk storage capacity, 89
display adapters, types of expansion cards, 60
display screen, troubleshooting physical damage, 338
displaying files, changing view, 197–199
DisplayPort
    monitor connectors and ports, 73
    setup desktop PC connections, 142
displays. *See* monitors
disposal, environmentally aware computer, 330–331
distributed denial-of-service (DDoS) attacks, 301

https://t.me/learningnets

distro, Linux versions, 17
document databases, NoSQL, 357
document formats, application file types, 233–234
document scanners, 79
documentation, help from, 343
domain controllers (DCs), Active Directory, 266
domain name, suspicious links on URL and, 304–306
domains, network organization via, 266
DoS (denial-of-service) attacks, 301
dot-matrix printers, 81
double data rate (DDR) RAM, 49, 51
double taps, mobile devices gestures, 158
downloads
    compressed archive file, 216
    streaming media, 27
drag-and-drop, files and folders, 192–193
DRAM (dynamic RAM), 47
drawing tablets, as input devices, 76–77
drive covers, well-maintained computers, 329–330
DRM (digital rights management), copyrights, 231
Dropbox, cloud storage, 99–100
dropped computer, troubleshooting damage, 338
DSL (digital subscriber line), network communications, 25
dual-core architecture, CPUs, 42
dumb terminals, 27
dumpster diving, unauthorized access, 278–279
dust control
    cleaning inside PC, 326, 328
    in well-maintained computers, 329
DVDs (digital versatile discs), 91–92, 215
DVI (Digital Video Interface)
    monitor connectors and ports, 70
    setting up desktop PC connections, 142
dynamic RAM (DRAM), 47

https://t.me/learningnets

E

e-book readers, 20
e-mail
    configuring mobile devices, 171–172
    deleting spam, 292
    limiting online use of PII, 307
EAP (Extensible Authentication Protocol), SOHO router wireless security, 256
Ease of Access Center, Windows OS, 131
eavesdropping, as network threat, 300
Edge, InPrivate Browsing, 310
Edit Plan Settings, power plan for PC, 322–324
editing files, 191–192
education, in malware recovery, 300
electromagnetic interference (EMI), avoiding, 139–140
electronic spray cleaner, computer hardware, 325
electrostatic discharge (ESD), avoiding, 138–139, 327
email, limiting online use of PII, 307
email phishing, social engineering, 294–295
EMI (electromagnetic interference), avoiding, 139–140
eMMC (embedded multimedia controllers), smartphones/tablets, 93
encryption
    device hardening via, 282–283
    ransomware, 297
    wireless security for SOHO router, 255–258
End User License Agreement (EULA), 109, 234
energy-efficient devices, power management, 320
Energy Star logo, energy-efficient devices, 320
environmentally aware computer disposal, 330–331
ergonomics, work area, 136–138
eSATA (external SATA), 65–66, 96–97
escalation, malware recovery process, 300
ESD (electrostatic discharge), avoiding, 138–139, 327
Ethernet cable, SOHO router, 250
Ethernet ports (RJ-45), 142, 250
EULA (End User License Agreement), 109, 234

https://t.me/learningnets

executable (EXE) file
as application file type, 228
compiled languages, 370
executing programs, OSs, 125–126
exiting applications, 214
expansion cards, 59–61, 85–88
expansion slots
motherboard features, 51
review, 85–88
types of, 61–62
expiration, password, 286
EXT4 (Extended Filesystem, version 4), 187
Extensible Authentication Protocol (EAP), SOHO router, 256
extensions, disabling unneeded browser, 312–313
external SATA (eSATA), 65–66, 96–97

F

fans, CPU, 44–45
FAQs (Frequently Asked Questions), technical support web sites, 344
fax machines, 84–85
features, device hardening by enabling, 282
File and Printer Sharing settings, 263–264
File Explorer. *See* Windows Explorer/Windows File Explorer
file extensions
associations and, 192
displaying, 195
file management
backup and restore, 201–203
deleting/undeleting files and folders, 195–197
file and folder size, 188–189, 191
file attributes, 187–188
folder attributes, 188
folders and paths, 181–183
keywords, 189
moving and copying files, 192–194

https://t.me/learningnets

navigating file structure, 185–187
opening, editing, saving files, 191–192
operating systems and, 127
permissions, 200–201
renaming files and folders, 194–195
review answers, 206
review, chapter, 204
review questions, 204–205
searching, sorting, and displaying files, 197–199
storage, 181
tools for, 183–185
uneditable properties, 188–189
viewing/modifying properties, 189–191
file path, 182
file servers, linking PCs, 10
File Sharing dialog, sharing folders, 269–271
File Transfer Protocol (FTP), 100
file types
audio and video formats, 230–232
compression formats, 229–230
document formats, 233–234
executables, 228
image formats, 231–233
overview of, 228
files
data organized by, 8
managing. *See* file management
measuring size as bits and bytes, 89
resource sharing, 26
sharing in workgroups, 265
sharing printers and, 263–264
transferring via FTP, 100
web-based downloads and storage of, 101
Files utility, Linux, 185
FileZilla
removing applications, 221

https://t.me/learningnets

transferring files via FTP, 100
updating applications, 219–220
filters, spam, 292
Finder utility, macOS file management, 184
fine-tune PC power plan, 323–324
firewalls, best practices, 312
FireWire (IEEE 1394)
external storage, 96–97
ports/connectors, 65–66
printer port/connectors, 85
firmware
motherboard features, 51
updating SOHO router, 254–255
first-party cookies, 310
flags. *See* attributes (flags)
flash memory, solid-state storage, 93
flat-file storage, 351
flat-panel displays (FPDs), 66–68
flatbed scanners, 79
fluorescent lighting, as source of EMI, 140
folders. *See also* file management
adding to homegroup, 268
attributes, 188
deleting/undeleting, 195–197
renaming, 194–195
resource sharing, 26
sharing in workgroups, 265
size of, 188–189, 191
understanding, 181–183
for loops, 377
Force Quit, frozen apps in macOS, 340
foreign keys, relational databases, 356
form factors, motherboard, 50–51
forms, disabling autofill, 312–313
FPDs (flat-panel displays), 66–68
freemium, licensing and, 235

https://t.me/learningnets

freeware, licensing and, 235
Frequently Asked Questions (FAQs), tech support, 344
friction feed mechanism, inkjet printers, 81
FTP (File Transfer Protocol), 100
FTPS (FTP over SSL), 100
function keys, keyboard, 74
functions, program flow, 382

G

Gb (gigabytes), file size/disk storage, 89–90
gestures, mobile device configuration, 158–159
Get-Service cmdlet, PowerShell, 370
GHz (gigahertz), CPU speed, 40
GitHub code repository, larger projects, 373–374
glass cleaner, for computer hardware, 325
Global Positioning System (GPS), 20, 32–33
Google Account, account IDs and passwords, 162
Google Drive, cloud storage, 99–100, 214
GPS (Global Positioning System), 20, 32–33
Graph API programming language, 373
Guest account, 283
GUI (graphical user interface) tools
    interface options in OSs, 13
    manual database creation, 357
    OS as interface between user and machine, 107
    query/report builder tools based on, 361–362
    running applications in Linux, 211
gyroscope, mobile device kinetics, 159

H

hands-free calling, 165
hard disk drives. *See* HDDs (hard disk drives)
hard drives
    threat mitigation by encrypting, 282
    troubleshooting physical damage, 338

https://t.me/learningnets

hard reset, mobile devices, 177
hardening database server, 360
hardware. *See also* system hardware
    choosing OS based on platform, 13
    connecting to, 127–128
    defined, 8
    operating system functions, 108
    Plug and Play, 128
    SDLC design phase requirements, 369
    system. *See* system hardware
    troubleshooting apps, 340
hardware maintenance, computer
    avoiding ESD, 327–328
    cleaning inside, 328–329
    cleaning inside desktop PC, 326–327
    cleaning monitors and removable media, 326
    proper cleaning materials, 325–326
    review answers, 334
    review, chapter, 331–332
    review questions, 332–333
    ventilation, dust, and moisture control, 329–330
hashes, activating applications, 236
HDDs (hard disk drives)
    data storage, 27
    files servers and, 97
    magnetic storage, 90–91
HDMI (High Definition Multimedia Interface)
    desktop PC connections, 142
    monitoring connectors and ports, 70
heat management, CPUs, 43–46
heat sinks, CPUs, 44, 46
help, getting
    Internet searches and community groups, 345
    manufacturer documentation and web sites, 343–344
    overview of, 342
    review answers, 348

https://t.me/learningnets

review questions, 347
technical support, 344–345
hertz (Hz), measuring CPU speed in, 40
hexa-core architecture, CPU features, 42
HFS (Hierarchical File System), 187
Hi-Speed USB, 63
Hibernate
PC power management, 321–322
putting PC into, 323, 325
troubleshooting low-power mode, 337
Hierarchical File System (HFS), 187
High Definition Multimedia Interface (HDMI)
desktop PC connections, 142
monitoring connectors and ports, 70
High performance power plan, PC power, 322–323
high-privacy settings, public workstations, 302–303
history, clearing browser, 311
home media servers, NAS, 98
home page redirection, caused by adware, 289
HomeGroup applet, 267, 268
homegroups, 266–267
horizontal scaling, databases, 353
hotkeys, navigating with, 128–129
HTML programming language, 372
http:// (HTTP over SSL), secure Web site, 303
HTTP (HyperText Transfer Protocol), web-based file downloads and storage, 101
HTTPS (HTTP over SSL), web-based file downloads and storage, 101
humidity, room conditions for PC setup, 136
HVAC (heating, ventilation, and air conditioning), room conditions for PC setup, 135
hypervisors, Type 1 and Type 2, 29
Hz (hertz), measuring CPU speed in, 40

I

https://t.me/learningnets

I/O (input/output) devices
audio devices, 77–79
digital cameras, 80
imaging devices, 79
overview of, 77
printers/fax machines, 81–85
review answers, 88
review, chapter, 85–86
review questions, 86–87
scanners, 79
IBM platform, 13
iCloud
cloud storage, 99–100
managing lost devices, 163–164
synchronizing photos, 172–173
IEEE
802.11. *See* Wi-Fi (wireless fidelity)
1394. *See* FireWire (IEEE 1394)
image formats, application file type, 231–233
imaging devices, 79, 80
imaging software, backups, 202
IMDB (In-Memory Database) cache, 355
impact printers, 81
in-memory cache, 355
In-Memory Database (IMDB) cache, 355
incident response plans (IRPs), disaster recovery, 331
infiltration, social engineering, 293–294
infrared (IR), wireless keyboards, 75
inherence factor, multifactor authentication, 284
inkjet printers, 81, 83
InPrivate Browsing, public workstations, 302–303
input, data flow through computers, 39
input devices
keyboards, 74–76
overview of, 74
pointing devices, 76–77

https://t.me/learningnets

review answers, 88
review, chapter, 85–86
review questions, 86–87
input/output devices. *See* I/O (input/output) devices
inside PC, cleaning
avoiding ESD, 327–328
blowing or vacuuming dust out, 328–329
overview of, 326–327
installing applications
desktop application in macOS, 217
desktop application in Windows OS, 215–217
from online store, 217–218
overview of, 215
instruction sets, CPU, 43
Intel
choosing OS based on hardware platform, 13
motherboard features, 51
types of CPUs, 40
intellectual property (IP), 8
interface
command-line. *See* CLI (command line interface)
graphical. *See* GUI (graphical user interface) tools
mobile devices, 155–158
SOHO router configuration, 251–252
Internet
operating system setup, 144
as remote network, 24
searches, 345
setting up desktop PC connections, 142
verifying and configuring connection, 145
Internet cache, clearing cookies, 309–310
Internet connectivity
cellular, 259
overview of, 128
review answers, 276
review, chapter, 273–274

https://t.me/learningnets

review questions, 274–275
satellite, 259–260
strengths and weaknesses of, 259–263
using SOHO router for, 250
verifying wireless, 250
wired. *See* wired connectivity
wireless. *See* wireless connectivity
Internet Explorer
clearing history and Temporary Internet Files, 311
disabling autofill for forms and passwords, 312
handling first-party/third-party cookies, 310
InPrivate Browsing, 302–303
security zones, 308
Internet of Things (IoT) devices
configuring peripherals, 147
examples of, 7
Internet Service Providers (ISPs), 246–247, 249
interpreted (scripted) languages
common types of, 370–373
compiled code vs., 370
creating database with, 357
IOPS (input and output operations per second), database storage performance, 354
iOS. *See also* iPhone
airplane mode, 171
controlling screen orientation, 159
e-mail configuration, 171–172
enabling Wi-Fi on mobile devices, 168
finding/installing apps, 174–175
hard reset, 177
mobile device operating systems, 154
operating systems for mobile devices, 21
pairing via Bluetooth, 165–166
removing apps, 175
running applications on smartphones, 212–213
sharing cellular connections, 170

https://t.me/learningnets

soft reset, 176–177
synchronization of devices, 172
synchronizing photos, 172–173
synchronizing with computer, 173
transferring data via Bluetooth, 167
understanding mobile device interface, 155–158
iOS 11.*x*, forcing frozen apps to exit, 341
IoT (Internet of Things) devices
configuring peripherals, 147
examples of, 7
IP addresses
configuring SOHO router, 251
evaluating URL for suspicious links, 304
IP (intellectual property), 8
iPads, 19
iPhone
account IDs and passwords, 162
categorizing smartphones by OS, 19
features, 4–5
managing lost device security, 163–164
pairing via Bluetooth, 165
passcode, 160–161
understanding interface, 155–158
IR (infrared), wireless keyboards, 75
IRPs (incident response plans), disaster recovery, 331
ISDN lines, 25
ISO files, installing applications, 215
ISPs (Internet Service Providers), 246–247, 249
IT security threat mitigation
being smart Web user, 301–308
browser security/privacy settings, 308–313
local security threats, 278–280
malware. *See* malicious software (malware)
malware protection, 297–300
network threats, 300–301
overview of, 277

https://t.me/learningnets

physical security, 280–283
review answers, 316–317
review, chapter, 314
review questions, 315–316
users and passwords, 283–288
IT troubleshooting
apps run but sometimes freeze, 340–341
apps will not install or run, 340
getting help, 342–345
methodology (steps), 335–336
no power, 336–337
overview of, 335
peripherals will not work, 341–342
physical damage, 337–338
review answers, 348
review, chapter, 346
review questions, 346–347
start up is abnormal, 338–340

J

Java programming language, 371
JavaScript programming language, 372
joysticks, input devices, 76–77

K

Kb (kilobytes), file size/disk storage, 89–90
key-value databases, NoSQL, 357
keyboard shortcuts, 74
keyboards
cleaning, 326
configuring peripherals, 147
ergonomic, 137
input devices, 74–76
setting up desktop PC connections, 142
keylogger utility, spyware, 291

https://t.me/learningnets

keywords, file details and, 189
kinetics, configuring mobile devices, 159
knowledge base, technical support help, 344
knowledge factors, authentication and, 284

L

LANs (local area networks)
    connecting two or more with routers, 248
    defined, 23, 243
    sharing files and printers, 263–264
    WANs composed of two or more, 244
    wired, connecting to switches, 246–248
    wireless, connecting to WAPs, 246–248
laplets, 19
laptop computers
    mitigating theft, 280–281
    operating systems for, 13–18
    overview of, 12–13
laser printers, 82, 83
LCDs (liquid crystal displays), 66–68
leaving PC running, power management for, 320
LED (light-emitting diode)
    flat-panel displays, 66
    printers, 82
legacy browsers, security risks, 308
libraries
    adding to homegroup, 268
    sharing in homegroups, 267
licenses
    application, 234–236
    operating system, 109
    theft of software, 280
lid action, PCs in Sleep or Hibernate, 323, 325
links, recognizing suspicious, 304–306
Linux OS

https://t.me/learningnets

Bash shell scripting language, 370
comparing OS interfaces, 120–121
cross-referencing feature, 124
daemons, 126–127
exiting applications, 214
file management, 127
file management tools, 185
filesystem (EXT4), 187
forcing frozen apps to exit, 341
hotkeys, 129
interface options in, 13–14
overview of, 17
paths, 182
running applications in, 211–212
screenshots, 130
software compatibility and, 109–110
switching between applications, 213
liquid cooling, CPUs, 46–47
liquid crystal displays (LCDs), 66–68
local area networks. *See* LANs (local area networks)
local permissions, 200
Local Security Policy app, password lockout, 285
local security threats
data destruction, 279
malware, 280
theft, 279–280
unauthorized access, 278–279
local storage, data storage options, 94–97
localization, operating system setup, 144
lock screen
configuring mobile devices, 160–161
mobile device hardening, 281
ransomware as, 297
lock symbol in address bar, secure Web sites, 303
lockouts
device hardening with, 281–282

https://t.me/learningnets

setting password, 285
login, to SOHO router, 252–253
Long-Term Evolution (LTE) cellular networks, 164
loops, program flow with, 377
lossless compression, 231
lossy compression, 231
low-power modes, PC power, 321–322
LTE (Long-Term Evolution) cellular networks, 164

M

Macintosh platform, choosing OS, 13
macOS
comparing OS interfaces, 119–120
creating user accounts, 149
cross-referencing feature, 124
exiting applications, 214
file management, 127
file management tools, 184
filesystem (HFS), 187
forcing frozen apps to exit, 340
hotkeys, 129
installing additional software, 149
installing desktop applications, 217
interface options in OSs, 14
keyboards, 75
monitor connectors and ports, 73
overview of, 14–16
paths, 182
removing desktop applications, 221–222
running applications in, 210–211
screenshots, 130
software compatibility and, 109–110
switching between applications, 213
uninstalling unneeded software, 149
magnetic storage, 90–91

https://t.me/learningnets

magnetometer, mobile device kinetics, 159
mainframes
as multi-user computers, 9
PCs much smaller than, 10
remotely accessed systems using same principles as, 27
maintenance. *See* computer maintenance and management
maintenance phase, SDLC, 375–376
malicious cookies, blocking, 310
malicious software (malware)
adware, 289–291
as local security threat, 280
overview of, 288–289
ransomware, 296
risk of public workstations, 302
social engineering, 293–295
spam, 292–293
spyware, 291–292
Trojan horses, 295–296
User Account Control mitigating, 286–288
viruses, 295
web-based file downloads and storage as, 101
worms, 296
malicious software (malware), protection from
anti-malware programs, 298
prevention tips, 299
recovery tips, 299–300
Windows Update, 297
malware shield, anti-malware programs, 299
man-in-the-middle (MiTM) attacks, networks, 301
managed service, 353
management policy, passwords, 286
management tasks, database, 358
manual creation methods, databases, 357
manufacturer documentation and web sites, help from, 343–344
materials, cleaning computer hardware, 325–326
Mb (megabytes), file size/disk storage, 89–90

https://t.me/learningnets

media clips, 230
megahertz (MHz), CPU speed in, 40
memory cards, solid-state storage, 93
memory, types of, 47
MemoryStick, 93
metadata, file properties, 187
methods, objects and, 379–380
MFA (multifactor authentication), 284
MFDs (multifunction devices), 84–85
MHz (megahertz), CPU speed in, 40
mice. *See* mouse
micro-B, USB connector, 63–64
microATX, motherboard form factors, 50–51
microphones, connections for desktop PC, 142
microprocessors. *See* CPUs (central processing units)
MicroSD, memory card formats, 93
microservices, SDLC coding phase, 370
Microsoft Access
    database, 227
    report designer, 361–362
Microsoft accounts, creating, 149
Microsoft Active Directory domain, 266
Microsoft Azure
    creating database with ARM templates, 357
    data replication services, 202
    in-memory cache provider, 355
Microsoft Edge
    blocking only third-party cookies, 310
    clearing history and Temporary Internet Files, 311
    InPrivate Browsing, 302–303
Microsoft Office Online, web apps, 28–29
Microsoft SQL Server, protecting data at rest, 360
Microsoft Surface/SurfacePro, 19
Microsoft System Center Configuration Manager 2016, software deployment, 375
Microsoft Windows. *See* Windows OS

https://t.me/learningnets

mini-B, USB connector, 63–64
Mini DisplayPort, monitors, 73
Mini-ITX, motherboard form factors, 50–51
mini-PCIe, expansion slots, 62
minicomputers, as multi-user computers, 9
MiTM (man-in-the-middle) attacks, networks, 301
mobile apps, 27
mobile devices
    account IDs and passwords, 162
    airplane mode, 170–171
    apps install/remove, 174–175
    configuring synchronization, 172–173
    connecting to Wi-Fi networks, 168
    e-mail configuration, 171–172
    enabling Wi-Fi, 168
    gestures, 158–159
    interfaces, 155–158
    kinetics, 159
    managing lost device security, 162–164
    operating systems for, 21–23
    overview of, 18, 153–154
    pairing via Bluetooth, 165–167
    passcode settings, 160–161
    platform types, 224
    resetting, 176–177
    review answers, 179–180
    review, chapter, 177–178
    review questions, 178–179
    screen orientation, 159–160
    security features, 160
    setting up, 155
    sharing cellular connections between, 170
    smartphones, 18–19
    specialty devices, 19–20
    tablets, 19
    transferring data via Bluetooth, 167–168

https://t.me/learningnets

troubleshooting dead, 337
troubleshooting physical damage to, 337–338
Wi-Fi access point, 169–170
wireless connectivity, 164–165
mobility, Internet connectivity options for, 260
modems
connecting Internet to SOHO router, 250
overview of, 61
moisture control, computers, 329
monitors
cleaning, 326
CRT, 68–69
desktop PC connection setup, 142
ergonomics, 137
LCDs and flat-panel displays, 66–68
overview of, 66
ports and connectors, 69–74
projectors, 69
review answers, 88
review, chapter, 85–86
review questions, 86–87
touchscreens, 74
monolithic applications, modular vs., 370
motherboards
audio processors, 78
bus speed, 41–42
CPUs plugging into, 40–41
features, 51–52
form factors, 50–51
overview of, 50
mouse
configuring peripherals, 147
ergonomic, 137
input devices, 76
setting up desktop PC connections, 142
troubleshooting, 342

https://t.me/learningnets

movement, accessibility options, 130
moving files, 192–194
multi-user computers, 9–10
multicore CPUs, 42
multifactor authentication (MFA), 284
multifunction devices (MFDs), 84–85
multiple-user licenses, 236
multitiered applications, 207
music, streaming media, 27
MySQL Workbench utility, 359

N

n-tiered applications, 207–208
NAS (network-attached storage), 97–98, 203
navigation, file structure, 185–187
near-field communication (NFC)
    wireless connectivity and, 164
    WPS setup, 258
network cards. *See* NICs (network interface cards)
Network Discovery, File and Printer Sharing, 264
network-enabled printers, sharing, 272–273
network interface cards (NICs), 61
network operation centers (NOCs), satellite connectivity, 259–260
network organization
    domains, 266
    homegroups, 266–267
    workgroups, 265–266
network volumes, accessing shared, 269–270
networking
    availability and, 261
    clients and servers, 244–246
    connecting mobile devices to Wi-Fi networks, 168
    connecting personal computers, 10
    connection delay/latency, 262
    file and printer sharing, 263–264

https://t.me/learningnets

IT security threat mitigation, 300–301
LANs and WANs, 243–244
local ad hoc networks and direct links, 248–249
making right choice, 259–260
mobility and, 260–261
network organization, 264
number of concurrent connections, 262
organization with domains, 266
organization with homegroups, 266–269
organization with workgroups, 265–266
overview of, 23–25, 243
reliability, 262
resource sharing, 26
review answers, 276
review, chapter, 273–274
review questions, 274–275
security level, 262–263
servers, 26
sharing folders, 269–272
sharing network volumes, 98–99, 269
sharing printer, 272–273
SOHO router, setup and configuration, 249–255
storage options, 97–99
switches and routers, 246–248
throughput/bandwidth, 261
wireless clients, 258–259
wireless security setup, 255–258
New Technology File System (NTFS), 187–189
NFC (near-field communication)
wireless connectivity and, 164
WPS setup, 258
NICs (network interface cards), 61
NOCs (network operation centers), satellite connectivity, 259–260
nonpersistent storage, 355
nonrepudiation, device hardening via, 282
nonvolatile memory, mobile devices and, 21

https://t.me/learningnets

NoSQL databases, 356–357
notebook computers. *See also* laptop computers, 11
NTFS (New Technology File System), 187–189
number of concurrent connections, Internet connectivity, 262
numeric keypad, keyboards, 75

O

object-oriented programming, software development/implementation, 378–382
objects
    methods, 379–380
    properties, 379
    scalar data types vs., 378
OCR (optical character recognition), scanners, 146
octa-core architecture, CPUs, 42
OEMs (original equipment manufacturers), 215
OLEDs (organic light-emitting diodes), 68
one-time passwords, 285–286
OneDrive (Microsoft)
    online storage for backups, 202
    saving work to cloud, 214
online storage
    backups, 202
    data, 99–101
online store, installing applications from, 217–218
open source
    operating systems, 109
    software and licensing, 235
opening files, 191–192
optical character recognition (OCR), scanners, 146
optical mice, 77
optical storage, data, 91–92
organic light-emitting diodes (OLEDs), 68
original equipment manufacturers (OEMs), 215
OS X. *See* macOS
OSs (operating systems)

https://t.me/learningnets

accessibility options, 130–131
applications vs., 207
categorizing smartphones by, 19
characteristics of, 108–109
Chrome interface, 121–124
comparing interfaces, 110–111
complexity of, 110
connecting to hardware, 127–128
connecting to Internet, 128
cross-referencing feature equivalent between, 124
for desktops and laptops, 13–18
executing programs, 125–126
forms of programming, 7
functions of, 107–108
licensing, 109
Linux interface, 120–121
mac interface, 119–120
managing files, 127
for mobile devices, 21–23
mobile devices, 154
navigating with hotkeys, 128–129
review answers, 133–134
review, chapter, 131
review questions, 132–133
screenshots, 129–130
services, 126–127
setting up, 144–145
software compatibility and, 109–110
VMs (virtual machines), 29
Windows 7 interface, 111–112
Windows 8 interface, 113–118
Windows 10 interface, 118–119
output devices. *See* I/O (input/output) devices
outputs, data flow through computer, 39

https://t.me/learningnets

P

packet sniffing (capturing) tools, eavesdropping on networks, 300
pairing mobile devices, 165–167
parallel ATA (PATA), hard drive connections, 95
parallel connectors
    legacy ports/connectors, 65–66
    printer ports/connectors, 85
passcode, mobile devices, 160–161
passive cooling, CPUs, 44
password cracking, unauthorized access, 278
password managers (or password vaults), 285–286
passwords
    authentication relying on, 284
    complexity (or strength) of, 285
    confidentiality of, 285–286
    creating homegroups with, 267–268
    device hardening by configuring lockout, 281–282
    disabling autofill for, 312–313
    expiration and re-use of, 286
    IT security threat mitigation and, 283
    management policy, 286
    mobile device configuration, 162
    one-time, 285–286
    resetting default SOHO router, 252–253
    sharing folders in File Sharing dialog, 271
    single sign-on (SSO), 286
    User Account Control (UAC), 286–288
    user authentication, 284–286
    using appropriate account types, 283–284
PATA (parallel ATA), hard drive connections, 95
patches
    management of, 297
    troubleshooting apps, 340
    updating applications, 219
paths, understanding, 181–183

https://t.me/learningnets

Pb (petabytes), file size/disk storage, 89–90
PBC (push-button configuration), WPS setup, 258
PCI (Peripheral Component Interconnect), expansion slots, 62
PCIe (PCI Express), expansion slots, 51, 61–62
PCs (personal computers)
    desktops and laptops, 11–12
    overview of, 10–11
PCs (personal computers), setting up
    avoiding ESD and EMI issues, 138–140
    cable management, 143–144
    choosing where to locate, 136
    completing post-setup tasks, 145–147
    creating user accounts, 149–150
    ensuring reliable AC power, 140–141
    installing/uninstalling software, 148–149
    making work area more comfortable, 136–138
    operating system, 144–145
    overview of, 135
    physical connections for desktop PC, 142–143
    preparing work area, 135–136
    review answers, 152
    review, chapter, 150
    review questions, 150–152
peer-to-peer file sharing, 98
peer-to-peer networks, 246
per-sear license, 236
per-user license, 236
performance
    database storage and, 354
    in maintenance phase, SDLC, 375
    NoSQL database benefits, 356–357
Peripheral Component Interconnect (PCI), expansion slots, 62
peripherals
    configuring, 146–147
    PCs and, 10, 11
    troubleshooting, 341

https://t.me/learningnets

permissions, file management, 200–201
persistence, database, 355
persistent storage, 355
personal computers. *See* PCs (personal computers)
personal hotspots, mobile devices, 170
personal identification number (PIN)
    device hardening by configuring lockout, 281
    WPS setup, 258
Personal Information Protection and Electronic Documents Act (PIPEDA), Canadian privacy law, 8
petabytes (Pb), file size/disk storage, 89–90
phablets. *See also* mobile devices, 19, 154
phone numbers, limiting online use of PII, 307
photos, synchronizing, 172–173
physical damage, troubleshooting mobile devices, 337–338
physical security, access control, 280
PIDs (process identifiers), frozen apps in Linux, 341
PII (personally identifiable information), limiting online use of, 307
PIN (personal identification number)
    device hardening by configuring lockout, 281
    WPS setup, 258
pinch gesture, mobile devices, 158
PIPEDA (Personal Information Protection and Electronic Documents Act), Canadian privacy law, 8
plasma displays, 68
platforms, application, 224
Plug and Play, OS support, 128
plug-ins
    disabling unneeded, 311
    updating, 307
point-of-sale (PoS) terminals, 32
pointing devices, 76–77
PoLP (principle of least privilege), hardening database server, 360
pop-ups
    closing windows, 289
    preventing, 290

https://t.me/learningnets

ports/connectors
ad hoc networks, 99
audio devices, 77–79
desktop PC, 142–143
Ethernet cable, 142
expansion cards, 61
hard drive connections, 95–96
keyboards, 75
monitors, 69–74
non-USB options, 64–66
pointing devices, 76
review answers, 88
review, chapter, 85–86
review questions, 86–87
troubleshooting, 341
USB, 63–64
PoS (point-of-sale) terminals, 32
possession factor, multifactor authentication, 284
power
CPU, 43–46
database scalability, and compute, 353–354
ensuring reliable AC, 140–141
troubleshooting, 336–337
power button
putting PC in Sleep or Hibernate, 323, 325
troubleshooting, 337
power conditioners, reliable AC power, 141
power management, computer
actions for power buttons/closing lid, 323, 325
energy-efficient devices, 320
leaving PC running and, 320
low-power modes, 321–322
power plans, 322–324
review answers, 334
review, chapter, 331–332
review questions, 332–333

https://t.me/learningnets

shutting down PC, 320–321
power plans, PCs, 322–324
power profiles, PCs, 322–323
Power savings power plan, PCs, 322–323
power supplies
dual-voltage options, 140
ensuring reliable AC power, 140–141
overview of, 52–54
power supply units (PSUs). *See* power supplies
PowerShell scripting language, Windows, 370
preshared key (WPA2–PSK), SOHO routers, 257
prevention tips, malware, 299
primary keys, relational databases, 356
principle of least privilege (PoLP), hardening database server, 360
printers
configuring, 147
consumables, 83
installing and sharing, 272–273
as multifunction devices, 84–85
overview of, 81
resource sharing, 26
sharing files, 263–264
sharing in workgroups, 265
technologies, 81–83
troubleshooting, 342
printhead, impact printers, 81
printwires, 81
privacy
clearing cookies, 309–310
laws, 8
risks of public workstations, 302–303
Private Browsing mode, Safari in iOS, 303
process identifiers (PIDs), frozen apps in Linux, 341
processing
data flow through a computer, 39
resource sharing, 26

https://t.me/learningnets

processors. *See also* CPUs (central processing units), 7, 8
product keys, applications, 236
productivity software, 225
Program Compatibility Troubleshooter, 340–341
program flow, software development, 380–382
programmers, 3
programming, 7
programming languages
    data types, 376–378
    interpreted (scripted) vs. compiled, 370
    program flow, 380–382
    tracking changes in larger projects, 373–374
    types of, 373
programs
    applications vs., 208
    commands in, 3
    operating systems executing, 125–126
projectors, 69
properties
    file attributes, 187–188
    folder attributes, 188
    object, 379
    uneditable, 188–189
    viewing/modifying, 189–191
proprietary software, licensing and, 235
PS/2
    keyboard ports/connectors, 75
    pointing device ports/connectors, 76
    ports/connectors, 65–66
pseudocode
    planning code using, 373
    planning loops using, 381
PSUs (power supply units). *See* power supplies
public domain software, licensing and, 235
push-button configuration (PBC), WPS setup, 258
Python programming language, 371

https://t.me/learningnets

Q

quad-core architecture, CPUs, 42
quarantine, malware recovery process, 299
queries, NoSQL databases based on, 356–357
query tools, database, 361–362
QWERTY layout, keyboard, 74–75

R

radio frequency. *See* Wi-Fi (wireless fidelity)
RAID (redundant array of independent disks), 97
RAM (random access memory)
    capacity, 48
    CPU cache and, 43
    database persistence and, 355
    motherboard features, 51
    operating system options, 110
    overview of, 47
    technologies and speeds, 49–50
    types, 47–48
random access memory. *See* RAM (random access memory)
ransomware, as malware, 296–297
raster formats, images, 231–232
RCA connectors, composite video, 71
RE (Windows Recovery Environment), troubleshooting startup, 340
read-only memory (ROM), 47
reboot, troubleshooting startup with, 338
recognition, malware recovery process, 299
records (rows), database table, 351–353
recovery mode, troubleshooting startup, 340
recovery tips, malware, 299–300
Recycle Bin, deleting/undeleting files and folders, 195–197
recycling, computer disposal, 330–331
Redis in-memory cache solution, 355
reducing attack surface, device hardening, 280–283
redundant array of independent disks (RAID), 97

https://t.me/learningnets

referential integrity, relational databases, 356
regression testing, 374
relational databases
    NoSQL databases vs., 356
    overview of, 355–356
reliability, Internet connectivity options, 262
remediation, malware recovery process, 300
remote access, 27
remote networks, WANs as, 24
removable media, cleaning, 326
renaming, files and folders, 194–195
replication of data, backup technique, 202
report builder tools, databases, 361–362
requirement analysis and planning phase, SDLC, 368–369
requirement specification document, SDLC, 369–370
reset, mobile devices, 176–177, 337
resistive screens, touchscreens, 74
resource sharing, in networks, 26
restart options, Windows Update, 297
restore, file management, 201–203
restore point, System Restore, 339
Restriction of Hazardous Substances (RoHS) directive, computer disposal, 330–331
reuse, password, 286
RF (radio frequency), wireless keyboards, 75
RGB (component) video, 71–73
risks
    of personal information on Internet, 307
    of public workstations, 302–303
RJ-11 ports/connectors, 61, 65–66
RJ-45 ports/connectors
    ad hoc networks, 99
    Ethernet cable, 142
    Internet, 142
    for NICs, 61
    ports/connectors, 65–66

https://t.me/learningnets

SOHO routers, 250
rogue sites, User Account Control mitigating, 286–288
RoHS (Restriction of Hazardous Substances) directive, computer disposal, 330–331
ROM (read-only memory), 47
root directory, in file hierarchy, 182
rotate screen orientation, mobile devices, 159–160
rotation speeds, hard disk drives, 91
routers
in LANs, 23
networking and, 246–248
role in sending network communications, 25
setting up/configuring SOHO. *See* SOHO (small office/home office) router
SOHO LANs, 247
rows (records), database table, 351–353

S

S-Video, monitor connectors and ports, 71–72
SaaS (Software as a Service) model, 218–219
sags, ensuring reliable AC power, 141
Samsung Galaxy
features common to computing devices, 4
types of tablets, 19
sandboxing, SDLC testing phase, 373–374
SATA (serial ATA), hard drive connections, 95
satellite networks
Internet connectivity via, 259–260
level of security, 262
mobility, 260
network latency, 261
throughput, 261
saving
files, 191–192
work, 213–214
scalability

https://t.me/learningnets

database, 353–355
NoSQL database benefits, 356–357
scalar data types, 378
scanners
optical character recognition, 146
resource sharing, 26
scareware, ransomware as, 297
schema-less, NoSQL databases as, 356–357
schema, relational database, 355, 356
scientific calculators, as specialty mobile devices, 20
screen
lock for mobile devices, 160–161
orientation in mobile devices, 159–160
resolution, OS setup, 144
troubleshooting cracked display, 338
screensaver, Windows, 281–282
screenshots (screen capture), 129–130
scripted (interpreted) languages
common types of, 370–373
compiled code vs., 370
creating database with, 357
SD (Secure Digital), memory card formats, 93
SDLC (software development life cycle)
coding, 370–373
deployment, 375
design, 369–370
maintenance, 375–376
overview of, 367–368
requirement analysis and planning, 368–369
review answers, 385–386
review, chapter, 383–384
review questions, 384–385
testing, 373–375
SDR (single data rate) RAM, 49
search and destroy, malware recovery process, 300
search engine redirection, caused by adware, 289

https://t.me/learningnets

searches, for specific files, 197
Secure Digital (SD), memory card formats, 93
Secure Sockets Layer/Transport Layer Security (SSL/TLS) security certificates, 360
secure Web sites
    recognizing, 303
    vs. trusted sites, 303
security
    alerts (fake and real) in social engineering, 295
    changing SSID on SOHO router, 255
    configuring browser, 308–309
    configuring mobile devices, 160
    database, 360
    file and folder permissions, 200–201
    installing and updating security software, 145–146
    Internet connectivity options for, 262–263
    login/changing password on SOHO router, 252–253
    managing lost device security, 162–164
    patches, 297
    SOHO router connectivity for wireless clients, 258–259
    SOHO router wireless setup, 255–258
    threat mitigation, IT security threat mitigation
    updates in maintenance phase, SDLC, 375
security zones, Internet Explorer, 308–309
select, multiple files and folders, 192
serial ATA (SATA), hard drive connections, 95
serial connectors
    legacy ports/connectors, 65–66
    printer port/connectors, 85
serial numbers, applications, 236
servers
    file, 97
    in networks, 26
    remote access and, 27
    understanding, 244–246
Service Set ID (SSID)

https://t.me/learningnets

changing on SOHO router, 255
selecting Wi-Fi access point, 169
SOHO router wireless connectivity, 258–259
services (daemons), operating systems, 126–127
Settings app, verifying wireless capabilities, 165
SFTP (Secure FTP), 100
Share (or Share with)
folders and libraries in homegroup, 268–269
sharing folders manually, 269–271
sharing
accessing shared network volumes, 269–270
file and folder permissions and, 200
files and printers, 263–264
files, folders, and printers in workgroups, 265
folders and libraries in homegroups, 268–269
folders in File Explorer, 271–272
folders manually, 269
libraries in homegroups, 267
local printer with other computers on LAN, 273
network-enabled printers, 272–273
network volumes, 98–99
online peer-to-peer files, 246
shortcuts, executing programs, 125
shoulder surfing, 279
shutting down, PC power management, 320–321
signatures
antivirus program detecting viruses via, 298
keeping definition file updated, 299
single data rate (SDR) RAM, 49
single-factor authentication, users, 284
single sign-on (SSO)
Microsoft AD domain, 266
passwords, 286
single tiered applications, 207
single-user licenses, application licensing, 236
site license, 236

https://t.me/learningnets

Skype, VoIP services, 33
SLAs (service level agreements), applications, 215
Sleep mode
    closing lid/using power button to put PC in, 323, 325
    PC power management, 321
    troubleshooting low-power mode, 337
small outline DIMMs (SODIMMs), RAM, 47–48
smartphones. *See also* mobile devices
    cellular connectivity for, 259
    as client computers, 244
    embedded multimedia controllers in, 93
    features common to computing devices, 4
    kinetics, 159
    mobile apps, 27
    as mobile device type, 18–19
    overview of, 154
    running applications, 212–213
    security features, 160
social engineering
    email phishing, 294–295
    infiltration, 293–294
    overview of, 293
    security messages (fake and real), 295
    telephone scams, 294
SODIMMs (small outline DIMMs), RAM, 47–48
soft cloth, cleaning computer hardware, 325, 326
soft reset, mobile devices, 176–177
software. *See also* applications (apps)
    business software, 226–227
    collaboration software, 226
    compatibility, 109–110
    defined, 9
    downloading from reputable site, 291
    installing additional, 149
    installing security software, 145
    knowing source of before loading, 299

https://t.me/learningnets

licensing, 234–236
operating system functions, 108
OS as software foundation, 13
for printers and MFDs, 85
product keys and activation, 236
productivity software, 225
requirements in SDLC design phase, 369–370
specialized software, 228
theft of, 280
uninstalling unneeded, 148
utility software, 226–227
Software as a Service (SaaS) model, 218–219
software development and implementation
data types, 376–378
object-oriented programming, 378–380
overview of, 367
program flow, 380–382
review answers, 385–386
review, chapter, 383–384
review questions, 384–385
SDLC. *See* SDLC (software development life cycle)
software licenses, theft of, 280
SOHO (small office/home office) networks
connecting to Internet, 246–248
defined, 246
overview of, 23–24
peer-to-peer networks in, 246
SOHO (small office/home office) router
accessing configuration utility, 250–252
built-in firewall, 312
changing SSID, 255
checking for Internet connectivity, 250
choosing appropriate, 249
logging in and changing password, 252–253
overview of, 249
setting up, 249–250

https://t.me/learningnets

updating firmware, 254–255
wired connection, 250
wireless client connectivity, 258–259
wireless security, 255–258
solid state
memory, 47
storage, 93–94
sorting files, 199–200
spam, as malware, 292–293
speakers
audio devices, 78–79
desktop PC connections, 142
specialized computer systems, 31–33
specialized software, 228
spikes, and reliable AC power, 140
spyware, as malware, 291–292
SQL programming language, 372
SQL Server, protecting data at rest, 360
SSDs (solid-state drives)
files servers and, 97
solid-state storage, 93
SSID (Service Set ID)
changing on SOHO router, 255
selecting Wi-Fi access point, 169
SOHO router wireless connectivity, 258–259
SSL/TLS (Secure Sockets Layer/Transport Layer Security) security certificates, 360
SSO (single sign-on)
Microsoft AD domain, 266
passwords, 286
Standard account, 283–284, 287
standards, wireless SOHO router, 249
start up, troubleshooting, 338–340
storage media, backups, 203
storing data. *See* data storage
streaming media, 27, 230–232

https://t.me/learningnets

strong passwords, 278, 285
structures, database, 355
stylus pens, as input device, 77
subnotebooks. *See also* laptop computers, 12
supercomputers, 9
SuperSpeed USB, 63
Support section, manufacturer web sites, 343
surges, and reliable AC power, 140–141
swipe gesture, mobile devices, 158
switches
    SOHO LANs, 247
    wired LANs, 23, 246–248
switching, between applications, 213
synchronization
    of computers, 173
    of devices, 172
    of mobile devices, 172–173
    of photos, 172–173
system board. *See* motherboards
system bus, CPU cache and, 43
system hardware
    CPU features, 42–43
    CPU overview, 40–42
    CPU power and heat management, 43–46
    motherboard features, 51–52
    motherboard form factors, 50–51
    overview of, 39–40
    power supplies, 52–54
    RAM capacity, 48
    RAM technologies and speeds, 49–50
    RAM types, 47–48
    review answers, 56–57
    review, chapter, 54
    review questions, 55–56
system health, monitoring OS, 108
system RAM, 47

https://t.me/learningnets

System Restore, troubleshooting startup, 338–339

T

T1/T3 lines, network communications, 25
tables, database
    relational, 356
    security features, 160
    structure of, 352–353
    understanding, 351–352
tablets. *See also* mobile devices
    cellular connectivity for, 259
    embedded multimedia controllers in, 93
    kinetics, 159
    mitigating theft, 280–281
    mobile apps, 27
    as mobile device type, 19
    overview of, 154
tap gesture, mobile devices, 158
Task Manager, forcing frozen apps to exit, 340
Tb (terabytes), file size/disk storage, 89–90
TDE (Transparent Data Encryption), SQL Server, 360
technical support, help from, 344–345
teleconferencing, VoIP and, 33
telephone lines, network communications via, 25
telephone scams, social engineering, 294
telepresence, VoIP and, 33
temperature, troubleshooting physical damage from, 337
templates, creating database with, 357
Temporary Internet Files
    clearing browser, 311
    clearing cookies, 309–310
testing phase, SDLC, 373–375
tethering, cellular connections between mobile devices, 170
theft, as local security threat, 279–280
thermal paste, CPU heat management, 44

https://t.me/learningnets

thermal printers, 83
third-party cookies, 310
third-party extensions, mitigating banner ads, 306–307
threats. *See* IT security threat mitigation
throughput/bandwidth, Internet connectivity options for, 261
Thunderbolt
    external storage, 96–97
    ports/connectors, 64–65
    ports/connectors for monitor, 73
    setting up desktop PC connections, 142
time zones, operating system setup, 144
TLS (Transport Layer Security)
    recognizing secure Web sites, 303
    web-based file downloads and storage, 101
toner, laser printers and, 82
toolbars, disabling unneeded, 312
tools, file management, 183–185
touchpads, as input devices, 76–77
touchscreens
    on laptops, 12
    as mobile device interfaces, 154
    overview of, 74
trackballs, as input devices, 76–77
tractor-feed impact paper, impact printers, 81
trail version, licensing and, 235
transformer blocks, laptop power cords, 53–54
transmission range, Bluetooth vs. Wi-Fi, 78
Transparent Data Encryption (TDE), SQL Server, 360
Trojan horses, 295–296
troubleshooting. *See* IT troubleshooting
trust, IE security zones and, 308–309
trusted site, secure Web site vs., 303
Type-A, USB connector, 63–64
Type-B, USB connector, 63–64
Type-C, USB connector, 63–64

https://t.me/learningnets

U

UAC (User Account Control)
    installing applications and, 216
    protection from malware or rogue sites, 286–288
Ubuntu Linux
    Linux distros, 17
    removing apps, 223
    running applications, 211–212
    switching between applications, 213
UEFI (Unified Extensible Firmware Interface), motherboard, 51
ultrabooks. *See also* laptop computers, 12–13
unauthorized access, IT security threat mitigation, 278–279
undeleting files and folders, 195–197
uninterruptible power supply (UPS), reliable AC power, 141
unit testing, 374
Unity (Linux), exiting applications, 214
UNIX, Linux variant of, 17
Unsubscribe link, avoiding in spam, 292
untrusted source warnings, recognizing, 304–305
updates
    anti-malware, 299
    application, 219–220
    browser and plug-in, 307
    in maintenance phase, SDLC, 375
    mitigating banner ads with browser, 307
    running as part of OS setup, 145–146
    SOHO router firmware, 254–255
    troubleshooting apps, 340
UPS (uninterruptible power supply), reliable AC power, 141
URLs
    evaluating for suspicious links, 304–306
    recognizing secure Web sites, 303
USB flash drives, solid-state storage, 93
USB (universal serial bus)
    audio devices, 79

https://t.me/learningnets

configuring peripherals, 146
connector types, 63–64
external storage, 96–97
generations and speeds, 63
keyboard ports/connectors, 75
monitor connectors and ports, 74
pointing device ports/connectors, 76
printer port/connectors, 85
User Account Control (UAC)
installing applications and, 216
protection from malware or rogue sites, 286–288
user accounts
creating, 149–150
operating system setup, 145
usernames, authentication relying on, 284
users and passwords
authenticating users, 284–286
IT security threat mitigation and, 283
User Account Control, 286–288
using appropriate account types, 283–284
users, smart Web. *See* browsing best practices
utility software, 226–227

V

vacuums
cleaning computer hardware, 325–326
cleaning inside PC, 328
values
functions returning, 382
of properties, 379
vector formats, images, 232–233
ventilation control, well-maintained computers, 329
vertically, scaling database, 354
VGA (Video Graphics Array)
monitor connectors and ports, 71

https://t.me/learningnets

setting up desktop PC connections, 142
video
card updates, 340
cards, 60
container files, 231
formats, 230–232
streaming media, 27
Video Graphics Array (VGA)
monitor connectors and ports, 71
setting up desktop PC connections, 142
virtual machine image, database creation, 357–8
virtual machines (VMs), 29–30
virtualization, 29–31
virus shields, antivirus programs as, 298
viruses
as malware, 295
removing adware that acts like, 291
Trojan horses as, 296
visual accessibility options, 130
VMs (virtual machines), 29–30
voice accessibility options, 130
Voice over IP (VoIP), 33
volume license, 236
volumes, sharing network, 98–99
Vonage, VoIP services, 33
VPNs (virtual private networks)
database security with, 360
installing applications, 215
man-in-the-middle attacks and, 301

W

WANs (wide area networks)
as collection of LANs, 24–25
defined, 23
understanding, 244–245

https://t.me/learningnets

WAPs (wireless access points)
selecting Wi-Fi access point, 169–170
SOHO LANs, 247
wireless connectivity in LANs, 23, 246–248
warnings
recognizing invalid certificates, 304–305
recognizing untrusted sources, 304–305
water blocks, liquid cooling systems, 46
water, troubleshooting physical damage from, 338
wearables. *See also* mobile devices, 154
web-based applications, 27–29, 218–219
web-based devices, 224
web sites
getting help from manufacturer, 343–344
technical support, 344–345
web-based file downloads and storage, 101
web users, smart. *See* browsing best practices
webcams, 80
WEP (Wired Equivalent Privacy), SOHO router, 255–256
Where-Object cmdlet, PowerShell, 370
while loops, 377–378
Wi-Fi Protected Setup (WPS), SOHO routers, 258
Wi-Fi (wireless fidelity)
connecting to, 168
enabling on mobile devices, 168
mobility and, 260
radio frequency used by, 260
selecting access point, 169–170
sound connectivity, 78
unauthorized usage of, 279
verifying wireless capabilities, 165
wireless connectivity and, 164
Windows 7
comparing OS interfaces, 111–112
running applications, 209
Windows Update, 146

https://t.me/learningnets

Windows 8/8.1
comparing OS interfaces, 113–118
running applications, 209–210
Windows Update, 146
Windows 10
comparing OS interfaces, 118–119
running applications, 209
Windows Update, 146
Windows Explorer/Windows File Explorer
accessing Clipboard commands, 194
accessing shared network volumes, 269–270
backing up files, 201
changing view options, 197–199
compressing files, 229–230
exploring new homegroup, 268
navigating file structure, 182–184, 186–187
renaming files and folders, 194–195
searching for specific files, 197
setting up folder permissions, 200–201
sharing folders in, 271–272
viewing/modifying properties, 189–191
Windows Firewall, 312
Windows libraries, sharing in homegroups, 267
Windows OS
accessibility options, 131
creating user accounts, 149–150
cross-referencing feature, 124
default folders, 181
exiting applications, 214
file management, 127
forcing frozen apps to exit, 340
hotkeys, 129
installing additional software, 149
installing desktop applications, 215–217
interface options in OSs, 13–14
keyboards, 75

https://t.me/learningnets

mobile device operating systems, 154
navigating file structure, 186–187
New Technology File System (NTFS), 187
overview of, 14–15
pairing via Bluetooth, 165–166
paths, 182
PowerShell scripting language in, 370
removing desktop applications and apps, 220–221
resource sharing, 26
running applications in, 208–210
screenshots, 130
services, 126–127
software compatibility and, 109–110
switching between applications, 213
tools for file management, 183–184
understanding mobile device interface, 155–158
uninstalling unneeded software, 148
Windows 7, 111–112
Windows 8, 113–118
Windows 10, 118–119
Windows Update, 146
Windows Phone
categorizing smartphones by OS, 19
OS for mobile devices, 22–23
transferring data via Bluetooth, 167
Windows Recovery Environment (RE), troubleshooting startup, 340
Windows Store, installing applications from, 217–218
Windows Update
protection against malware, 297
updating applications, 219
Windows OS, 146
Windows versions, troubleshooting apps, 340
wired connectivity
SOHO routers for, 250
strengths and weaknesses of, 259–263
wireless routers for administrators vs., 255

https://t.me/learningnets

wireless ad hoc networks, 248–249
wireless clients, SOHO routers for, 258–259
wireless connectivity
    device hardening by disabling unused, 281
    overview of, 164–165
    strengths and weaknesses of, 259–263
wireless keyboards, 75
wireless local area networks (WLANs), 243
wireless networks
    ad hoc networks, 99
    malware from LAN, 287
    security for SOHO router, 255–258
Wireless Protected Access 2 (WPA2), 256–257
Wireless Protected Access (WPA), 256
wireless SOHO router, choosing, 249
WLANs (wireless local area networks), 243
work area
    making comfortable, 136–138
    setting up PC, 135–136
    where to locate PC, 136
workgroups, network organization via, 265–266
workstations
    as client computers, 244
    risks of public, 302–303
    sharing network-enabled printers from, 272–273
    SOHO LAN, 247
worms, as malware, 296
WPA (Wireless Protected Access), 256
WPA2–PSK (preshared key), SOHO routers, 257
WPA2 (Wireless Protected Access 2), SOHO routers, 256–257
WPS (Wi-Fi Protected Setup), SOHO routers, 258

X

XML programming language, 372

https://t.me/learningnets

Z

ZIP files
    compression formats, 229–230
    downloading for install on macOS, 217
    downloading for install on Windows OS, 216
zombies, DDoS attacks and, 301

https://t.me/learningnets

https://t.me/learningnets

totalvideo

Certification Exam Training

TOTAL Seminars



Over an hour of *FREE* Mike Meyers / Scott Jernigan Video Training

Free episodes at hub.totalsem.com

Get the Full Version at a SPECIAL PRICE

Buy Now - use coupon code AIOITF18V at totalsem.com/itfv

Attention Educators

- ✓ Comprehensive Mike Meyers Curriculum
- ✓ Classroom in a Box Equipment Solutions
- ✓ Special Educator Pricing

Discount Exam Vouchers

CompTIA IT Fundamentals | CompTIA A+ | CompTIA Network+ | CompTIA Security+

BUY totalsem.com/vouchers

www.totalsem.com • (800) 446-6004

https://t.me/learningnets