Save 10% on Exam Voucher

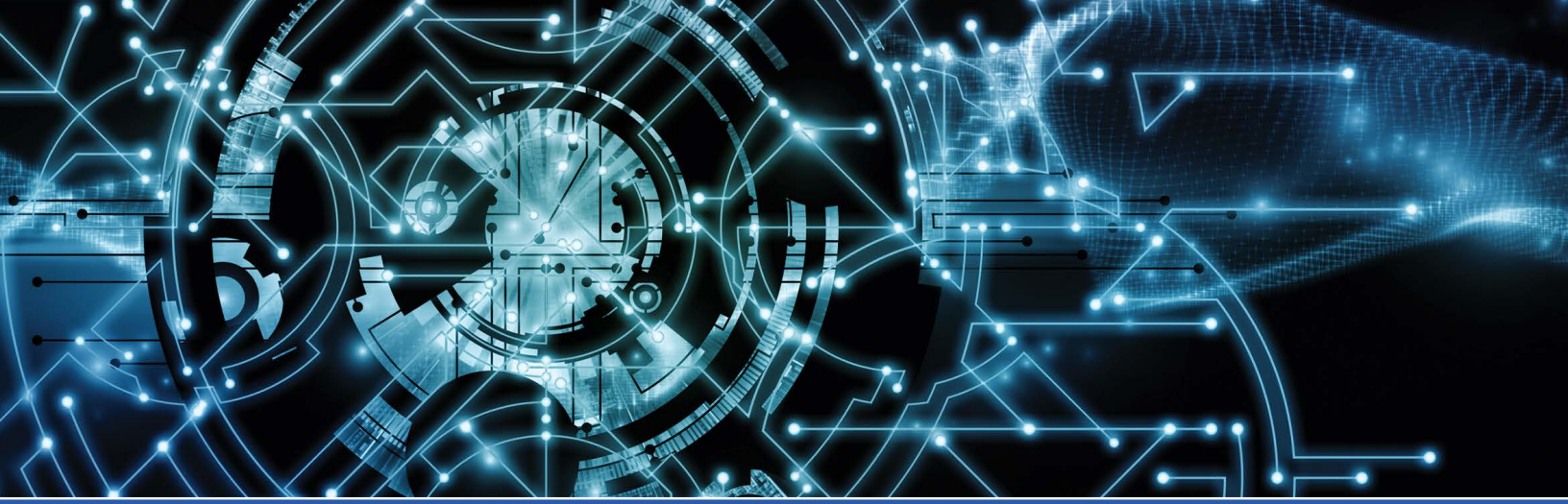
See Inside

PEARSON IT CYBERSECURITY CURRICULUM

COMPLETE A+ GUIDE TO IT HARDWARE AND SOFTWARE

CompTIA® A+ Core 1 and Core 2 Exams (V15)

CHERYL A. SCHMIDT
CHRISTOPHER A. LEE



Complete A+ Guide to IT Hardware and Software

A CompTIA A+ Core 1 and Core 2 Exams (V15) Textbook

TENTH EDITION

CHERYL A. SCHMIDT
CHRISTOPHER A. LEE
FLORIDA STATE COLLEGE AT JACKSONVILLE

PEARSON IT
CERTIFICATION

Complete A+ Guide to IT Hardware and Software, Tenth Edition

Copyright © 2026 by Pearson Education, Inc.

All rights reserved. This publication is protected by copyright, and permission must be obtained from the publisher prior to any prohibited reproduction, storage in a retrieval system, or transmission in any form or by any means, electronic, mechanical, photocopying, recording, or likewise. For information regarding permissions, request forms, and the appropriate contacts within the Pearson Education Global Rights & Permissions Department, please visit www.pearson.com/global-permission-granting.html.

No patent liability is assumed with respect to the use of the information contained herein. Although every precaution has been taken in the preparation of this book, the publisher and author assume no responsibility for errors or omissions. Nor is any liability assumed for damages resulting from the use of the information contained herein.

Please contact us with concerns about any potential bias at
www.pearson.com/en-us/report-bias.html

$PrintCode

Library of Congress Cataloging-in-Publication Data: 2025939499

ISBN-13: 978-0-13-543977-7
ISBN-10: 0-13-543977-9

Trademarks

All terms mentioned in this book that are known to be trademarks or service marks have been appropriately capitalized. Pearson IT Certification cannot attest to the accuracy of this information. Use of a term in this book should not be regarded as affecting the validity of any trademark or service mark.

Warning and Disclaimer

Every effort has been made to make this book as complete and as accurate as possible, but no warranty or fitness is implied. The information provided is on an "as is" basis. The authors and the publisher shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this book.

Head of IT & Professional Learning, Enterprise Learning and Skills
Julie Phifer

Executive Editor
James Manly

Development Editor
Ellie C. Bru

Managing Editor
Sandra Schroeder

Senior Project Editor
Mandie Frank

Copy Editor
Kitty Wilson

Indexer
Ken Johnson

Proofreader
Debbie Williams

Technical Editors and Contributors
Justin Valentino
Jeff Burns
David Singletary
Jason Brenneman
Melodie Schmidt
Karl Schmidt
Elizabeth Drake
Christine Farrington
David Brown

Cover Designer
Chuti Prasertsith

Compositor
Tricia Bronkella

Art Production
Justin Ache
Marc Durrence
Katherine Martin
Amanda McIntosh
KC Frick
Vived Graphics

Photographers
Raina Durrence
Jennifer Cansler
George Nichols

Credits

Figure	Credits
Cover	spainter_vfx/Shutterstock
Chapter opener image	agsandrew/Shutterstock
Figure 01-07	MaverickLEE/Shutterstock
Figure 01-10	NAN728/Shutterstock
Figure 01-12	Sashkin/Shutterstock
Figure 01-13	sergeytikhomirov/123RF
Figure 01-14	MNI/Shutterstock
Figure 01-15	norikko/Shutterstock
Figure 01-16	AlexLMX/Shutterstock
Figure 01-17	Oleksiy Mark/Shutterstock
Figure 01-21	Petr Malyshev/Shutterstock
Figure 01-24A	Robert Milek/Shutterstock
Figure 01-24B	magraphics/123RF
Figure 01-24C	CactusG/Shutterstock
Figure 01-25	Agenturfotografin/Shutterstock
Figure 01-31	alexlmx/123RF
Figure 01-32	Equipoise/Shutterstock
Figure 01-32(3)	Unkas Photo/Shutterstock
LAB-Figure 01-01, LAB-Figure 01-02, LAB-Figure 01-03, LAB-Figure 01-04, LAB-Figure 01-05, LAB-Figure 01-06, LAB-Figure 01-07, Figure 04-09, Figure 04-10, Figure 04-11, Figure 06-06, Figure 06-17, Figure 06-18, Figure 07-29, Figure 07-34, Figure 07-37, Figure 07-39A, Figure 07-39B, Figure 07-40, Figure 08-07, Figure 08-17, Figure 08-18, Figure 08-28, Figure 09-17, Figure 09-18, Figure 09-19, Figure 09-20A, Figure 09-29, Figure 09-30, Figure 09-31, Figure 09-32, Figure 09-34, Figure 09-35A, Figure 09-36, Figure 09-39, Figure 09-43, Figure 09-45, Figure 09-46, Figure 10-45, Figure 10-51, Figure 10-65, Figure 12-16a, Figure 12-16b, Figure 12-21, Figure 13-34, Figure 13-40, Figure 13-58, Figure 13-59, Figure 13-63, Figure 13-67, Figure 13-69, Figure 13-71, Figure 13-73, Figure 13-75 to Figure 13-77, Figure 13-85 to Figure 13-97, Figure 13-55, Figure 14-02a, Figure 14-02b, Figure 14-03, Figure 14-04, Figure 14-05, Figure 14-06, Figure 14-07, Figure 14-08, Figure 14-09, Figure 14-10, Figure 14-11, Figure 14-12, Figure 14-13, Figure 14-14, Figure 14-15, Figure 14-16, Figure 14-19, Figure 14-20, Figure 14-21, Figure 14-22, Figure 14-23, Figure 14-24, LAB-Figure 14-01, LAB-Figure 14-02, LAB-Figure 14-03, LAB-Figure 14-01, LAB-Figure 14-02, LAB-Figure 14-03, UNFigure 14-01, UNFigure 14-02, UNFigure 14-06, UNFigure 14-07, Figure 15-01, Figure 15-03, Figure 15-04, Figure 15-06, Figure 15-07, Figure 15-08, Figure 15-09, Figure 15-10, Figure 15-11, Figure 15-12, Figure 15-13, Figure 15-14, Figure 15-15, Figure 15-18, Figure 15-19, Figure 15-20, Figure 15-21, Figure 15-22, Figure 15-23, Figure 15-24, Figure 15-25, Figure 15-26, Figure 15-27, Figure 15-28, Figure 15-29, Figure 15-30, Figure 15-31, Figure 15-32, Figure 15-33, Figure 15-34, LAB-Figure 15.01, Figure 16-01, Figure 16-06, Figure 16-07, Figure 16-08, Figure 16-09, Figure 16-10, Figure 16-11, Figure 16-12, Figure 16-14, Figure 16-15, Figure 16-16, Figure 16-17, Figure 16-18, Figure 16-19, Figure 16-20, Figure 16-21, Figure 16-22, Figure 16-23, Figure 16-24, Figure 16-25, Figure 16-26, Figure 16-27, Figure 16-28, Figure 16-29, Figure 16-31, Figure 16-32, Figure 16-33, Figure 16-34, Figure 16-35, Figure 16-36, Figure 16-37, Figure 16-38, Figure 16-39, Figure 16-40, Figure 16-41, Figure 16-42, Figure 16-43, Figure 16-44, Figure 16-45, Figure 16-46, Figure 16-47, Figure 16-48, Figure 16-49, Figure 16-51, Figure 16-52, Figure 16-53, Figure 16-54, Figure 16-55, Figure 16-57, Figure 16-58, Figure 16-59, Figure 16-60, Figure 16-61, Figure 16-62, Figure 16-63, Figure 16-64, Figure 16-65, Figure 16-66, Figure 16-67, Figure 18-16 to Figure 13-27, Figure 18-33, Figure 18-34, Figure 18-36, Figure 18-40, Figure 18-41, Figure 18-46 to Figure 13-50	© Microsoft 2025
Figure 02-13A	Vieloryb/123RF
Figure 02-01	Montree Saowang/Shutterstock
Figure 02-02A	kanvag/Shutterstock

Figure	Credits
Figure 02-02C	kanvag/Shutterstock
Figure 02-05	Mehmet Cetin/Shutterstock
Figure 02-06	Alexander_Evgenyevich/Shutterstock
Figure 02-07	Tuomas Lehtinen/Shutterstock
Figure 02-08	Shawn Hempel/Shutterstock
Figure 02-15	normaals/123RF
Figure 02-18	Adam Wasilewski/Shutterstock
Figure 02-19B	Peter Gudella/Shutterstock
Figure 02-20A	ravl/Shutterstock
Figure 02-20B	Feng Yu/Shutterstock
Figure 02-21	Ruslan Kudrin/Shutterstock
Figure 02-24A	arnut09job/123RF
Figure 02-27	kanvag/Shutterstock
Figure 02-29	Mau Horng/Shutterstock
Figure 02-30	Andrea Leone/Shutterstock
Figure 02-34A	Ferhat/Shutterstock
Figure 02-34B	Alexey Rotanov/Shutterstock
Figure 02-36	samsonovs/123RF
Figure 02-37	gefufna/123RF
Figure 02-39	pairoj903/123RF
Figure 02-40A	alehdats/123RF
Figure 02-40B	Mikhail hoboton Popov/Shutterstock
Figure 02-45	Unkas Photo/Shutterstock
Figure 02-46B	kanvag/Shutterstock
Figure 02-47D	Dragana Gerasimoski/Shutterstock
Figure 02-49A	MRS. NUCH SRIBUANOY/Shutterstock
Figure 02-49B	Alexander_Evgenyevich/Shutterstock
Figure 02-49C	ericlefrancais/Shutterstock
Figure 02-49D	Nata-Lia/Shutterstock
Figure 02-49E	ericlefrancais/Shutterstock
Figure 02-49F	Tuomas Lehtinen/Shutterstock
Figure 02-49G	1125089601/Shutterstock
Figure 02-49H	Mikhail hoboton Popov/Shutterstock
Figure 02-49J	Desintegrator/Shutterstock
Figure 03-01	Aleksei Lazukov/Shutterstock
Figure 03-02	madmaxer/123RF
Figure 03-11	Denis Dryashkin/Shutterstock
Figure 03-14	ruslanlytvyn/123RF
Figure 03-15	anmbph/123RF
Figure 03-16	Zadorozhnyi Viktor/Shutterstock
Figure 03-17	mark800/123RF
Figure 03-18	Denis Dryashkin/Shutterstock
Figure 03-19	Georgii Shipin/Shutterstock
Figure 03-22	Unkas Photo/Shutterstock
Figure 03-24	Zadorozhnyi Viktor/Shutterstock
Figure 03-28	BonD80/Shutterstock

Figure	Credits
Figure 03-32	wavebreakmedia/Shutterstock
Figure 04-01	daniidfoto/123RF
Figure 04-06	BonD80/Shutterstock
Figure 04-08	daniidfoto/123RF
Figure 04-13, Figure 05-10, Figure 10-16b	Wikimedia Commons
Figure 04-19	Stokkete/Shutterstock
Figure 05-35	Rafal Olechowski/Shutterstock
Figure 05-01	dmitr1ch/123RF
Figure 05-04	StockPhotosArt/Shutterstock
Figure 05-06	ironstuff/123RF
Figure 05-07	StockPhotosArt/Shutterstock
Figure 05-08A	cristi180884/Shutterstock
Figure 05-08B	BonD80/Shutterstock
Figure 05-12	thodonal/123RF
Figure 05-13	yemelyanov/123RF
Figure 05-17	anakeseenadee/123RF
Figure 05-18	chokmoso/Shutterstock
Figure 05-19	Richard z/Shutterstock
Figure 05-20	thodonal/123RF
Figure 05-21	dmitryi/123RF
Figure 05-26A	Olga Popova/Shutterstock
Figure 05-26B	cristi180884/Shutterstock
Figure 05-28	stasysk/123RF
Figure 05-31	sdm1984/123RF
Figure 05-33	Brazhnykov Andriy/Shutterstock
Figure 05-34	Qoncept/Shutterstock
Figure 06-01	Denis Dryashkin/Shutterstock
Figure 06-03	S.Dashkevych/Shutterstock
Figure 06-04	vetkit/Shutterstock
Figure 06-14	Joseph Scott Photography/Shutterstock
Figure 06-19	diegomaravilla/123RF
Figure 06-20	Svitlana Kataieva/Shutterstock
Figure 06-21	shaffandi/123RF
Figure 06-22	ESB Professional/Shutterstock
Figure 07-17	mbnq/123RF
Figure 07-01	photka/123RF
Figure 07-02	Net Vector/Shutterstock
Figure 07-03	scyther5/123RF
Figure 07-06	mbongo/123RF
Figure 07-07	SvedOliver/Shutterstock
Figure 07-11	Artush/Shutterstock
Figure 07-12	Matee Nuserm/Shutterstock
Figure 07-13	SvedOliver/Shutterstock
Figure 07-14A	servantes/Shutterstock

Figure	Credits
Figure 07-14B	servantes/Shutterstock
Figure 07-15A	ravl/Shutterstock
Figure 07-15B	scorpion26/123RF
Figure 07-15C	Crepesoles/Shutterstock
Figure 07-16A	maxoidos/123RF
Figure 07-16B	Lipowski Milan/Shutterstock
Figure 07-19	CyberVam/Shutterstock
Figure 07-20	daniidfoto/123RF
Figure 07-21	paylessimages/123RF
Figure 07-22	wavebreakmedia/Shutterstock
Figure 07-24	Igor Grochev/Shutterstock
Figure 07-25	believeinme33/123RF
Figure 07-26	MaxkyTH/Shutterstock
Figure 07-35	concept w/Shutterstock
Figure 07-42	Ilya Andriyanov/Shutterstock
Figure 07-44	GOODLUZ/Alamy Stock Photo
Figure 08-02	Designua/Shutterstock
Figure 08-03	Gorodenkoff/Shutterstock
Figure 08-04	golibtolibov/123RF
Figure 08-05	kitaec/123RF
Figure 08-08	Mny-Jhee/Shutterstock
Figure 08-09	Jan Mika/Shutterstock
Figure 08-12	Istvan Csak/Shutterstock
Figure 08-14	Denis Dryashkin/Shutterstock
Figure 08-15	Oleksandr Lysenko/Shutterstock
Figure 08-19	DenisProduction.com/Shutterstock
Figure 08-21	pathdoc/Shutterstock
Figure 08-24	Song_about_summer/Shutterstock
Figure 08-27	Olha Vlasiuk/Shutterstock
Figure 08-29	Valeriy Lebedev/Shutterstock
Figure 08-30	Gustavo Frazao/Shutterstock
Figure 09-01	ProstoSvet/Shutterstock
Figure 09-02	burnel1/123RF
Figure 09-05	Sinisa Botas/Shutterstock
Figure 09-08	Dario Sabljak/Shutterstock
Figure 09-10	manaemedia/Shutterstock
Figure 09-11	Michal Vitek/Shutterstock
Figure 09-12	vetkit/Shutterstock
Figure 09-14	Zern Liew/Shutterstock
Figure 09-15, Figure 09-22, Figure 19-09	Gareth Boden/Pearson Education Ltd
Figure 09-21	kitaec/123RF
Figure 09-23	esbobeldijk/Shutterstock
Figure 09-25	artranq/123RF
Figure 09-37	ldprod/123RF

Figure	Credits
Figure 09-40	Daniel Krason/Shutterstock
Figure 09-41, Figure 10-11, Figure 10-32	©2025 Google
Figure 09-42	kitaec/123RF
Figure 09-44	Michael Pettigrew/Shutterstock
Figure 10-23	© 2025 Bluetooth SIG, Inc
Figure 10-01	multicanarias/123RF
Figure 10-02	ZouZou/Shutterstock
Figure 10-03	RHJPhtotos/Shutterstock
Figure 10-04	forest71/Shutterstock
Figure 10-05	Moreno Soppelsa/Shutterstock
Figure 10-06	3DMAVR/Shutterstock
Figure 10-07	Renars 2013/Shutterstock
Figure 10-08	Oleg Troino/Shutterstock
Figure 10-09	Olga Popova/Shutterstock
Figure 10-10	Jason Nemeth/Shutterstock
Figure 10-12, Figure 10-29, Figure 10-33, Figure 10-35, Figure 10-66, Figure 10-71, Figure 17-02, Figure 17-03, Figure 17-04, Figure 17-05, Figure 17-06, Figure 17-07, Figure 17-08, Figure 17-09, Figure 17-10, Figure 17-11, Figure 17-12, Figure 17-13, Figure 17-14, Figure 17-15	Copyright © 2025 Apple Inc
Figure 10-14a	Blackboard/Shutterstock
Figure 10-14b	Eric Buell Photography/Shutterstock
Figure 10-16a	Brian A Jackson/Shutterstock
Figure 10-18	prykhodov/123RF
Figure 10-21	Anton Starikov/Shutterstock
Figure 10-22	highwaystarz/123RF
Figure 10-24	fkdkondmi/Shutterstock
Figure 10-25	Oleksiy Mark/Shutterstock
Figure 10-27	leaf/123RF
Figure 10-30	ProStockStudio/Shutterstock
Figure 10-31	Christos Georghiou/Shutterstock
Figure 10-37	andreypopov/123RF
Figure 10-43a	fserega/123RF

Figure	Credits
Figure 10-43b	ratmaner/123RF
Figure 10-44a	NET_Photog/Shutterstock
Figure 10-44b	JIPEN/Shutterstock
Figure 10-47	Romash Denis/Shutterstock
Figure 10-50	Joggie Botma/Shutterstock
Figure 10-54b	Piotr Adamowicz/123RF
Figure 10-56	JIPEN/Shutterstock
Figure 10-57	H_Ko/Shutterstock
Figure 10-64	tab62/Shutterstock
Figure 10-67	hit003/123RF
Figure 10-68	Yomka/Shutterstock
Figure 10-69	kulyk/Shutterstock
Figure 10-70	selinofoto/Shutterstock
Figure 10-72	NataLT/Shutterstock
Figure 10-73	kovalska/123RF
Figure 10-74	weerapat/123RF
Figure 10-75	Pasko Maksim/Shutterstock
Figure 10-76	pixssa/Shutterstock
Figure 10-77	Tartila/Shutterstock
Figure 10-78	grafvision/Shutterstock
Figure 11-01	artellia/123RF
Figure 11-02	Corepics VOF/Shutterstock
Figure 11-03	Dejan Stanic Micko/Shutterstock
Figure 11-04	Stocked House Studio/Shutterstock
Figure 11-05	300dpi/123RF
Figure 11-06	MilousSK/Shutterstock
Figure 11-07	Kittichai/Shutterstock
Figure 11-08	improvize/Shutterstock
Figure 11-09	RAJ CREATIONZS/Shutterstock
Figure 11-10	mikeledray/Shutterstock
Figure 11-11	DeSerg/Shutterstock
Figure 11-12	Natalia Siverina/Shutterstock
Figure 11-13	Andriy Popov/123RF
Figure 11-14	Phovoir/Shutterstock
Figure 11-15	sirgunchik/123RF
Figure 11-17	Galyna Andrushko/Shutterstock
Figure 11-22	Sashkin/Shutterstock
Figure 11-26	imtmphoto/123RF
Figure 12-03	Evan Lorne/Shutterstock
Figure 12-04	Roman Pyshchyk/Shutterstock
Figure 12-05	S1001/Shutterstock
Figure 12-06	Suti Stock Photo/Shutterstock
Figure 12-07	Andrey_Popov/Shutterstock
Figure 12-11	federicofoto/123RF
Figure 12-14	dr911/123RF
Figure 12-17	JustAnotherPhotographer/Shutterstock

Figure	Credits
Figure 12-19	Zern Liew/Shutterstock
Figure 12-23	Marishatti/Shutterstock
Figure 12-27	stockasso/123RF
Figure 13-01	karelnoppe/123RF
Figure 13-03	siiixth/Shutterstock
Figure 13-04	TechnoVectors/Shutterstock
Figure 13-05	FrameStockFootages/Shutterstock
Figure 13-06	Lia Gloss/Shutterstock
Figure 13-07	Arjuna Kodisinghe/Shutterstock
Figure 13-08	kubais/Shutterstock
Figure 13-100a	Evan Lorne/Shutterstock
Figure 13-100b	Oleksiy Mark/Shutterstock
Figure 13-100c	Structured Vision/Shutterstock
Figure 13-100d	svetlanaangelus/123RF
Figure 13-100e	dotshock/Shutterstock
Figure 13-102	Nikonaft/Shutterstock
Figure 13-11	SKT Studio/Shutterstock
Figure 13-12	Georgios Alexandris/Shutterstock
Figure 13-16a	Duard van der Westhuizen/Shutterstock
Figure 13-16b	Zakhar Mar/Shutterstock
Figure 13-17	Fotofermer/Shutterstock
Figure 13-18	ludinko/Shutterstock
Figure 13-19a	Everything I Do/Shutterstock
Figure 13-19b	Anthony O'Donnell/Shutterstock
Figure 13-20	Plus69/Shutterstock
Figure 13-24	eugenesergeev/123RF
Figure 13-25	SeventyFour/Shutterstock
Figure 13-26	svetlanaangelus/123RF
Figure 13-27	hxdyl/123RF
Figure 13-29	Plus69/Shutterstock
Figure 13-30	gregg williams/Shutterstock
Figure 13-38	Christos Georghiou/Shutterstock
Figure 13-39	diabl/123RF
Figure 13-41	Magnetic Mcc/Shutterstock
Figure 13-44, Figure 13-52a, Figure 13-52b, Figure 13-60, Figure 13-61	© 2025 TP-Link Systems Inc.
Figure 13-66	alphaspirit/Shutterstock
Figure 13-72	PGMart/Shutterstock
Figure 13-78	Denis Dryashkin/Shutterstock
Figure 13-79	ultramcu/123RF
Figure 13-81	riverlim/123RF
Figure 13-82	aleksanderdn/123RF
Figure 13-83	elenabsl/Shutterstock
Figure 13-99	Peter Kotoff/Shutterstock

Figure	Credits
LAB-Figure 13-01	Aliaksandr Bukatsich/Shutterstock
LAB-Figure 13-02	Darkwisper S/Shutterstock
LAB-Figure 13-03	Georgios Alexandris/Shutterstock
LAB-Figure 13-04	a_v_d/Shutterstock
LAB-Figure 13-05	samsonovs/123RF
Figure 15-16	calado/shutterstock
Figure 15-17	Yury Zap/shutterstock
LABFigure 15.01, LABFigure 15.02, LABFigure 15.03, LABFigure 15.05	© Copyright 2001-2025, Python Software Foundation.
Figure 16-02	iuriimotov/123RF
Figure 16-03	binaryproject/123RF
Figure 16-04	scanrail/shutterstock
Figure 16-05	jijomathaidesigners/Shutterstock
Figure 16-30	anyaberkut/123RF
Figure 16-50	siiixth/123RF
Figure 16-56	ojogabonitoo/123RF
Figure 16-68	AntiMartina/shutterstock
Figure 17-01	belchonock/123RF
Figure 17-16, Figure 17-17, Figure 17-18, Figure 17-19, Figure 17-20, Figure 17-21a, Figure 17-21b, Figure 17-22, Figure 17-23, Figure 17-24	© 2025 Canonical Ltd
Figure 18-01	gorlovkv/123RF
Figure 18-02	gifted/Shutterstock
Figure 18-03	apatrimonio/Shutterstock
Figure 18-04	anjonik/123RF
Figure 18-06	qingwa/123RF
Figure 18-07	Demetrio Media/Shutterstock
Figure 18-08	all_is_magic/Shutterstock
Figure 18-09	liudmilachernetska/123RF
Figure 18-10	buchachon/123RF
Figure 18-11	nicescene/123RF
Figure 18-12	ocusfocus/123RF
Figure 18-13	Cartoon Resource/Shutterstock
Figure 18-14	Nicescene/Shutterstock
Figure 18-15	JustAnotherPhotographer/Shutterstock

Figure	Credits
Figure 18-28	escova/Shutterstock
Figure 18-30	Bedrin/Shutterstock
Figure 18-31	lukassek/123RF
Figure 18-35	Red Vector/Shutterstock
Figure 18-37	alexmit/123RF
Figure 18-38	Oez/Shutterstock
Figure 18-44	marigranula/123RF
Figure 18-51	iqoncept/123RF
Figure 19-01	Rawpixel.com/Shutterstock
Figure 19-02	ESB Professional/Shutterstock
Figure 19-03	photosync/Shutterstock
Figure 19-04	ninun/123RF
Figure 19-05	AlisaRut/Shutterstock
Figure 19-06	petovarga/123RF
Figure 19-07	wk1003mike/Shutterstock
Figure 19-08	enterphoto/Shutterstock
Figure 19-10	Pepermpron/Shutterstock
Figure 19-11	evilratalex/123RF
Figure 19-12	bwf211/123RF
Figure 19-13	Winai Tepsuttinun/Shutterstock
Figure 19-14a	Mile Atanasov/Shutterstock
Figure 19-14b	vetkit/Shutterstock
Figure 19-19	Yury Asotov/Shutterstock
Figure 19-20	PrasitRodphan/Shutterstock
Figure 19-24	Benjamin Haas/Shutterstock
Figure 19-25	Kheng Guan Toh/Shutterstock
Figure 19-26	desdemona72/Shutterstock
Figure 19-27	Cartoon Resource/Shutterstock
Figure 19-28	beatpavel/123RF
Figure 19-29	iqoncept/123RF
Figure 19-31	iqoncept/123RF
Figure 19-32	studiostoks/123RF
Figure 19-33	andrewgenn/123RF
Figure 19-34	Flashon Studio/Shutterstock

Contents at a Glance

Introduction xxv
Features of This Book xxvii
Chapter 1: Introduction to the World of IT 1
Chapter 2: Connectivity 29
Chapter 3: On the Motherboard 65
Chapter 4: Introduction to Configuration 103
Chapter 5: Disassembly and Power 135
Chapter 6: Memory 177
Chapter 7: Storage Devices 213
Chapter 8: Video and Multimedia Devices 263
Chapter 9: Printers/Multifunction Devices 301
Chapter 10: Mobile Devices 357
Chapter 11: Computer Design and Troubleshooting Review 439
Chapter 12: Internet Connectivity, Virtualization, and Cloud Technologies 479
Chapter 13: Networking 517
Chapter 14: Introduction to Operating Systems 613
Chapter 15: Introduction to Scripting 655
Chapter 16: Advanced Windows 721
Chapter 17: macOS and Linux Operating Systems 817
Chapter 18: Computer and Network Security 861
Chapter 19: Operational Procedures 941
Appendix A: Subnetting Basics 985
Index 991

Online Only Elements

Appendix B: Certification Exam Objectives
Glossary

Contents

Introduction xxv

Features of This Book xxvii

Chapter 1: Introduction to the World of IT 1

Who Needs This Book? 2
Technician Qualities 2
Breaking into IT with the CompTIA A+ Certification 5
Basic Skills for This Course 5
Types of Computers 8
Basic Computer Hardware 8
Mice and Keyboards 14
Common Peripherals 17
1s and 0s 18
Safety Notes 20
Chapter Summary 21
Key Terms 22
Review Questions 23
Exercises 25
Exercise 1.1 Identifying Tower Computer Parts 25
Exercise 1.2 Identifying Computer Parts 27
Activities 27
Internet Discovery 27
Soft Skills 28
Critical Thinking Skills 28

Chapter 2: Connectivity 29

Introduction to Connectivity 30
External Connectivity 30
Mouse and Keyboard Ports 30
Video Ports 38
Audio Ports 43
eSATA Ports 43
Modem and Serial Ports 44
Network Ports 46
Network Cabling 47
Integrated Motherboard Ports 53
Getting to Know Ports 53
Wireless Connectivity for Input Devices 55
Chapter Summary 56
Key Terms 57
Review Questions 58
Exercises 59
Exercise 2.1 Identifying Computer Ports 59
Exercise 2.2 Identifying More Computer Ports 60
Exercise 2.3 Identifying Display Ports 60
Exercise 2.4 Identifying USB Ports 61
Exercise 2.5 Identifying Cables 62

Activities 62
Internet Discovery 62
Soft Skills 63
Critical Thinking Skills 63

Chapter 3: On the Motherboard 65
Introduction to the Motherboard 66
Processor Overview 66
Processor Basics 67
Speeding Up Processor Operations Overview 68
Cache 69
Connecting to the Processor 70
Multicore Processors 71
Graphics Processing Unit (GPU) 72
Introduction to Virtualization Support 73
Intel Processors 74
AMD Processors 75
CPU Sockets 76
Processor Cooling 77
Installing a Processor 78
Upgrading Processors 80
Overclocking Processors 80
Installing CPU Thermal Solutions 81
Troubleshooting Processor Issues 82
Expansion Slots 83
PCI (Peripheral Component Interconnect) 83
PCIe (Peripheral Component Interconnect Express) 84
Motherboard Security Options 87
Types of Motherboards 88
Upgrading and Replacing Motherboards 89
Motherboard Troubleshooting 90
Chapter Summary 93
Key Terms 94
Review Questions 95
Exercises 97
Exercise 3.1 Identifying ATX Motherboard Parts 97
Exercise 3.2 Motherboard Analysis 98
Activities 99
Internet Discovery 99
Soft Skills 100
Critical Thinking Skills 101

Chapter 4: Introduction to Configuration 103
Configuration Overview 104
BIOS Overview 104
UEFI 105
BIOS/UEFI Configuration Settings 107
CMOS Memory 110
Flashing/Clearing the BIOS/UEFI 112
Other Configuration Parameters 113

Hardware Configuration Overview 115
Installing a USB Device 117
Installing an eSATA Card 120
Installing a Network Interface Card 121
Troubleshooting Configurations 122
Chapter Summary 124
Key Terms 124
Review Questions 125
Exercises 127
Exercise 4.1 System Expansion 127
Exercise 4.2 BIOS/UEFI Options 129
Activities 131
Internet Discovery 131
Soft Skills 132
Critical Thinking Skills 132

Chapter 5: Disassembly and Power 135
Disassembly Overview 136
Electrostatic Discharge (ESD) 136
Electromagnetic Interference (EMI) 138
Tools 139
Disassembly 140
Reassembly 147
Preventive Maintenance 147
Basic Electronics Overview 150
Power Supply Overview 153
Replacing or Upgrading a Power Supply 160
Power Protection 162
Symptoms of Power Supply Problems 163
Chapter Summary 167
Key Terms 168
Review Questions 169
Exercises 172
Exercise 5.1 Identifying Power Supply Connectors 172
Exercise 5.2 Recognizing Computer Replacement Parts 172
Exercise 5.3 Describing Computer Parts 173
Activities 173
Internet Discovery 173
Soft Skills 174
Critical Thinking Skills 175

Chapter 6: Memory 177
Memory Overview 178
Memory Physical Packaging 178
Planning a Memory Installation 179
Installing Memory Overview 190
Virtual RAM 192
Monitoring Memory Usage in Windows 193
Older Applications in Windows 195

Troubleshooting Memory Problems 195
Removable Storage 197
Chapter Summary 201
Key Terms 202
Review Questions 203
Exercises 205
Exercise 6.1 Configuring Memory on Paper 205
Exercise 6.2 Configuring Memory on Paper 206
Exercise 6.3 Configuring Memory on Paper 208
Exercise 6.4 Configuring Memory on Paper 210
Activities 211
Internet Discovery 211
Soft Skills 212
Critical Thinking Skills 212

Chapter 7: Storage Devices 213
Storage Devices Overview 214
Hard Drive Overview 215
Solid-State Drive (SSD) Overview 217
Mechanical Drive Interfaces Overview 219
SATA and SAS Connectivity 220
Storage Device Configuration Overview 222
System BIOS/UEFI Configuration for Storage Devices 228
Hard Drive Preparation Overview 229
Windows Disk Management 236
Fault Tolerance 238
Windows Storage Spaces 240
Disk Caching/Virtual Memory 241
Troubleshooting Storage Devices Overview 243
Data Loss and Corruption 245
Troubleshooting New Storage Device Installation 246
Troubleshooting Previously Installed Storage Devices 247
RAID Issues 251
SSD Issues 251
Chapter Summary 253
Key Terms 255
Review Questions 256
Exercises 258
Exercise 7.1 Planning Storage Device Installation and Configuration 258
Exercise 7.2 Configuring a SATA Hard Drive on Paper 259
Activities 261
Internet Discovery 261
Soft Skills 262
Critical Thinking Skills 262

Chapter 8: Video and Multimedia Devices 263
Multimedia Devices Overview 264
Video Overview 264
Projectors 274
Introduction to Audio 276

Sound Cards Using Windows 279
Speakers 281
Troubleshooting Sound Problems 282
Optical Drive Overview 283
Optical Drive Installation 286
Troubleshooting Optical Drive Issues 286
Scanners 287
Other Multimedia Devices 290
Chapter Summary 293
Key Terms 294
Review Questions 295
Exercises 297
Exercise 8.1 Video and Multimedia Device Research 297
Exercise 8.2 Which One Will You Buy? 298
Activities 298
Internet Discovery 298
Soft Skills 299
Critical Thinking Skills 300

Chapter 9: Printers/Multifunction Devices 301
Printer/Multifunction Device Overview 302
Categories of Printers 302
Impact Printers 303
Inkjet Printers 305
Laser Printers 308
Thermal Printers 311
Paper 313
Virtual Printing 316
Refilling Cartridges, Re-inking Ribbons, and Recycling Cartridges 317
Upgrading Printers 318
Printer Maintenance 318
Printer Installation Overview 324
Installing Multifunction Devices 326
USB Printer Installation 326
Printers in the Windows Environment 327
Printer Sharing 332
Cloud Printing/Scanning 337
General Printer Troubleshooting 338
Chapter Summary 349
Key Terms 350
Review Questions 351
Exercises 353
Exercise 9.1 Research a Local Printer 353
Exercise 9.2 Printer Driver Research 353
Activities 354
Internet Discovery 354
Soft Skills 354
Critical Thinking Skills 355

Chapter 10: Mobile Devices **357**
Mobile Device Overview 358
Using Mobile Devices 364
Cell Phones 366
Mobile Apps 368
Mobile Device Wired Connectivity 371
Mobile Device Wireless Connectivity 373
Mobile Device Email Configuration 379
Mobile Device Synchronization and Backup 381
Other Mobile Software Tools 385
Laptops Overview 387
Laptop Hardware 387
Laptop Power 391
Laptop Repairs Overview 394
Mobile Device Security 410
Mobile Device Troubleshooting Overview 415
Chapter Summary 429
Key Terms 431
Review Questions 432
Exercises 434
Exercise 10.1 Identifying Laptop Parts 434
Exercise 10.2 Common Laptop Keys 435
Exercise 10.3 Where's the Part? 435
Activities 436
Internet Discovery 436
Soft Skills 437
Critical Thinking Skills 437

Chapter 11: Computer Design and Troubleshooting Review **439**
Design Overview 440
Computer System Design 441
Motherboard and Associated Component Design 447
Power Supply and Case Design 447
Storage Subsystem Design 449
Audio Subsystem Design 449
Display Subsystem Design 450
Troubleshooting Overview 451
Step 1. Identify the Problem 452
Step 2. Establish a Theory of Probable Cause (Question the Obvious) 453
Step 3. Test the Theory to Determine the Cause 461
Step 4. Establish a Plan of Action to Resolve the Problem and Implement the Proposed Solution 463
Step 5. Verify Full System Functionality and, If Applicable, Implement Preventive Measures 463
Step 6. Document the Findings, Actions, and Outcomes 463
Sample Troubleshooting Flowcharts 464
Chapter Summary 468
Key Terms 469
Review Questions 470

Exercises 471
Exercise 11.1 Recommending Computer System Design 471
Exercise 11.2 Understanding Design Components 473
Exercise 11.3 Understanding Subsystem Design Components 474
Exercise 11.4 Determining the Troubleshooting Process Step 476
Activities 476
Internet Discovery 476
Soft Skills 478
Critical Thinking Skills 478

Chapter 12: Internet Connectivity, Virtualization, and Cloud Technologies 479
Internet Connectivity Overview 480
Dial-up Connectivity 480
Cable Modems 482
xDSL Modems 483
VoIP 484
Fiber Networks 486
Satellite Modems 488
Mobile/Cellular Connectivity Overview 489
Web Browsers 492
Introduction to Virtualization 498
Containers 503
Cloud Computing 503
Chapter Summary 509
Key Terms 511
Review Questions 512
Exercises 513
Exercise 12.1 Exploring Internet Connectivity Options 513
Exercise 12.2 Exploring the Internet Options Window 514
Activities 515
Internet Discovery 515
Soft Skills 515
Critical Thinking Skills 516

Chapter 13: Networking 517
Networking Overview 518
Network Media Overview 525
Ethernet over Power 534
Protecting Your Network and Cable Investment 535
The OSI Model 538
The TCP/IP Model 540
Network Addressing 542
More IPv4 Addressing 543
Wireless Networks Overview 546
Wireless Network Standards 547
Wireless Network Components 548
Wireless Network Design 550
Wireless and Wired Client Device Configuration Overview 559
Configuring an End Device: IP Addressing 560
Adding a Computer to a Windows Domain 566

Wireless NIC–Specific Settings 567
Advanced NIC Properties 568
NIC Configuration When Using Virtualization 569
Wireless AP/Router Configuration 570
WWAN Cellular Configuration 572
IoT and Smart Devices 572
Network Troubleshooting 573
Networking Multifunction Devices 582
Network Servers 584
Embedded, SCADA, and Legacy Systems 585
Software-Defined Networking 586
Network Terminology 587
The TCP/IP Model in Action 588
More Windows Network Settings 590
Introduction to Shared Folders 594
Chapter Summary 598
Key Terms 601
Review Questions 602
Exercises 604
Exercise 13.1 Understanding Wireless AP Paper Configuration 604
Exercise 13.2 Understanding T568B Color Sequence 605
Exercise 13.3 Recognizing Network Devices 606
Exercise 13.4 Identifying Basic Wireless Network Parts 606
Exercise 13.5 Wireless Network Case Study 607
Exercise 13.6 Practicing with Network Numbers and Broadcast Addresses 608
Exercise 13.7 Practicing with CIDR Notation 608
Exercise 13.8 Determining the Default Gateway 609
Activities 610
Internet Discovery 610
Soft Skills 611
Critical Thinking Skills 612

Chapter 14: Introduction to Operating Systems 613
Operating Systems Overview 614
User Interaction with Operating Systems 615
Overview of Popular Operating Systems 616
32-Bit vs. 64-Bit Operating Systems 617
Windows 11 Versions 618
Workstation Operating Systems 619
Operating Systems for Mobile Devices 619
End-of-Life (EOL) Concerns 620
Update Limitations 620
Compatibility Concerns 621
Corporate Operating System Needs 621
Basic Windows Usage Overview 623
Windows 11 Desktop Components 624
Shortcuts 627
Recycle Bin 628
Interactions Within a Window 629

Managing Windows Files and Folders 630
Searches and Indexing 635
Attributes, Compression, and Encryption 637
Introduction to Windows Settings 640
Determining the Windows Version 642
Windows Registry 643
Editing the Windows Registry 643
Backing Up Data 644
WinRE 645
Recovering the Windows OS 645
Chapter Summary 647
Key Terms 648
Review Questions 649
Exercises 650
Exercise 14.1 Windows Settings Categories 650
Exercise 14.2 Common Operating Systems 651
Exercise 14.3 CLI vs GUI 651
Activities 652
Internet Discovery 652
Soft Skills 652
Critical Thinking Skills 653

Chapter 15: Introduction to Scripting 655
Scripting Overview 656
Command Prompt Overview 656
Command Prompt Basics 657
Moving Around from a Command Prompt 659
The `md` and `rd` Commands 662
Two Useful Commands: `del` and `type` 663
Copying Files 664
The `attrib` Command 665
Why Learn Commands? 666
PowerShell 666
Other Commands You Should Look Over 667
Command Format 668
Introduction to Scripting 692
Script File Types 693
Use Cases for Scripting 694
Mitigating Consequences of Scripting 695
Environment Variables 696
Script Syntax 698
Introduction to Script Programming 699
Variables 699
Data Types 701
Examples of Using Variables 702
Comments Within Scripts 703
Basic Script Constructs 704
Decisions: The Selection Structure 704
Compound Conditions and Logical Operators 708

Loops: The Repetition Structure 708
A Brief Look at VBScript and PowerShell 711
Chapter Summary 714
Key Terms 715
Review Questions 716
Exercises 717
Exercise 15.1 Identifying Command-Line Commands 717
Exercise 15.2 Scripting Concepts 718
Activities 718
Internet Discovery 718
Soft Skills 719
Critical Thinking Skills 719

Chapter 16: Advanced Windows 721
Advanced Windows Overview 722
Preinstallation of Windows 722
Installation/Upgrade of Windows 732
Corporate Windows Deployment 733
Verifying the Installation 735
Troubleshooting a Windows Installation 735
System Restore 737
Reloading Windows 737
Windows Updates 739
Backing Up the Windows Registry and Data 740
Configuring Windows Overview 741
Configuring Windows 743
Adding Devices 743
Installing/Removing Software 750
Computer Management Console 754
System Tools 755
User Account Management 759
Managing Storage 765
Managing Services and Applications 769
Data Sources (ODBC) 770
Print Management Console 771
Overview of the Windows Boot Process 772
Windows Recovery Environment (WinRE) 773
Startup Settings Menu 776
Task Manager 782
Monitoring System Performance 784
Speeding Up the Windows Boot Process 789
Troubleshooting the Windows Boot Process 790
Black Screen/Video Issues 792
Troubleshooting a Service That Does Not Start 793
Slow Boot 795
Troubleshooting Windows Network Settings 796
Windows Reboots/System Instability 797
Shutdown Problems 798
Summary of Troubleshooting Steps 799

Power Options 799
Supporting Windows Computers Remotely 801
Preventive Maintenance for Your Operating System 803
Cloud-Based Productivity Tools 804
Chapter Summary 809
Key Terms 811
Review Questions 812
Exercises 813
Exercise 16.1 Using Windows Tools 813
Exercise 16.2 Using Task Manager Tabs 814
Exercise 16.3 Using System Configuration Tabs 815
Activities 815
Internet Discovery 815
Soft Skills 816

Chapter 17: macOS and Linux Operating Systems 817
Introduction to macOS 818
Navigating the User Interface 819
Basic System Usage, Applications, Updates, and Backups 822
Management and Troubleshooting Tools 827
Utilities 830
Introduction to Linux 839
OS Components and Common Configuration Files 840
Navigating the User Interface 840
Basic System Usage, Updates, and Backups 842
Command-Line Interface 845
macOS and Linux Best Practices 854
Chapter Summary 855
Key Terms 856
Review Questions 857
Exercises 858
Exercise 17.1 macOS Tools 858
Exercise 17.2 macOS Commands 858
Activities 859
Internet Discovery 859
Soft Skills 859
Critical Thinking Skills 860

Chapter 18: Computer and Network Security 861
Security Overview 862
Security Policy 862
Physical Security 863
Logical Security 870
Considering the End User 875
Licensing 876
Security Threats and Vulnerabilities 878
Protecting Access to Local and Network Resources 884
Permissions 891

Folder Options 897
Protecting the Operating System and Data 898
Internet Security 906
Remote Access to Network Devices 918
Internet Appliances 920
Wireless Network Security Overview 921
Security Incident Response 928
A Final Word About Security 930
Chapter Summary 932
Key Terms 934
Review Questions 935
Exercises 937
Exercise 18.1 Examining the Security Incident Response 937
Exercise 18.2 Wireless Security 938
Exercise 18.3 Data Security 938
Activities 939
Internet Discovery 939
Soft Skills 940
Critical Thinking Skills 940

Chapter 19: Operational Procedures 941
Operational Procedures Overview 942
Proper Power Handling and Adverse Power Conditions 951
IT Documentation 959
Change Management 964
Chapter Summary 975
Key Terms 977
Review Questions 978
Exercises 980
Exercise 19.1 Determining a Power Solution 980
Exercise 19.2 Determining the Type of Documentation Needed 981
Activities 981
Internet Discovery 981
Soft Skills 982
Critical Thinking Skills 983

Appendix A: Subnetting Basics 985
Exercise 988
Exercise A.1 Subnet Practice Exercise 988

Index 991

Online Only Elements

Appendix B: Certification Exam Objectives

Glossary

About the Authors

Cheryl Schmidt is a professor of Network Engineering Technology at Florida State College at Jacksonville. Prior to joining the faculty ranks, she oversaw the LAN and PC support for the college and other organizations. She started her career as an electronics technician in the U.S. Navy. She teaches computer repair and various networking topics, including CCNA, network management, and network design. She has published other works with Pearson, including *IP Telephony Using CallManager Express* and *Routing and Switching in the Enterprise Lab Guide*.

Cheryl has won awards for teaching and technology, including Outstanding Faculty of the Year, Innovative Teacher of the Year, Cisco Networking Academy Instructor Excellence Award, and Cisco Networking Academy Stand Out Instructor. She has presented at U.S. and international conferences. Cheryl keeps busy maintaining her technical certifications and teaching but also loves to travel, hike, do all types of puzzles, and read.

Christopher Lee teaches Information Technology, Electronics, and Robotics at Florida State College at Jacksonville. A native of Greenville, South Carolina, Chris earned a bachelor's degree and a master's degree in Electrical Engineering from Georgia Institute of Technology. He taught his first computer programming classes at age 14! Since then, he has worked for a variety of companies, including IBM, Nortel Networks, Evans Solutions, Convergys Corporation, NGA Human Resources, and himself. His experience spans several industries: telecommunications, youth outside the educational mainstream, information technology, higher education, human resources outsourcing, and community development.

Chris has devoted countless volunteer hours to technology outreach. He enjoys helping children and adults (especially those in underserved communities) learn the skills and access the resources they need in order to be competitive in today's technological society. He has built strong partnerships with and implemented successful programs in organizations such as National Society of Black Engineers Jr (NSBE Jr), FIRST LEGO® League, Mentoring Families and Kids, Tristan's Acceleration Academy, and Builders of Tomorrow.

Dedications

A Note to Instructors from Cheryl Schmidt:

I was a teacher long before I had the title professor. Sharing what I know has always been as natural as walking to me, but sitting still to write what I know is not as natural, so composing this text has always been one of my greatest challenges. Thank you so much for choosing this text. I thank you for sharing your knowledge and experience with your students. Your dedication to education is what makes the student experience so valuable.

A Note to Students from Cheryl Schmidt:

Writing a textbook is really different from teaching class. I have said for years that my students are like my children, except that I don't have to pay to send them through college. I am happy to claim any of you who have this text. I wish that I could be in each classroom with you as you start your IT career. How exciting!

Another thing that I tell my students is that I am not an expert. IT support is an ever-changing field, and I have been in it since PCs started being used. You have to be excited about the never-ending changes to be good in this field. You can never stop learning, or you will not be very good anymore. I offer one important piece of advice:

> Consistent, high-quality service boils down to two equally important things: caring and competence.
> —Chip R. Bell and Ron Zemke

I dedicate this book to you, the reader. I can help you with the competence piece, but you are going to have to work on the caring part. Do not ever forget that there are people behind those machines that you love to repair. Taking care of people is as important as taking care of the computers.

A Note to Students from Chris Lee:

I dedicate this book to my late grandfather, Roosevelt Nelson. During our weekly phone calls, he would often ask me, "What projects are you working on, son?" The list would include a variety of things like remote server labs, robotic competitions, car repairs, lawn sprinkler systems, summer camp workshops, home renovations, or new recipes. Sometimes, he would say, "You'll never go hungry with all those skills."

He encouraged me to learn as much as possible so I could choose the life I want to live. I offer the same advice to everyone who uses this book. The CompTIA A+ Certification is a gateway to many amazing opportunities in information technology. As you travel along this journey, take time to explore other facets of life, either as hobbies or as careers. You'll appreciate the diversion from the pressures of the IT world, and you'll discover people and ideas that you would otherwise never experience. This additional education (whether formal or informal) will increase your "value" at home, in your profession, and throughout your community.

Acknowledgments

From Cheryl Schmidt:

I am so thankful for the many blessings from God throughout my lifetime and the support of my family during the production of this book. My husband, Karl, daughter, Raina, and son-in-law, Marc, are always a source of encouragement. My grandsons, Gavin, Riley, Logan, and Liam, and my granddaughters, Brie and Liv, are a constant source of wonderment for me. They are shining lights for me. Thanks to my mother, Barbara Cansler, who recently passed and who taught me to love words and my brother Jeff Cansler for just listening. Thanks to my walking buddy, Kellie, for the miles of letting me work through knotty sections. Thanks to my colleagues, adjuncts, and students at my college who offered numerous valuable suggestions for improvement and tested the new material. A special thanks to my colleagues Pamela Brauda and David Singletary as well as Jason Brenneman for helping me with my weak areas. Finally,

I want to thank my co-author and a great teacher, Chris Lee as well as my personal technical team, Justin Ache, Raina Durrence, and Jeff Burns.

Many thanks are also due the folks at Pearson. The professionalism and support given during this edition was stellar. Thank you so much, Pearson team, especially James Manly, Eleanor Bru, Kitty Wilson, Mandie Frank, and a wonderful technical reviewer, Justin Valentino. I hope all of you can see the results of your contributions. I thank the whole team so much for your conscientious efforts.

Finally, thank you to the students who have taken the time to share their recommendations for improvement. You are the reason I write this book each time. Please send me any ideas and comments you may have. I love hearing from you and of your successes. I may be reached at cheryl.schmidt@fscj.edu.

From Chris Lee:

I am thankful for the lifetime of support and guidance that have enabled me to achieve my dreams and contribute to this book. My parents, Brenda McClinton and Herman Brown, have always encouraged me to follow my own path. They have also been my favorite remote "clients," as they have embraced computer technology, whereas many of their peers find it intimidating. My grandparents, Roosevelt (deceased) and Bettye Nelson, have always been my biggest cheerleaders; Grandma still reminds me to take some time for myself in the midst of all that I do. I appreciate the patience and motivation from my son, Jawara, as he discovers his own niche in the world of video game programming and in life itself. And I thank my colleague and principal author Cheryl Schmidt for the wealth of guidance during my career at Florida College at Jacksonville and for the opportunity to contribute to this book.

Some very special teachers also deserve recognition. Mr. William Marshall at the Phyllis Wheatley Community Center allowed me to make or build whatever I wanted in the arts and crafts room. He saw the budding engineer in me and allowed me to discover my passion. Mrs. Linda Dillard at Duncan Chapel Elementary School instilled the discipline that I needed to stay focused amid so many distractions. Mrs. Jeanne Perkinson at Wade Hampton High School took my B.A.S.I.C. programming to the next level and introduced me to structured programming. Dr. George Lee Cain helped me weather my first term at Georgia Tech. OMED Student Services and Dr. Gary S. May at Georgia Tech gave me numerous resources to navigate college life and exposed me to several opportunities to develop my skills and serve my community.

We Want to Hear from You!

As the reader of this book, *you* are our most important critic and commentator. We value your opinion and want to know what we're doing right, what we could do better, what areas you'd like to see us publish in, and any other words of wisdom you're willing to pass our way.

We welcome your comments. You can email or write to let us know what you did or didn't like about this book—as well as what we can do to make our books better.

Please note that we cannot help you with technical problems related to the topic of this book.

When you write, please be sure to include this book's title and author as well as your name and email address. We will carefully review your comments and share them with the author and editors who worked on the book.

Email: community@informit.com

Reader Services

Register your copy of *Complete A+ Guide to IT Hardware and Software*, tenth edition, for convenient access to downloads, updates, and corrections as they become available. To start the registration process, go to www.pearsonitcertification.com/register and log in or create an account*. Enter the product ISBN 9780135439777 and click Submit. When the process is complete, you will find any available bonus content under Registered Products.

*Be sure to check the box that you would like to hear from us to receive exclusive discounts on future editions of this product.

Introduction

Complete A+ Guide to IT Hardware and Software, tenth edition, is a textbook and optional lab manual intended for one or more courses geared toward CompTIA A+ Certification and computer repair. It covers all the material needed for the CompTIA A+ Core 1 (220-1201) and CompTIA A+ Core 2 (220-1202) exams. The book is written so that it is easy to read and understand, with concepts presented in building-block fashion. The book focuses on hardware, software, mobile devices, virtualization, basic networking, and security.

Some of the best features of the book include the coverage of difficult subjects in a step-by-step manner, carefully developed graphics that illustrate concepts, photographs that demonstrate various technologies, reinforcement questions, critical thinking skills, soft skills, and hands-on exercises at the end of each chapter. Also, this book is written by teachers who understand the value of a textbook from authors who have been in IT their entire career.

What's New in the Tenth Edition?

This edition has been revised to provide coverage of SIMs/eSIMs, BYOD mobile devices, updated server types, additional DNS/DHCP concepts, updated display types and attributes, USB-C as a video cable type, BIOS temperature monitoring, power supply energy efficiency, printer firmware, expanded virtualization requirements, containers, updated cloud concepts, and troubleshooting situations.

Now Available Online for Free: The Companion Lab Manual!

The *Complete A+ Guide to IT Hardware and Software Lab Manual* offers hands-on practice with computer parts, mobile devices, networking, operating systems, and security. With 140 step-by-step labs, students can experiment with real technologies, answer reflection questions, and build practical skills. Challenge sections in some labs provide extra practice to deepen understanding. The Lab Manual helps students gain the experience and confidence needed for success in the IT industry.

This edition also includes more information regarding the installation/uninstallation of apps, a deeper dive into the Mac system, system folders, and common configuration files, and installing specific cloud apps and tools. The security sections throughout the book have been updated, and some additional information on change management is also provided.

The following are a few of the many new features of this edition:

- This book conforms to the latest CompTIA A+ exam requirements, including those of the CompTIA A+ Core 1 (220-1201) and CompTIA A+ Core 2 (220-1202) exams.
- Chapter 12 includes new information regarding containers.
- Chapter 16 discusses the installation and configuration of cloud-based productivity tools such as spreadsheets, word processing tools, and video conferencing.
- Chapter 17 discusses the purpose and content of macOS's most important system folders, and it describes the installation procedures for `.pkg`, `.app`, and `.dmg` files. The chapter also the explores System Settings, which replaces System Preferences.
- The book has always been filled with graphics and photos, but even more have been added to target those who are naturally drawn to the IT field. This edition is full color.
- There are questions at the end of each chapter, and even more questions are available in the test bank available from the Pearson Instructor Resource Center.

Organization of the Text

The text is organized to allow thorough coverage of all topics and also to be a flexible teaching tool. It is not necessary to cover all the chapters, nor do the chapters have to be covered in order.

Chapters 1 through 9 focus on hardware. Chapter 10 covers mobile devices. Chapter 11 is on computer design and serves as a troubleshooting review. Chapter 12 covers internet connectivity, virtualization, and cloud computing. Chapter 13 dives into networking. Chapters 14 through 17 cover operating systems. Chapter 18 handles security concepts. Finally, Chapter 19 discusses operational procedures. Appendix A provides an introduction to subnetting. Here's a closer look at what each chapter covers:

- **Chapter 1** provides an introduction to IT and careers that need the information in this book. It identifies computer parts. Chapter 1 does not have a specific soft skills section, as do the other chapters. Instead, it focuses on common technician qualities that are explored in greater detail in the soft skills sections of later chapters. Finally, Chapter 1 provides information on using Notepad, the Windows Snipping Tool, and internet search techniques.
- **Chapter 2** is about connecting things to the computer and port identification. Details are provided on video, USB, and sound ports. The soft skills section is on using appropriate titles.
- **Chapter 3** details components, features, and concepts related to motherboards, including processors, caches, expansion slots, and chipsets. Active listening skills are the focus of the soft skills section.
- **Chapter 4** deals with system configuration basics. BIOS options, UEFI BIOS, and system resources are key topics. The soft skills section covers the importance of doing one thing at a time when replacing components.
- **Chapter 5** steps through how to disassemble and reassemble a computer. Tools, ESD, EMI, and preventive maintenance are discussed. Subsequent chapters also include preventive maintenance topics. Basic electronics and computer power concepts are also included in this chapter. The soft skills section involves written communication.
- **Chapter 6** covers memory installation, preparation, and troubleshooting. The importance of teamwork is emphasized as the soft skill.
- **Chapter 7** deals with storage devices, including SATA, SAS, and SSDs. RAID is also covered. Phone communication skills are covered in the soft skills section of this chapter.
- **Chapter 8** covers video and multimedia devices, including optical drives, sound cards, cameras, scanners, and speakers. The chapter ends with a section on having a positive, proactive attitude.
- **Chapter 9** provides details on printers and multifunction devices. A discussion of work ethics finishes the chapter.
- **Chapter 10** is on mobile devices, including details on mobile device operating systems, configuration, backup, security, and troubleshooting. The soft skills section takes a brief foray into professional appearance.
- **Chapter 11** covers computer design. It discusses the specialized computers and components needed within the types of systems covered, and also explores computer subsystem design. Because design and troubleshooting use higher levels of critical thinking skills, the chapter also includes a review of troubleshooting, including logic, error codes, and troubleshooting flowcharts. The soft skills section provides recommendations for dealing with irate customers.
- **Chapter 12** handles internet connectivity, virtualization, and cloud technologies. It covers internet browser configuration, along with the soft skill mentoring.
- **Chapter 13** introduces networking. Basic concepts, terminology, and exercises make this chapter a favorite. Appendix A provides an introduction to subnetting that can be used in conjunction with this chapter. The focus of the soft skills section is being proactive instead of reactive.
- **Chapter 14** provides an introduction to operating systems in general and discusses basic differences between the Windows versions and how to function in the various Windows environments. The soft skills section includes tips on how to stay current in this fast-paced field.
- **Chapter 15** provides an introduction to scripting and includes how to function at the command prompt and the basics of scripting in Python, JavaScript, shell scripting, VBScript, batch files, and PowerShell. The soft skills section discusses looking at a problem from the user's perspective and being more empathetic.

- **Chapter 16** covers Windows 10 and 11, including how to install, configure, and troubleshoot the environment. This chapter also discusses the installation and configuration of cloud-based productivity tools such as email, word processing tools, and video conferencing tools. Avoiding burnout is the soft skill discussed in this chapter.
- **Chapter 17** provides a basic introduction to macOS and Linux to help technicians become familiar with these operating systems and a few tools. The soft skills section talks about being humble.
- **Chapter 18** describes computer, mobile device, and network security. The soft skills section is on building customer trust.
- **Chapter 19** guides the student through operational procedures such as workplace safety, recycling, disposal, a review of power protection, change management, and communication skills.

Features of This Book

The following key features of the book are designed to enable a better learning experience.

- **Objectives:** Each chapter begins with chapter objectives and the CompTIA A+ exam objectives.
- **Graphics and photographs:** Many more full-color images and all-new graphics have been added to the book to better illustrate concepts.
- **Tech Tips:** The chapters are filled with Tech Tips that highlight technical issues and certification exam topics.
- **Key terms in context:** As you read each chapter, you will find terms that appear in **blue**. They are considered key terms and are defined in the glossary.
- **Key Terms list:** At the end of the chapter, all key terms are listed.
- **Soft Skills:** Technology is not the only thing you must learn and practice; each chapter offers advice, activities, and examples of how to be a good technician, an ethical technician, a good work mate, a good communicator, and so on.
- **Chapter Summary:** The summary recaps the key concepts of the chapter, and you can use it for review to ensure that you've mastered the chapter's learning objectives.
- **A+ Certification Exam Tips:** Read through these tips on the CompTIA A+ exams so you aren't caught off guard when you sit for the exam.
- **Review Questions:** Hundreds of review questions, including true/false, multiple-choice, matching, fill-in-the-blank, and open-ended questions, help you assess your knowledge of the topics taught in each chapter.
- **Applying your knowledge:** This book provides hundreds of exercises and activities to help you put into practice what you are learning:
  - **Exercises:** Sometimes called "paper labs," the exercises can be completed without lab devices and can be completed in the classroom or for homework.
  - **Activities:** The activities provide extensive practice with internet discovery, soft skills, and critical thinking skills to round out your technical knowledge so that you can be prepared for IT work. These can be used to "Flip the Classroom" so that instruction is interactive and in the hands of the students.

Companion Website

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

To access this companion website, follow the steps below:

1. Go to www.pearsonITcertification.com/register and log in or create a new account.
2. Enter the ISBN *9780135439777*.
3. Answer the challenge question as proof of purchase.
4. Click the *Access Bonus Content* link in the Registered Products section of your account page to be taken to the page where your downloadable content is available.

Please note that many of our companion content files can be very large, especially image and video files.

If you are unable to locate the files for this title by following the steps above, please visit www.pearsonITcertification.com/contact and select the *Site Problems/Comments* option. Our customer service representatives will assist you.

CompTIA A+ Exam Objectives

To earn CompTIA A+ certification, you must pass both the CompTIA A+ Core 1 (220-1201) and CompTIA A+ Core 2 (220-1202) certification exams.

Tables I-1 and I-2 summarize the domain content for each exam.

TABLE I-1 CompTIA A+ Core 1 (220-1201) exam

Domain	Percentage of examination
1.0 Mobile Devices	13%
2.0 Networking	23%
3.0 Hardware	25%
4.0 Virtualization and Cloud Computing	11%
5.0 Hardware and Network Troubleshooting	28%
Total	100%

TABLE I-2 CompTIA A+ Core 2 (220-1202) exam

Domain	Percentage of examination
1.0 Operating Systems	28%
2.0 Security	28%
3.0 Software Troubleshooting	23%
4.0 Operational Procedures	21%
Total	100%

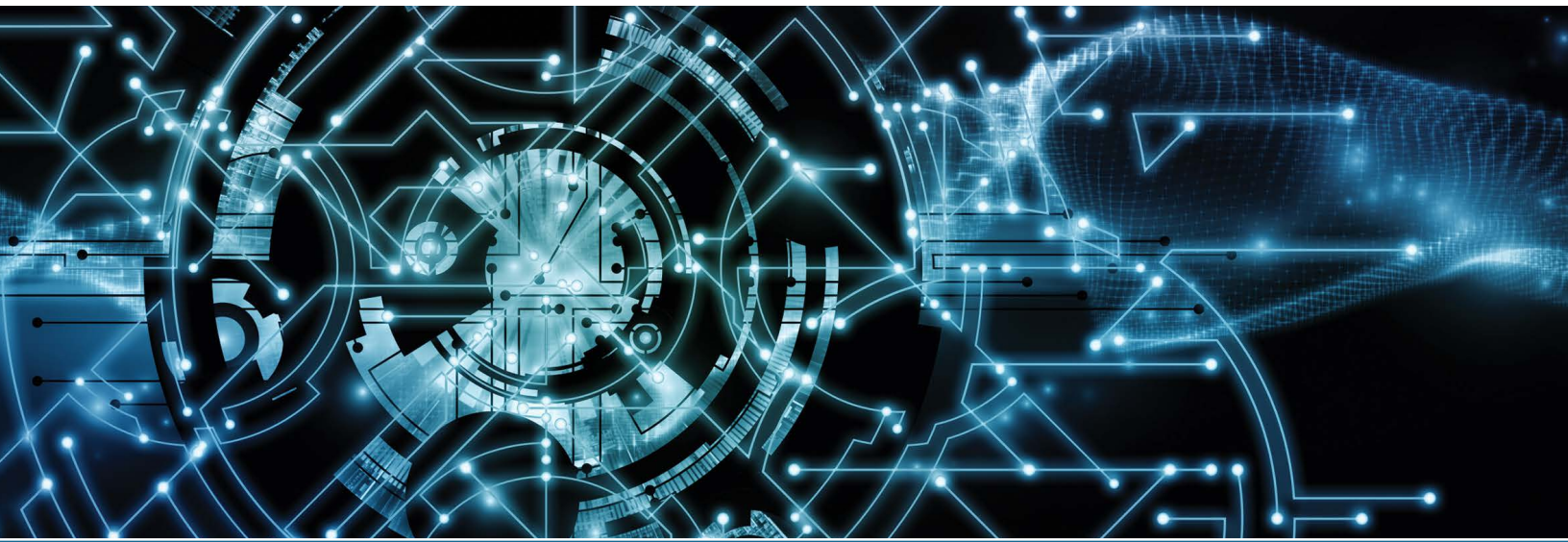
Table I-3 shows a summary of the exam domains addressed in each chapter. Each chapter lists the certification objectives it covers in the chapter opener. See Appendix B on the companion website for a detailed table that identifies where you can find all the CompTIA A+ exam objectives covered in this book.

TABLE I-3 Summary of exam domains by chapter

Table of contents	220-1201 domains	220-1202 domains
Chapter 1: Introduction to the World of IT	3	4
Chapter 2: Connectivity	1, 2, 3	4
Chapter 3: On the Motherboard	3, 5	4
Chapter 4: Introduction to Configuration	3, 5	
Chapter 5: Disassembly and Power	3, 5	4
Chapter 6: Memory	3, 5	1
Chapter 7: Storage Devices	3, 5	1, 2, 3, 4
Chapter 8: Video and Multimedia Devices	3	1, 4
Chapter 9: Printers/Multifunction Devices	2, 3, 5	1, 3, 4
Chapter 10: Mobile Devices	1, 2, 3, 5	1, 2, 3
Chapter 11: Computer Design and Troubleshooting Review	3, 5	4
Chapter 12: Internet Connectivity, Virtualization, and Cloud Technologies	2, 3, 4	1, 2, 3
Chapter 13: Networking	2, 3, 4, 5	1, 2, 3, 4
Chapter 14: Introduction to Operating Systems		1, 2, 3
Chapter 15: Introduction to Scripting		1, 3, 4
Chapter 16: Advanced Windows		1, 2, 3, 4
Chapter 17: macOS and Linux Operating Systems		1, 3
Chapter 18: Computer and Network Security	2, 3	1, 2, 3, 4
Chapter 19: Operational Procedures		4

This page intentionally left blank

1 Introduction to the World of IT



In this chapter you will learn:

- Qualities a technician should have
- Basic skills needed to function in the Windows environment and in the technical world
- Important computer parts
- Basic computer terms

CompTIA Exam Objectives:

- ✓ 1201-3.2 Summarize basic cable types and their connectors, features, and purposes.
- ✓ 1202-4.4 Given a scenario, use common safety procedures.
- ✓ 1202-4.7 Given a scenario, use proper communication techniques and professionalism.

Who Needs This Book?

More types of people than you would first think need this book. People who obviously need this information are those who will fix computers or work on a help desk or support desk. However, there are other types of users who might not be so obvious. Many folks who break into the information technology (IT) world do so through jobs that require the A+ certification. Consider medical electronics technicians who repair common equipment used in hospitals. These technicians need this material because many medical devices connect to a PC or have PC-based software that controls the device. Further, the medical devices commonly attach to wired and wireless networks.

Look at Figure 1.1 to see the types of jobs and people who need the information in this book. It might also give you ideas about something you might like to do for a career.

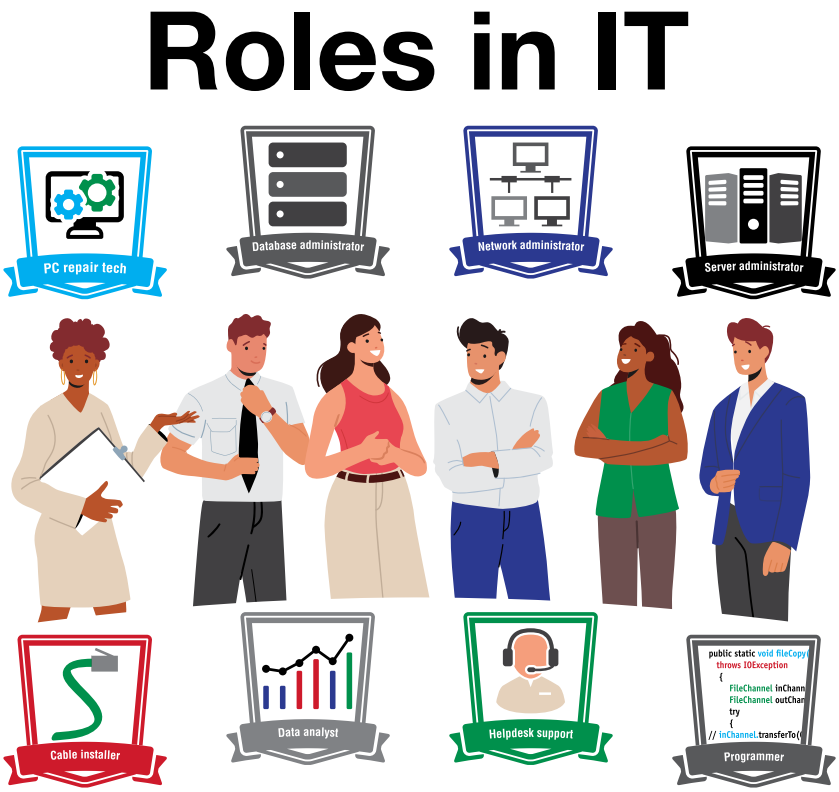


FIGURE 1.1 IT roles

Technician Qualities

Each chapter includes a small bit of space on qualities a technician should possess or strive toward. Spending a little brain power on improving what many call your "soft skills" will pay off in promotions. Three of the most important qualities of a technician are active listening skills, a good attitude, and logic. Active listening means that you truly listen to what a person (especially one who is having a problem) is saying. **Active listening skills** involve good eye contact, nodding your head every now and then to show that you are following the conversation, taking notes on important details, and avoiding distractions such as incoming cell phone calls or text messages. **Clarify customer statements** by asking pertinent questions and avoid interrupting. Listen to the entire problem. Ask **open-ended questions**—questions that allow the user to expand on the answer rather than answer with a single word, such as *yes* or *no*. Figure 1.2 illustrates this point.

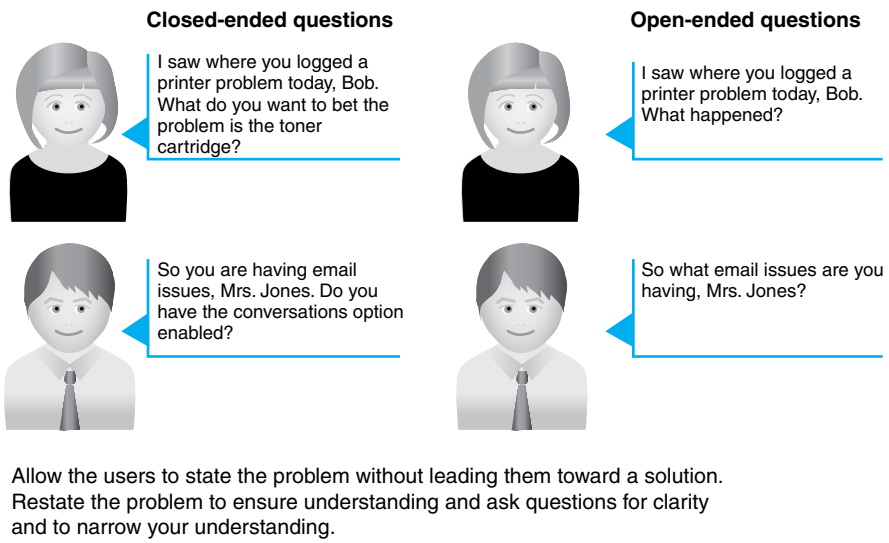


FIGURE 1.2 Asking technical questions

A positive attitude is probably the best quality a technician can possess. A technician with a positive attitude does not diminish the customer's problem; every problem is equally important to the computer user. A positive attitude is critical for being successful in the computer service industry. Figure 1.3 illustrates how maintaining a positive attitude can enhance your chances of success in the workplace.

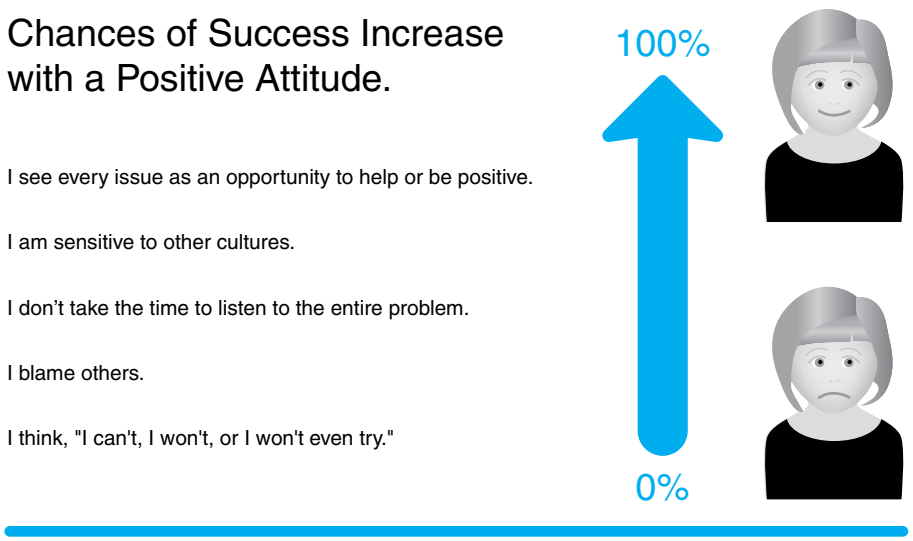


FIGURE 1.3 Have a positive attitude

Avoid developing tunnel vision (that is, thinking that there is only one answer to a problem). Step back and look at the problem so that all possible issues can be evaluated. Be logical in your assessment and the methods used to troubleshoot and repair. This book will help you by explaining computer terms in easy-to-understand language and offering examples to use when talking to customers.

Before delving into computer topics, you should remember that a class can't fully prepare you for every aspect of a job. You must learn things on your own and constantly strive to update your skills so you do not become obsolete. The IT field changes rapidly. Figure 1.4 illustrates this concept. Finally, you will find that you must be a jack-of-all-trades, as shown in Figure 1.5.

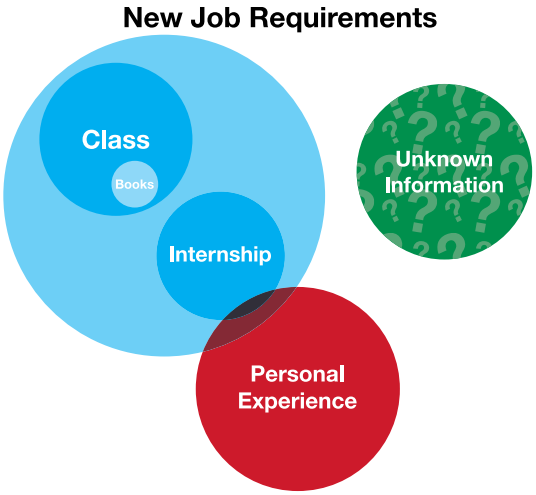


FIGURE 1.4 Preparing for IT job requirements

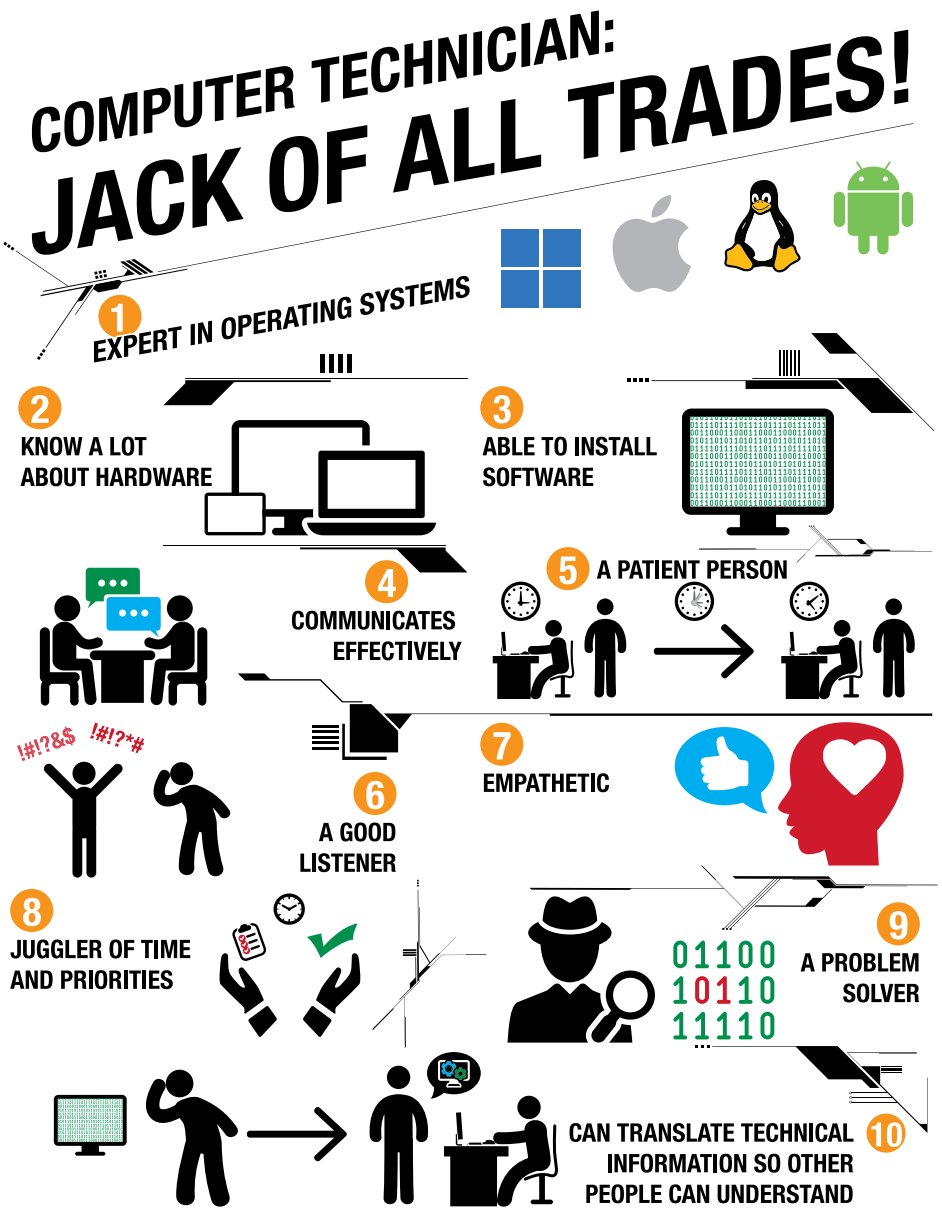


FIGURE 1.5 Computer technician skills

Breaking into IT with the CompTIA A+ Certification

Many IT-related jobs require the A+ certification. Even if not required, the certification shows that you have a good understanding of how computers work. This certification doesn't guarantee a job, but it can help you get into the interview process even if you lack IT experience.

A+ certification requires that you take two exams: Core 1 (220-1201) and Core 2 (220-1202). Each of these exams covers specific material. Tables 1.1 and 1.2 show the major categories (domains) for each exam and the extent to which they are represented.

TABLE 1.1 CompTIA Core 1 (220-1201) A+ certification domains

Domain	Percentage of examination	Chapter(s)
1.0 Mobile Devices	13%	10
2.0 Networking	23%	12–13
3.0 Hardware	25%	1–9, 11
4.0 Virtualization and Cloud Computing	11%	3, 12
5.0 Hardware and Network Troubleshooting	28%	1–13

TABLE 1.2 CompTIA Core 2 (220-1202) A+ certification domains

Domain	Percentage of examination	Chapter(s)
1.0 Operating Systems	28%	14–17
2.0 Security	28%	18
3.0 Software Troubleshooting	23%	14–18
4.0 Operational Procedures	21%	19

"What are the exams like?" you might ask. The exams include multiple-choice and performance-based questions. A performance-based question might be a drag-and-drop scenario or might ask you to do something specific on a particular device or within a particular operating system environment. Each exam is 90 minutes long and contains a maximum of 90 questions. The testing system allows you to bookmark questions that you might want to return to at the end if you have time. More information can be found on the CompTIA website (www.comptia.org).

At the beginning of each chapter, you will see a list of the CompTIA A+ exam objectives that are covered in that chapter. At the end of each chapter, I've provided some A+ certification exam tips—tips to definitely pay attention to if you plan on taking the A+ exams. I recommend that you review the exam objectives, study material specific to them, and take some practice exams. Pearson IT Certification, the publisher of this book, develops many different certification exam prep resources that suit various study styles. See the back of this book for more information or go to http://pearsonitcertification.com/aplus to browse the options.

Basic Skills for This Course

In order to repair a computer, you need a few basic skills that include being familiar with the keyboard and inputting information, searching for information on the internet, and capturing information. Just because you may not be a good typist does not mean that you will not be good in an IT-related field.

Searching for Information on the Internet

IT people need to use all available resources, including online resources. As noted, you need to be capable of searching for information online. Figure 1.6 illustrates various online resources that IT people search all the time.

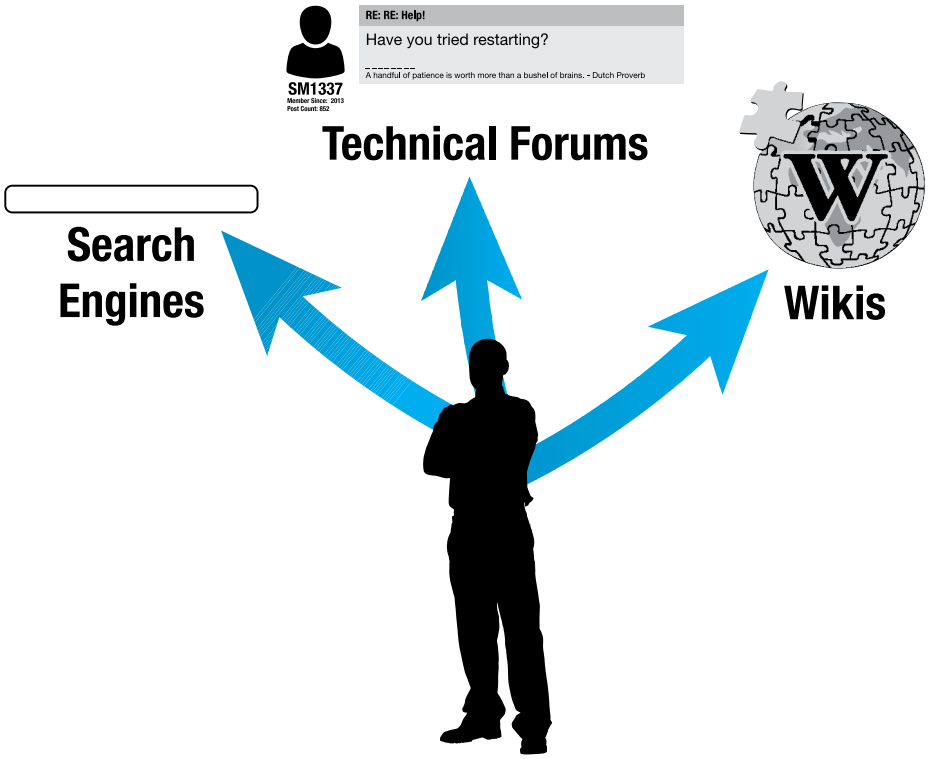


FIGURE 1.6 Search skills

Each chapter in the book has an activity at the end of it that enables you to practice searching the internet for information relevant to the chapter. Tips for searching include the following:

> Remember that search engines use different algorithms, so if one does not work, try another one. Examples of search engines are Google, Bing, Yahoo, Brave, DuckDuckGo, and Ask. To access a search engine, open a web browser and type one of the search engine names followed by `.com`. Figure 1.7 shows where you enter the search engine name in the address bar.

FIGURE 1.7 Web browser address bar

> Use descriptive key words.

> Do not include common words like *the*, *in*, *at*, or *for* because search engines tend to skip these words anyway. If you do want to use one of them, put a plus sign (+) in front of the word.

- Avoid using a complex version, plural, or past tense of a word. When you include such word versions, the search engine is likely to eliminate pages that are relevant. For example, to search for how to install a Bluetooth headset, avoid using the word *installation*, *installed*, or *installing* in the search window. Simply include the word *install*.
- To search for an exact phrase (that is, several words used together), put quotation marks around the phrase. For example, to search for Windows 11, enter the search term `"Windows 11"`.
- Use as many distinguishing words as possible.
- If two words have the same meaning and are commonly used, use the word *or* in the search. For example, to search for generic information on a dot matrix printer, which is sometimes called an impact printer, you might search as follows: `"dot matrix" or "impact printer"`. Note that the vertical bar (|), which is the key above the [Enter] key, can be used instead of the word *or*, as follows: `"dot matrix"` [|] `"impact printer"`.
- If a particular term can have two meanings (such as the word *memory* relating to something inside a computer or else relating to a brain function), you can use the minus sign in order to prevent some information from being displayed. `memory -brain`, for example, would be a search for memory without any brain function results included.
- If a particular term (such as memory) is generic, you can add a word and use the word *AND* in order to clarify the search, such as `computer AND memory`.
- When searching for technical information, include the hardware or software manufacturer. A search for `Microsoft Windows 10` provides different results than simply a search for `Windows 10`.
- If nothing relevant is on the first page of links, change the key words used in your search.

Consider the situation of a keyboard that intermittently works on a Microsoft Surface computer. The keyboard does not come standard as part of a Surface purchase. You do not own a Surface yourself and are unfamiliar with the tablet but must support it. An example of what you might type into a search engine is `Microsoft Surface intermittent keyboard`.

Screen Capturing

Documentation is a part of all IT jobs, so no matter what IT job you have when you enter the workforce, you will need to get familiar with it. Sometimes, technical documentation involves being able to capture what is on the screen. Windows versions come with the Snipping Tool and Snip & Sketch. In addition, to take a screenshot on a Windows machine, hold down the [⊞] key and press the [⇧Shift] key and, while holding both of these keys down, press the [S] key. Documenting problems is easy with screenshots, and you can copy what you capture into other applications.

To take a screenshot on a Mac, hold these three keys down one at a time (keeping each one down as you add another key): [⇧Shift]+[⌘]+[3].To capture a portion of the screen, use the [⇧Shift]+[⌘]+[4] keys. To capture a window or menu, use the [⇧Shift]+[⌘]+[4]+[Spacebar] keys. By default the screenshots are saved to the desktop, and you can move them to a folder later.

Creating a Text File

Documentation sometimes involves creating or using a text file, known as a .txt file. Text files are popular because they can be opened by many applications or other mobile apps. Text files commonly include only text, without multiple fonts or graphics.

You might need to send a text file as an attachment, or you might need to create a text file as part of the documentation process or for another part of your job. A text file is one of the easiest types of file to create, especially on a mobile device. Text files can be created using a word processor and the *Save As* process, or they can be created using specific text software or an app. Windows Notepad and Apple TextEdit can be used to create and open text files.

Types of Computers

The simplest place to start to learn about computer technical support is with the devices themselves. **PCs**, or personal computers, come in desktop, tower, and all-in-one models, as well as mobile models such as laptops, smartphones, and tablets. Figure 1.8 shows some of the computing devices technical staff are expected to support.

FIGURE 1.8 Types of computers

Basic Computer Hardware

Computer systems include hardware, software, and firmware. **Hardware** is something you can touch and feel, like the physical computer and the parts inside the computer. The display, keyboard, and mouse are hardware components. **Software** interacts with the hardware. Windows, Linux, macOS, Microsoft 365, Google Chrome, Adobe Acrobat Reader, Intuit TurboTax, and WordPerfect are examples of software.

Without software that directs the hardware to accomplish something, a computer is no more than a doorstop. A computer needs an important piece of software called an **operating system**, which coordinates the interaction between hardware and software applications. The operating system also handles the interaction between a user and the computer. Examples of operating systems include Windows 10 and 11, macOS, and various Linux systems, such as Red Hat and Ubuntu. Firmware is a combination of hardware and software such as the chip used to boot the computer and locate the operating system.

A **device driver** enables the operating system to recognize, control, and use the hardware component. Device drivers are hardware and operating system specific. For example, a printer requires a specific device driver when connected to a computer that has Windows 10 installed. The same printer might require a different device driver when using Windows 11. That Windows print driver would not work on an Apple computer. Each piece of installed hardware requires a device driver for the operating system being used. Figure 1.9 shows how hardware and software must work together.

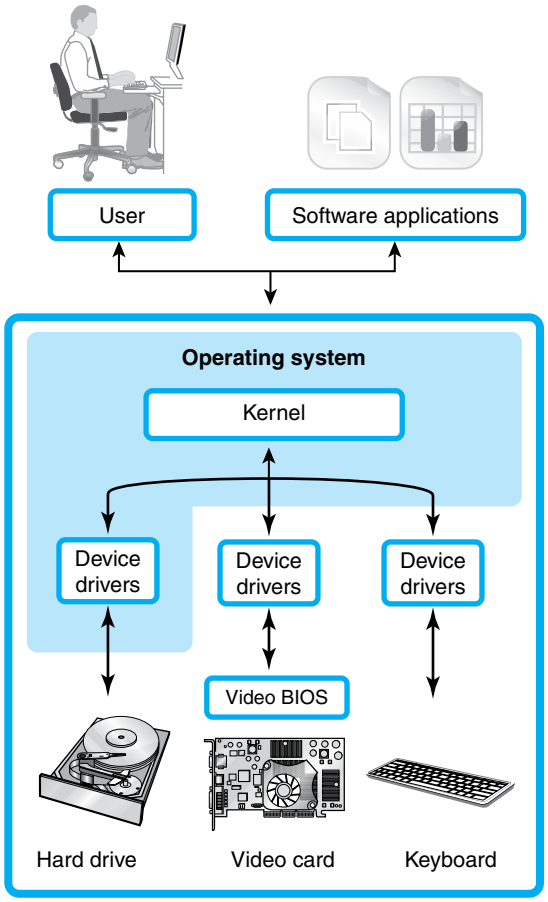


FIGURE 1.9 Hardware and software

Notice in Figure 1.9 the operating system kernel. The kernel is the central part of an operating system. The kernel is the connection between hardware and the applications being used.

A PC typically consists of a case (chassis), a keyboard that allows users to provide input into the computer, a **display** that outputs or displays information, and a mouse that allows data input or is used to select menus and options. Figure 1.10 shows a computer display, which may also be called a flat panel, display, or screen.

FIGURE 1.10 Computer display

When the computer cover or side is opened or removed, the parts inside can be identified. The easiest part to identify is the **power supply**, which is the metal box normally located in a back corner of a case. A power cord connects the power supply to a wall outlet or surge strip. One

purpose of the power supply is to convert the outlet AC voltage to the DC voltage used internally in the PC. The power supply distributes this DC voltage using power cables that connect to the various internal computer parts. A fan located inside the power supply helps keep the computer cool to prevent damage to the components.

A PC usually has a device to store software applications and files. Two examples of storage devices are the hard drive and optical drive. The **hard drive**, sometimes called the hard disk, is a rectangular box normally inside the computer's case that is sealed to keep out dust and dirt. The hard drive has no external opening. The computer must be opened in order to access an internal hard drive. An **optical drive**, sometimes called a DVD drive, holds discs (compact discs, or CDs), digital versatile discs (DVDs), or Blu-ray discs (BDs) that have data, music, video, or software applications on them. The front of the optical drive has a tray that can eject outward so a disc may be inserted. Figure 1.11 shows the major components of a tower computer. Figures 1.12 through 1.14 show components as they look before being installed. Figure 1.12 shows a hard drive, Figure 1.13 shows an optical drive, Figure 1.14 shows a power supply, and Figure 1.15 shows a tower computer case.

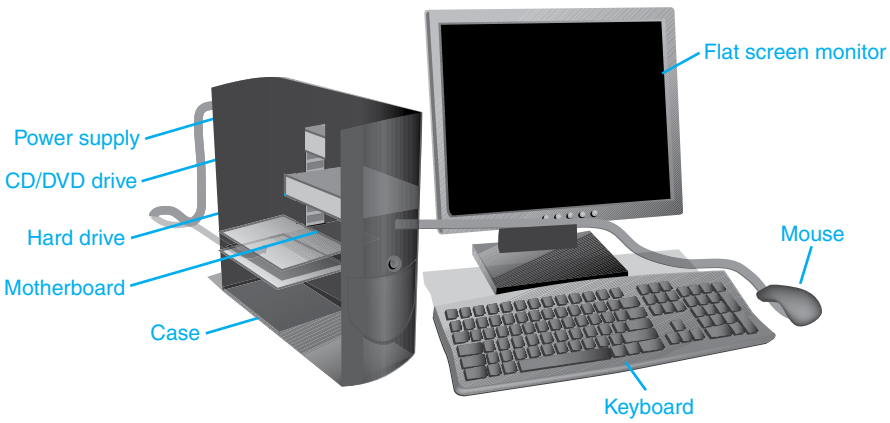


FIGURE 1.11 Tower computer

FIGURE 1.12 Hard drive

FIGURE 1.13 Optical drive

FIGURE 1.14 Power supply

FIGURE 1.15 Tower case

The **motherboard** is the main circuit board inside a PC and contains the most electronics. It is normally located on the bottom of a desktop or laptop computer and mounted on the side of a tower computer. Other names for the motherboard include mainboard, planar, and system board. External devices connect directly to the back of the motherboard or ports on the front of the computer. Figure 1.16 shows a motherboard when it is not installed inside a computer as well as memory and an adapter (card), which are covered next.

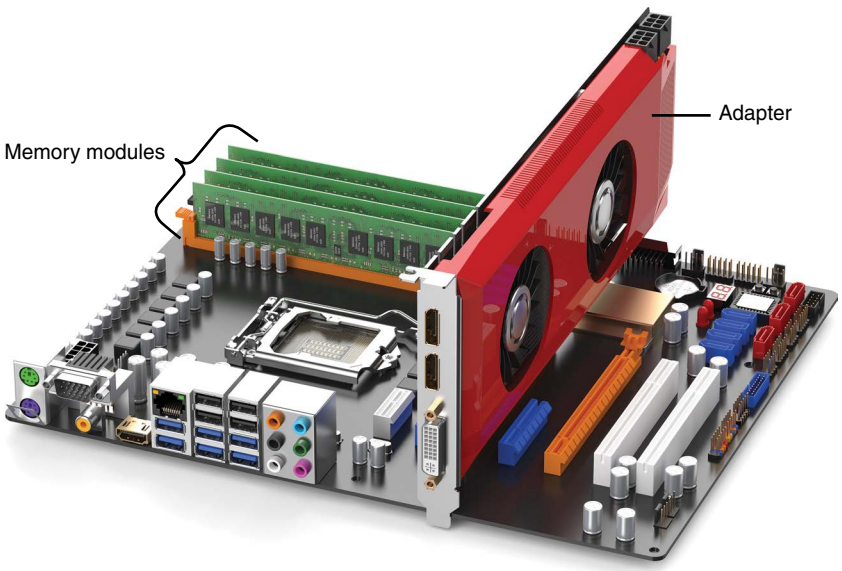


FIGURE 1.16 Computer motherboard

The motherboard holds memory modules. **Memory** modules hold applications, part of the operating system, and user documents. Random-access memory (**RAM**), which is the most common type of memory on the motherboard, is volatile—that is, the data inside the module is lost when power is removed. When a user types a document in a word processing program, both the word processing application and the document are in RAM. If the user turns off the computer without saving the document to removable media, the local drive, or to cloud storage, the document is lost because the information does not stay in RAM. (Note that some applications have the ability to periodically save a document, but this is not a guarantee that it has the latest information.) Figure 1.17 shows memory modules when they are not installed into the motherboard memory slots. Memory is covered in great detail in Chapter 6, "Memory."

FIGURE 1.17 Memory modules

A device may connect directly to the motherboard or to an adapter through a cable that connects the device to either one. An **adapter** is an electronic card that plugs into an **expansion slot** on the motherboard. Other names for an adapter are controller, card, controller card, circuit card, circuit board, and adapter board. Adapters allow someone to add a functionality or enhancement that is not provided through the ports on the motherboard. An example is someone who wants better sound or video graphics or additional ports of some type in order to connect external devices.

Figure 1.18 shows an adapter. Notice how the contacts at the bottom are a particular shape. Chapter 3, "On the Motherboard," goes into more detail about the types of expansion slots and adapters. You can also look back at Figure 1.16 to see a video card/adapter installed into a motherboard expansion slot.

FIGURE 1.18 Adapter

TECH TIP

How to identify an adapter's function

Tracing the cable attached to an adapter or looking at the device connected to an adapter can help identify the adapter's function.

The following are the generic steps for installing adapters:

Step 1. Always follow the manufacturer's installation directions. Use an antistatic wrist strap when handling adapters. Electrostatic discharge (ESD) can damage electronic parts. (See Chapter 5, "Disassembly and Power," for more details on ESD.)

Step 2. Be sure the computer is powered off and unplugged.

Step 3. Remove any brackets from the case or plastic covers from the rear of the computer that may prevent adapter installation. Install the adapter in a free expansion slot and reattach any securing hardware.

Step 4. Attach any internal device cables that connect to the adapter, as well as any cables that go to an external port on the adapter.

Step 5. Attach any internal or external devices to the opposite ends of the cable, if necessary.

Step 6. Power on any external devices connected to the adapter, if applicable.

Step 7. Reattach the computer power cord and power on the computer.

Step 8. Load any application software or device drivers needed for the devices attached to the adapter.

Step 9. Test the device connected to the adapter.

See Figure 1.19 for an illustration of a motherboard, expansion slots, memory, and an adapter in an expansion slot.

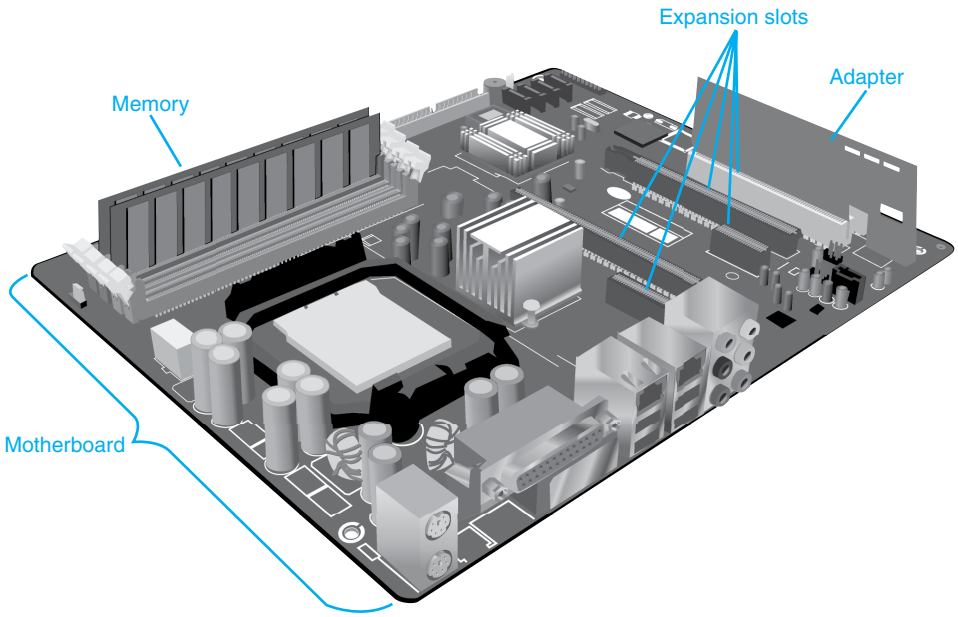


FIGURE 1.19 Motherboard with expansion slots and an adapter

Mice and Keyboards

Input devices, such as the mouse and keyboard, attach to the motherboard. The most common type of **mouse** is an optical mouse, which has optical sensors that detect the direction in which the mouse moves. It uses reflections from light-emitting diodes (LEDs) from almost any surface to detect the mouse location. Mice commonly can be adjusted for sensitivity—how far you have to move the mouse to move the cursor on the screen a desired amount. Figure 1.20 shows the bottom of an optical mouse.

A **keyboard** is an input device that connects to a port on the motherboard or attaches wirelessly. Features users look for in a keyboard include a separate numeric keypad for those who have to input numbers frequently, adjustable tilt legs, and spill resistance. Figure 1.21 shows the type of keyboard and mouse that are commonly used with a tower, desktop, or all-in-one computer.

FIGURE 1.20 Optical mouse

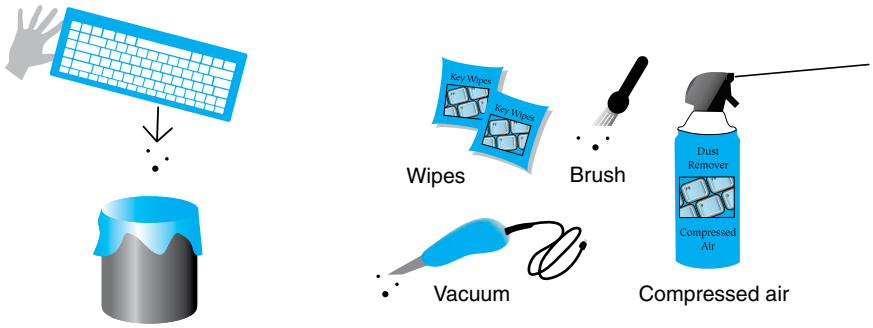
FIGURE 1.21 Keyboard and mouse

Mouse and Keyboard Preventive Maintenance

Mouse cleaning kits are available in computer stores, but normal household supplies also work. Use the following procedures to clean an optical mouse:

> Wipe the bottom with a damp, lint-free cloth.
> Use compressed air to clean the optical sensors.

Keyboards also need to be cleaned periodically. Figure 1.22 shows keyboard-cleaning techniques.



1. Turn keyboard upside down and gently shake out debris

2. Clean the keyboard (several options shown)

FIGURE 1.22 Keyboard cleaning techniques

Keyboard/Mouse Troubleshooting

One of the easiest ways to determine whether a keyboard is working is to press the Caps Lock or Num Lock key and watch to see if the keyboard light illuminates. Sometimes an application setting may be causing what appears to be a keyboard problem. Use another application to see if the keyboard is the problem. Keyboards can have LED lights that indicate particular functions. Table 1.3 lists the most common ones. Note that different vendors label the lights in various ways.

TABLE 1.3 Common keyboard lights

Associated toggle key	Keyboard light	Description
Num Lock	Number lock (NUM LOCK)	Toggles the 10-key pad between digits 0 through 9 and various functions, such as HOME, PG UP, PG DOWN, END, and various arrow keys.
Caps Lock	Capital letters lock (CAPS LOCK)	Toggles between all uppercase and lowercase letters.
Scroll Lock	Scroll lock	A rarely used key used to prevent scrolling and use of the arrow keys to progress through information displayed.

TECH TIP

One key doesn't work

If a particular key is not working properly, remove the key cap. A small, flat-tipped screwdriver can assist with this. After removing the key cap, use compressed air around the sticky or malfunctioning key.

If coffee or another liquid spills into a PC keyboard, all is not lost. Quickly unplug the keyboard and turn it upside down to prevent further damage. Use paper towels to absorb as much liquid as you can. Afterward, the keyboard can be disassembled and/or scrubbed with lint-free swabs or cloths. However, PC keyboards and mice are normally considered throw-away technology. It is cheaper to get a new one than to spend a lot of time trying to repair it.

Common Peripherals

Many devices connect to a computer to provide input, such as a mouse, drawing pad, or keyboard, or output, such as a display. Some devices can be both input and output devices, such as smart TVs, Musical Instrument Digital Interface- (MIDI-) enabled devices (which are electronic musical devices), touch screens, or printers. In the case of a printer, data is sent from a computer to the printer, and the printer can send data (information), such as an out-of-ink message, back to the computer. Figure 1.23 shows some common input and output devices.

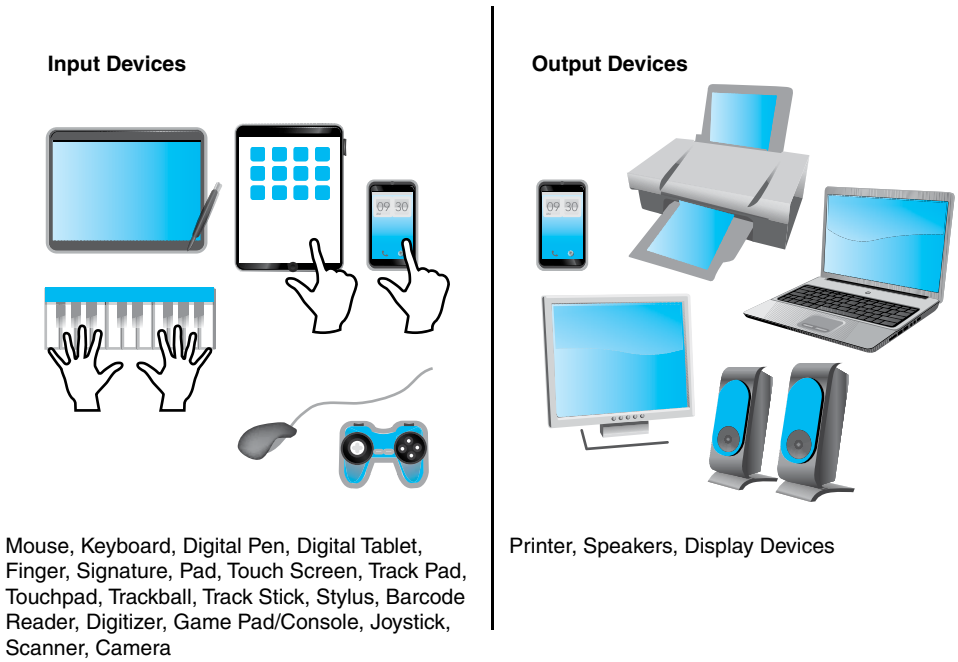


FIGURE 1.23 Input and output devices

Table 1.4 lists various peripherals that you will see used and attached to computers today. We will be examining some of these devices in more depth and learn how to configure them in later chapters, but this chapter gives you the basics.

TABLE 1.4 Common peripherals

Peripheral	Description
Printer	An output device that transfers information such as text and graphics from a computer onto paper or other media (see Figure 1.24).
Flatbed scanner	An input device that digitizes words or graphics and can be used as a copier. A scanner (see Figure 1.24) may have an automatic document feeder (**ADF**) that allows one or more documents to be fed into the scanner.
All-in-one printer	A device, sometimes known as a multifunction printer, that has printer, scanner, copier, and sometimes fax capabilities (see Figure 1.24).
Camera/webcam	An input device used to provide live video feed, such as when you participate in a video conference, or capture video images or motion (see Figure 1.25). More information can be found in Chapter 8, "Video and Multimedia Devices."
Microphone	An input device used to capture sound (see Figure 1.25). More information can be found in Chapter 8.
Headset	An input/output device that commonly has a microphone and headphones, as shown in Figure 1.25.

FIGURE 1.24 Printer, scanner, and all-in-one printer

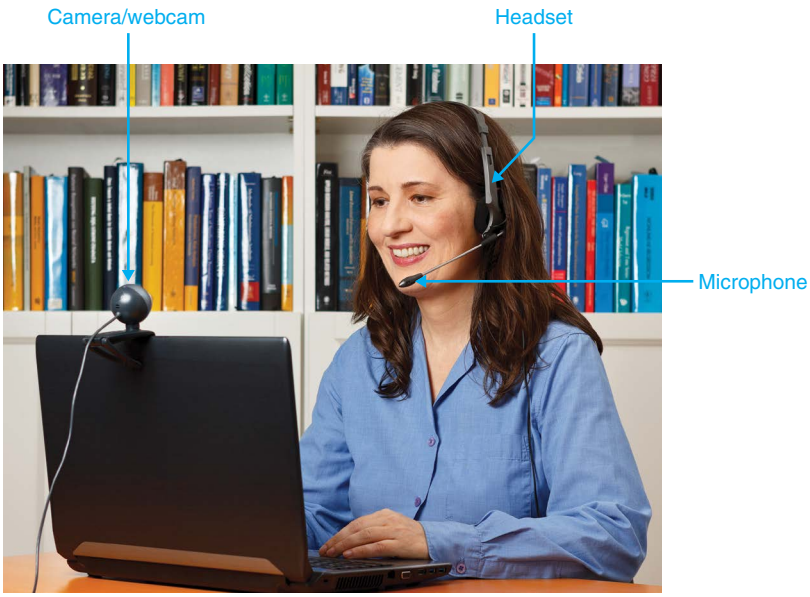


FIGURE 1.25 Camera/webcam, headset, and microphone

1s and 0s

Computers are digital devices. That means they understand 1s and 0s. One 1 or one 0 is known as a **bit**. In actuality, a 1 is simply a voltage level. So, when we type characters into a word processing application, the keyboard translates those characters into voltage levels. Figure 1.26 illustrates this concept. Notice that each letter is represented by a combination of eight 1s and 0s. Each 1 is a voltage level sent to the motherboard (and components on it). Each 0 is simply the absence of a voltage level.

	D	E	A	R	[space]	M	O	M
What we see	01000100	01000101	01000001	01010010	00100000	01001101	01010010	01001101
What a computer sees	ϟ ϟ	ϟ ϟϟ	ϟ ϟ	ϟ ϟ ϟ	ϟ	ϟ ϟϟϟ	ϟ ϟ ϟ	ϟ ϟϟϟ

FIGURE 1.26 Binary bits

Technicians need to be able to describe capacities such as hard drive capacities and available drive space. Eight bits grouped together are a **byte**. Figure 1.27 shows a hot dog divided into eight sections (which make a big old "byte").

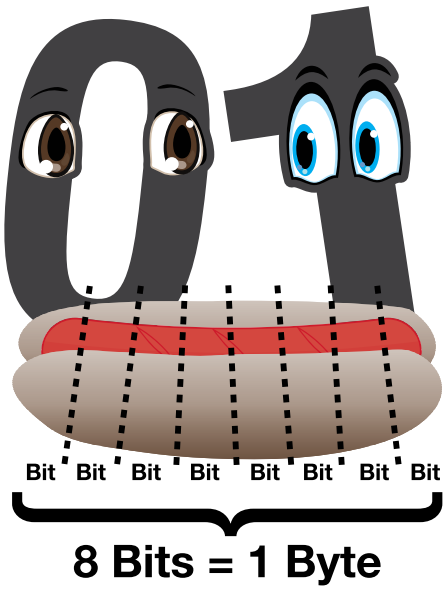


FIGURE 1.27 A byte

Approximately 1,000 bytes is a **kilobyte** (kB), as shown in Figure 1.28. 1 kB is 1,024 bytes to be exact, but industry folks simply round off the number to the nearest thousand for ease of calculation. Approximately 1 million bytes is a **megabyte** (MB), but a true megabyte is 1,048,576 bytes. 540 megabytes is abbreviated as 540 MB, or 540 M. Notice in Figure 1.28 that a megabyte stores a lot more 1s and 0s than a kilobyte.

Approximately 1 billion bytes (1,073,741,824 bytes) is a **gigabyte** (GB), which is shown as 1 GB or 1 G. Approximately 1 trillion bytes (1,099,511,627,776 bytes) is a **terabyte**, which is shown as 1 TB or 1 T. Figure 1.28 shows how storage capacities get larger.

FIGURE 1.28 A kilobyte, megabyte, gigabyte, and terabyte illustrated

When information needs to be expressed exactly, binary prefixes are used. For example, when describing the value 2^{10} (1,024), instead of saying this it is 1 kilobyte, which people tend to think of as approximately 1,000 bytes, the term kibibyte (KiB) is used. When describing the value 2^{20}, or 1,048,576, the term mebibyte (MiB) is used. Table 1.5 shows the terms used with computer storage capacity and binary prefixes when exact measurements are needed.

TABLE 1.5 Storage terms and binary prefixes

Term	Abbreviation	Description
Kilobyte/kibibyte	kB/KiB	~1 thousand bytes/2^{10} bytes
Megabyte/mebibyte	MB/MiB	~1 million bytes/2^{20} bytes
Gigabyte/gibibyte	GB/GiB	~1 billion bytes/2^{30} bytes
Terabyte/tebibyte	TB/TiB	~1 trillion bytes/2^{40} bytes
Petabyte/pebibyte	PB/PiB	~1,000 trillion bytes/2^{50} bytes
Exabyte/exbibyte	EB/EiB	~1 quintillion bytes/2^{60} bytes
Zettabyte/zebibyte	ZB/ZiB	~1,000 exabytes/2^{70} bytes
Yottabyte/yobibyte	YB/YiB	~1 million exabytes/2^{80} bytes

Frequencies are also important measurements in computers because people want to know how fast their computers, processors, memory, and other parts are operating. Frequencies are shown in similar measurements, but instead of bits (b) or bytes (B), speeds are shown in hertz (Hz). A hertz is a measurement of cycles per second. Something that operates at approximately 1 million cycles per second is said to operate at 1 megahertz (1 MHz). For 1 billion cycles per second, the measurement is known as 1 gigahertz, or 1 GHz. Transfer speeds are commonly shown in bits per second, such as gigabits per second, or Gb/s, or bytes per second, such as in megabytes per second, or MB/s. Notice the capital letter B to indicate bytes as compared to the lowercase b to indicate bits. These measurements are used in a lot of IT-related hardware and software.

Safety Notes

Safety is covered in most chapters, especially in Chapter 5, but no book on computer repair can begin without stating that both the technician and the computer can be harmed by poor safety habits. Before beginning any PC service, remove jewelry. To protect yourself and the computer, make sure to power off the computer and remove the power cord when disassembling, installing, or removing hardware or when doing preventive maintenance (cleaning).

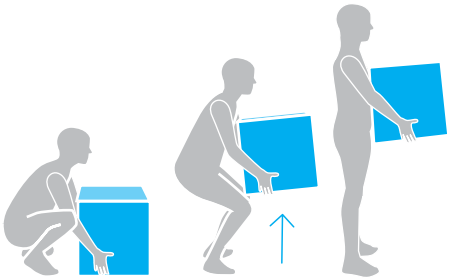
TECH TIP

Some things should be left alone

Never take apart computer parts such as a power supply unless you have had specific training.

Technicians can also be harmed when doing menial tasks such as lifting a computer or heavy laser printer. Lifting is a common requirement listed in IT job advertisements or explained during interviews. Technical jobs frequently specify a maximum lifting requirement of 40 to 50 pounds. Use proper safety precautions, such as those shown in Figure 1.29. The type of equipment you need and things you can do to prevent harm to the computer are covered more explicitly in Chapter 5, on power and disassembly.

Remove jewelry
before working
inside of a computer



- Bend at the knees
- Use your legs to lift
- Use lifting aids when possible
- Ask for assistance when possible

FIGURE 1.29 Safety tips

Chapter Summary

> Many IT roles require detailed knowledge of PC hardware and software.
> Computer technicians should actively listen, have a positive attitude, and use logic when solving problems.
> The CompTIA A+ certification requires two exams: Core 1 (220-1201) and Core 2 (220-1202). Many people break into the IT field with this certification.
> IT staff must be proficient at searching for information on the internet, capturing files, and documenting technical information.
> Computers consist of hardware (the physical parts) and software (the operating system and applications).
> A technician needs to be able to identify important computer parts installed in a computer and as standalone parts: case, keyboard, mouse, motherboard, display, power supply, hard drive, optical drive, adapter, and memory.
> A technician needs to know the purposes of common peripherals used in the industry: printer, flatbed scanner with ADF, camera/webcam, microphone, and headset.
> Mice and keyboards are important input devices. To clean a keyboard, turn it over to remove debris and then use a vacuum, compressed air, and wipes as needed.
> Safety is important when working on a computer. Before working inside a computer, power it down and remove the power cord.
> Use proper lifting techniques when servicing equipment and remove jewelry before working inside a computer.

A+ CERTIFICATION EXAM TIPS

- ✓ Familiarize yourself with the acronyms at the end of the official CompTIA A+ exam objectives document. You can expect the exam to use these acronyms without defining them.
- ✓ Ensure that you are knowledgeable about and proficient with all the terms and technologies listed in the official CompTIA A+ exam objectives. Some students study for a particular exam by going through the objectives one by one and reviewing the material as they go through.
- ✓ Ensure that you can identify the basic parts of a computer and explain the purpose of each one. Ensure that you know the following parts: hard drive, optical drive, power supply, motherboard, and RAM.
- ✓ Become familiar with the following common pieces of hardware before you get to the chapters that go into the details of installing, configuring, and troubleshooting them: printer, flatbed scanner, ADF, display, optical drive, mouse, keyboard, trackpad, drawing pad, camera/webcam, microphone, speakers, and headset.
- ✓ Know the following safety procedures: disconnecting power and using proper lifting techniques.
- ✓ Ensure that you know what open-ended questions are.

Key Terms

active listening skills, adapter, ADF, bit, byte, camera, clarify customer statements, device driver, display, expansion slot, flatbed scanner, gigabyte, hard drive, hardware, headset, keyboard, kilobyte, megabyte, memory, microphone, motherboard, mouse, open-ended question, operating system, optical drive, PC, power supply, printer, RAM, software, terabyte, webcam

Review Questions

1. Match each part to the appropriate description.

____ motherboard	a. Converts AC to DC.
____ RAM	b. Holds the most data.
____ DVD drive	c. Has the most electronics.
____ hard drive	d. Fits in an expansion slot.
____ adapter	e. Contents disappear when power is off.
____ power supply	f. Holds a disc.

2. A technician has been asked to provide support to an administrative assistant who is participating in a video conference session. Which peripheral would be used in the conference more so than in normal daily operational tasks?

   [mouse | webcam | all-in-one printer | hard drive]

3. Which of the following are important suggested internet search tips? (Choose two.)

   a. Try another search engine if the first one does not provide satisfactory results.

   b. Use as many common words—such as the, in, at, or for—as possible.

   c. Put quotation marks around two or more words that might be found consecutively in output.

   d. Use as few words as possible.

   e. Avoid using the name of the equipment manufacturer.

4. What is the acronym used to describe memory that is commonly found on a motherboard?

   _____

5. When lifting a heavy computer, you should squat, bend at the knees, and use your legs to lift. [T | F]

6. How many tests must a person take in order to be A+ certified?

   [0 | 1 | 2 | 3 | 4]

7. Is the following question open ended or closed ended? "You say your computer has been running slowly since Monday. Which applications have you installed this week?" [open ended | closed ended]

8. List one example of having a positive attitude.

   _____

9. Which of the following devices are common output devices? (Choose all that apply.)

   [digital piano | speakers | display | stylus | track stick | barcode reader | printer]

10. People who work with computers might be expected to lift up to how many pounds?

    [10 to 20 | 20 to 30 | 30 to 40 | 40 to 50]

11. Which Microsoft Windows application could be used to create a text file?

    [Textpad | Notepad | WriteIt | NoteIt]

12. Which Windows tool can be used to make a screenshot?

    [Notepad | Bluetooth | Microsoft Edge | Snip & Sketch]

13. Rewrite the following so that it includes an open-ended question.

Technician: Good morning. I have a service log that states you are getting an error message whenever you access a PDF file. Have you done your Acrobat updates lately?

_____

14. List one procedure you would try to fix an erratic optical mouse.

_____

_____

15. Match the capacity to the description.

____ bit	a. 8 bits
____ kilobyte	b. a 1 or a 0
____ megabyte	c. approximately 1,000 bytes
____ byte	d. approximately 1 million bytes
____ gigabyte	e. approximately 1 trillion bytes
____ terabyte	f. approximately 1 billion bytes

16. Match the device to the description. Note that each description will best fit only one answer.

____ flatbed scanner	a. Could have an ADF
____ adapter	b. Used to feed multiple sheets of paper one page at a time
____ ADF	c. Used to capture video
____ power supply	d. Inserts into an expansion slot
____ webcam	e. Converts AC to DC

17. What is a feature of an optical mouse?

a. LED

b. contacts

c. volatility

d. electrical conversion

18. Which device is normally found inside a computer?

[ADF | printer | headset | hard drive]

19. Which device normally can be seen if looking inside a desktop computer with the cover off and when normally looking at the front of a desktop computer?

[hard drive | motherboard | optical drive | RAM]

20. Where can you find the motherboard in a tower computer?

a. inside the power supply

b. on the side of the case

c. below the hard drive

d. beside the RAM

Exercises

Exercise 1.1 Identifying Tower Computer Parts

Objective: To identify various computer parts correctly

Procedure: Identify each computer part in Figure 1.30. Match the part to the number in Figure 1.31.

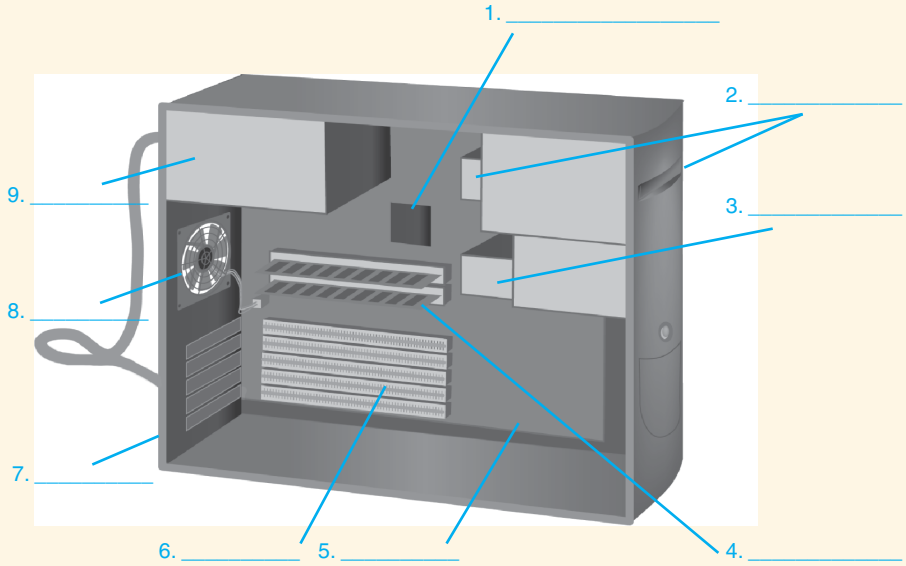


FIGURE 1.30 Tower computer parts identification

1. _____
2. _____
3. _____
4. _____
5. _____
6. _____
7. _____
8. _____
9. _____

FIGURE 1.31 Second tower computer parts identification

1.	_____	**a.**	motherboard
2.	_____	**b.**	RAM
3.	_____	**c.**	power supply
4.	_____	**d.**	case fan
5.	_____	**e.**	adapter
6.	_____	**f.**	optical drive
7.	_____	**g.**	case

Exercise 1.2 Identifying Computer Parts

Objective: To identify various computer parts correctly

Procedure: Identify each computer part in Figure 1.32.

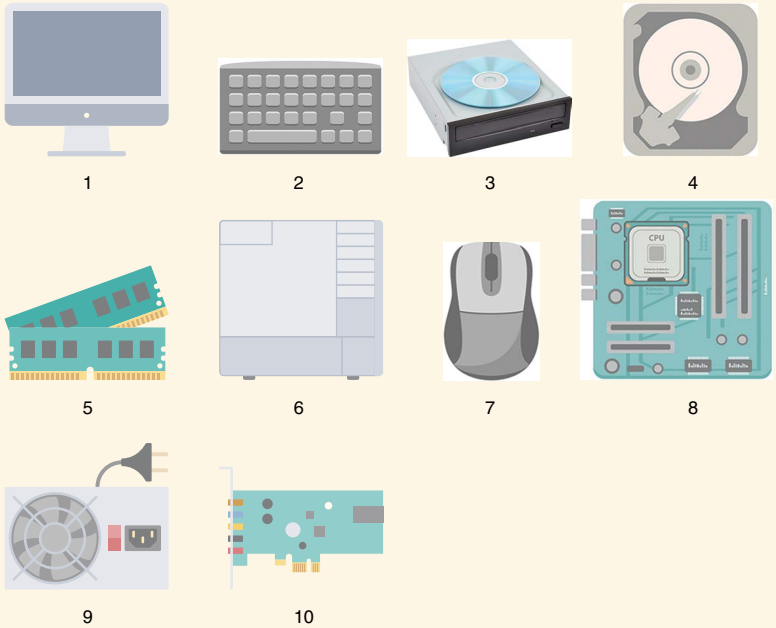


FIGURE 1.32 Computer parts identification

1. _____
2. _____
3. _____
4. _____
5. _____
6. _____
7. _____
8. _____
9. _____
10. _____

Activities

Flip the CLASSROOM

Internet Discovery

Objective: To obtain specific information from the internet regarding a computer or its associated parts

Parts: Computer with internet access

Procedure: Using the internet, locate technical information about a computer. Answer the following questions based on the retrieved information. Note that you may need to open more than one document in order to answer the questions.

Questions:

1. What is the name of the computer for which you found technical information?

_____

2. How much RAM comes with the computer?'

_____

3. Which URL did you use to find this information?

_____

4. Which search term(s) would you use for the following scenario? An HP Windows 10 computer has a Samsung ML-2160 laser printer attached. This printer supports both wired and wireless printing. The computer that is wired to the printer can print just fine, but no wireless devices in the house can access or even see the printer.

_____

_____

_____

5. Which search term(s) would you use in a search engine to help a friend who has accidentally deleted a file on a Windows 10 computer?

_____

6. Which search terms would you use to find a video that shows you how to add an application to a Windows 10 desktop computer?

_____

Soft Skills

Objective: To enhance and fine-tune a future technician's ability to listen, communicate in both written and oral forms, and support people who use computers in a professional manner

Procedure:

1. In a team environment, list three qualities that are important in a computer technician. Create scenarios that demonstrate these qualities. Share these findings with the class in a clear and concise way.
2. In a team environment, list three qualities that are not good practices for computer technicians. Create scenarios that demonstrate these qualities. Share these findings with the class in a clear and concise way.

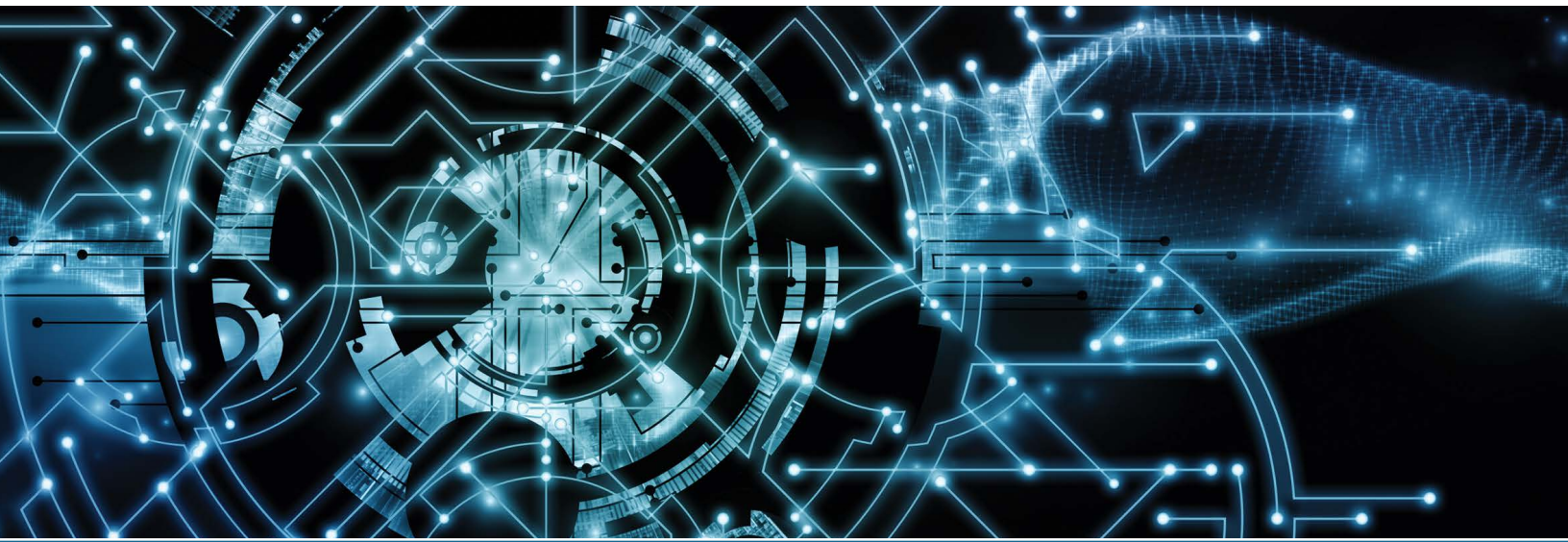
Critical Thinking Skills

Objective: To analyze and evaluate information as well as apply learned information to new or different situations

Procedure:

1. Find an advertisement for a computer in a local computer flyer, in a newspaper, in a magazine, in a book, or on the internet. List the components you know in one column and the components you do not know in another column. Select one component you do not know and research that component. On a separate piece of paper, write a description of the component, based on your research, and then share it with at least one other person. Write the name of the person with whom you shared.
2. Why do you think that many computer components are considered "throw-away" technology? List your reasoning. In groups of three or four, share your thoughts. Nominate a spokesperson to share your group reaction in two sentences or less.
3. One device touts a transfer speed of 1 Gb/s, whereas another device advertises 100 MB/s. Compare the two devices' transfer speeds and indicate which one is faster. For a hardware component you have or would like to have, find various products on the internet. Compare the products, paying particular attention to the transfer speed. Document your findings.

2 Connectivity



In this chapter you will learn:

- The purposes of various computer ports
- What to do if you don't have a particular port
- What types of devices connect to specific ports
- Different types of connectors and cables

CompTIA Exam Objectives:

- ✓ 1201-3.2 Summarize basic cable types and their connectors, features, and purposes.
- ✓ 1201-3.5 Given a scenario, install and configure motherboards, central processing units (CPUs), and add-on cards.
- ✓ 1202-4.7 Given a scenario, use proper communication techniques and professionalism.

Introduction to Connectivity

Now that we've discussed the basic parts of a PC, we are ready to dive into the technical details. This chapter explores wired and wireless connectivity—specifically, how to connect devices to specific ports. Some of the ports may be challenging at first, but it is important that people going into the IT field know how to connect devices to ports and the purpose of each port.

External Connectivity

A **port** is a connector on a motherboard or on a separate adapter that allows a device to connect to a computer. Ports can be found all around a computer or mobile device. Figure 2.1 shows a motherboard with some of the ports we will be covering. See how many you can already identify and then return to this figure after finishing the chapter. IT professionals should be able to recognize and identify the common ports used today.

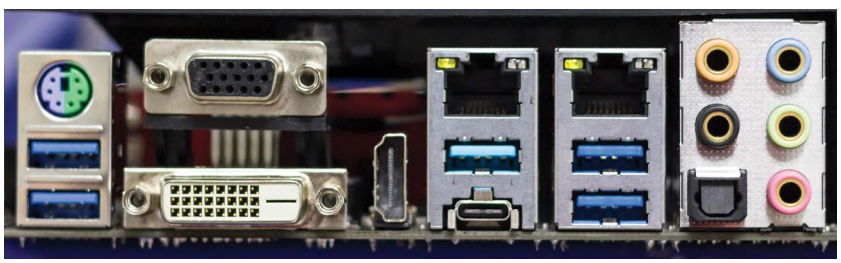


FIGURE 2.1 Motherboard ports

Mouse and Keyboard Ports

Mouse ports and **keyboard ports** were traditionally 6-pin **mini-DIN** ports that are sometimes called **PS/2 ports**. The mini-DIN port is keyed so the cable can be inserted only one way. Today, USB ports are more commonly used for mouse and keyboard connectivity, but some gaming motherboards still have a mini-DIN port. Manufacturers color-code a mouse port as green and a keyboard port as purple; they may put a small diagram of a keyboard or a mouse by each connector. Figure 2.2 shows mouse and keyboard connectivity options.

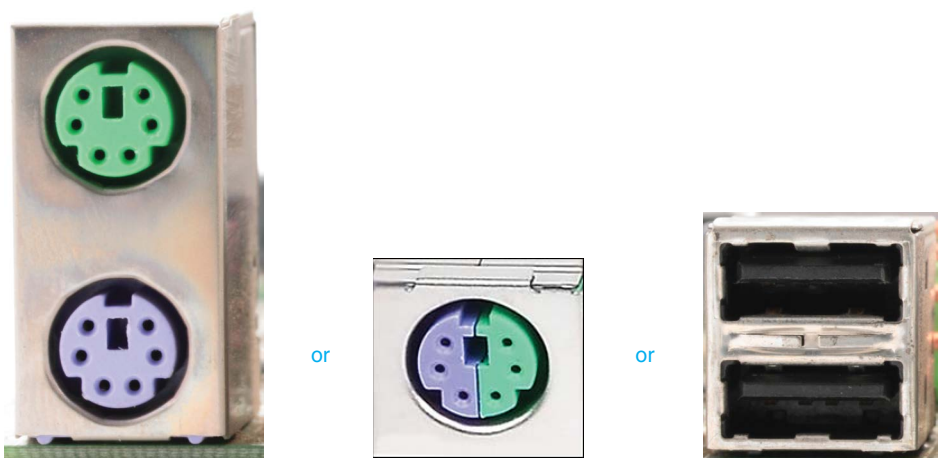


FIGURE 2.2 Mouse and keyboard ports

Multipurpose Ports

Some ports/cables can be used for multiple devices, including USB 2.0, USB 3.x, USB 4, USB-C, Thunderbolt, and Lightning. The USB port is probably the one people are most familiar with, but the Thunderbolt and Lightning ports are also considered multipurpose ports. Let's explore these ports.

USB Ports

USB stands for Universal Serial Bus and is one of the most popular ports on most devices. A USB port allows up to 127 connected devices to transmit at speeds up to 40 Gb/s (40 billion bits per second). Devices that connect to a USB port include printers, scanners, mice, keyboards, joysticks, optical drives, game pads, cameras, modems, speakers, IP phones, video phones, data gloves, and digitizers. Additional ports can sometimes be found on the front of a PC case or on the side of a mobile device. Figure 2.3 shows some USB ports.

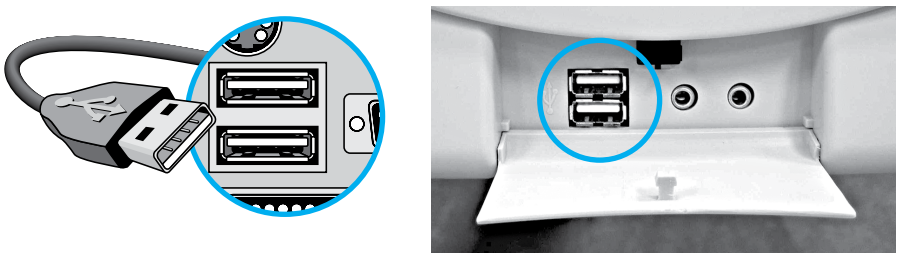


FIGURE 2.3 USB ports

USB Versions

USB ports come in several versions: USB 1.0/1.1, **USB 2.0** (Hi-Speed), **USB 3.0** (3.2 Gen 1 SuperSpeed and 3.2 Gen 2 SuperSpeed+), and USB4.x. Figure 2.4 shows the different USB versions and speed symbols.

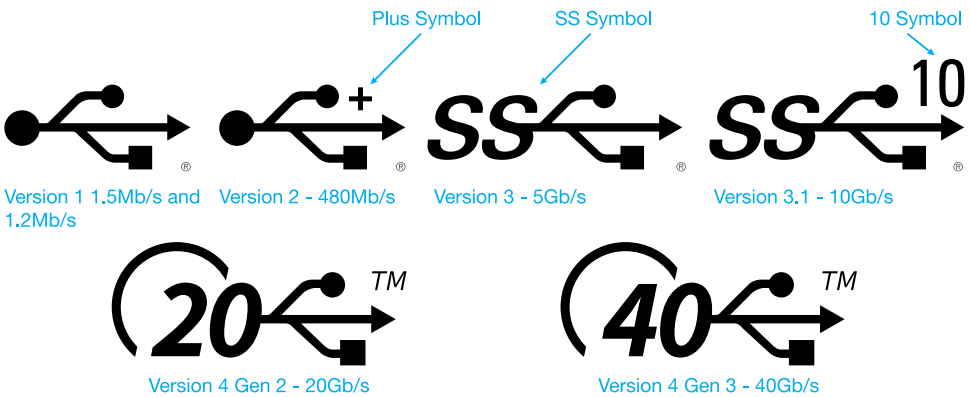


FIGURE 2.4 USB versions, speeds, and symbols

TECH TIP

Understanding USB speed through documentation

When you're trying to figure out the speed of your USB ports, documentation can be really helpful. Not every port has a clear label, so the most reliable way to find out what you're working with is to look at the technical specifications of your computer or motherboard. This will give you a better idea of the types of USB connections available and what they can do.

USB Power Delivery (USB-PD)

USB ports have been able to provide 5V at 500mA for 2.5 watts of power to devices since version 2.0. The newest USB standard, Power Delivery (**PD** or **USB-PD**), can provide up to 48V at 5A for 240 watts of power. The standard actually has several levels of power delivery: 10, 18, 36, 60, 100, 140, and 240 watts of power. All USB4 connections allow charging a USB device.

USB Cables

Each USB standard has a maximum cable length (shown in Table 2.1, later in the chapter). These standards are provided to ensure that devices function properly. USB cables can be longer than these specifications, but if they are, they may not work as well. You can use an active USB extension cable (repeater cable) or a powered USB hub (covered later in the chapter) to go further distances.

If a USB port provides power to a device, the maximum cable length is shorter. For example, if a USB 2.0 PD device is being used, the maximum cable length is less than 13 feet (4 m). If a USB 3.1 PD device is used with a USB Type-C cable, then the cable length should be less than 3.3 feet (1 m). A PD device requires a Type-C cable, but not all ports or cables support PD.

USB Connectors

Older USB ports are commonly known as **USB Type-A** and **USB Type-B**. A USB printer cable, for example, has a Type-A male connector on one end and a Type-B male connector on the other end. The port on the computer is a Type-A port. Figure 2.5 shows Type-A and Type-B connectors.

FIGURE 2.5 USB Type-B and Type-A connectors

The **USB Type-C** (sometimes called **USB-C**) connector is the latest type and will eventually replace the Type-A and Type-B connectors. With older devices, it is possible to use an adapter in order to attach to a Type-C connector. While many USB 3.0 ports use the Type-C design, some still feature the traditional Type-A connector. It's worth noting that for USB 3.1 ports and newer versions, you'll need a Type-C cable to take advantage of their advanced features and faster speeds. USB-C can carry audio, video, can data. Notice in the photo of a USB Type-C connector in Figure 2.6 that the cable connector could be inserted into the USB-C port with either side facing up.

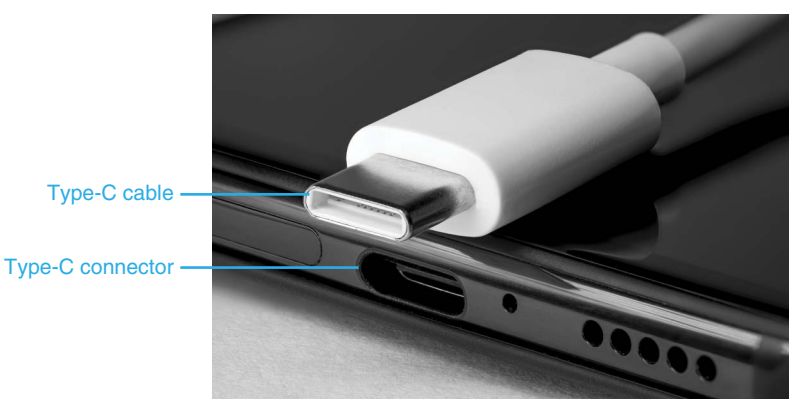


FIGURE 2.6 USB Type-C cable and connector

MiniUSB and MicroUSB

Two smaller USB ports used on portable devices such as hubs, external hard drives, digital cameras, and smartphones are the **miniUSB** and **microUSB** ports. There are several types of these smaller USB ports: mini-A, mini-AB, micro-B, and micro-AB. The mini-AB and micro-AB ports accept either a mini-A/micro-A or a mini-B/micro-B cable end. Figure 2.7 shows the standard Type-A USB cable that would be inserted into a PC port compared to the mini- and micro-USB cables used with mobile devices. Figure 2.8 shows a USB 3.0 micro-B port and connector.

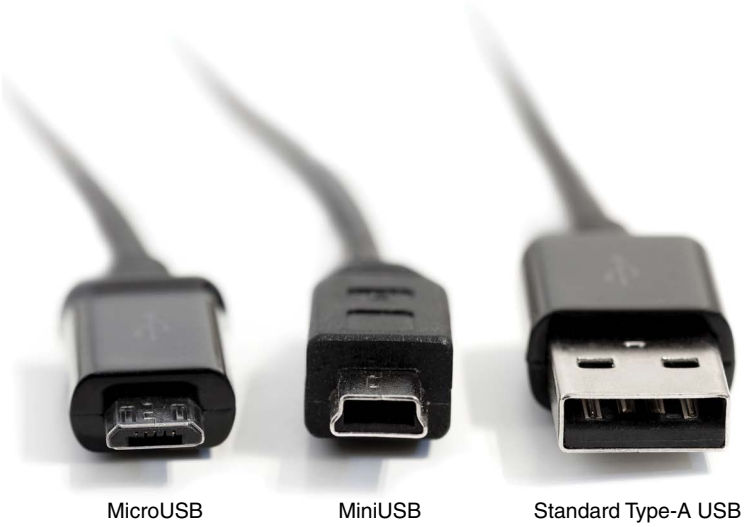


FIGURE 2.7 Micro-USB, mini-USB, and USB Type-A cables

FIGURE 2.8 USB 3.0 micro-B port and connector

USB Hubs

A USB port can connect to multiple devices by using a USB hub. Many hubs operate in two power modes: self-powered and bus powered. A self-powered hub (sometimes called a powered hub) has an external power supply attached. A bus-powered hub has no external power supply connected to it. It's important to note that a self-powered hub may have a toggle switch that needs to be set in order to provide power.

After you have tested the USB devices connected to a self-powered hub, you can disconnect the hub's power supply and retest the devices. If all the devices function properly without the power supply, you can leave it disconnected. This process helps ensure that the devices are working correctly even without external power. Figure 2.9 shows USB hub connectivity, and Figure 2.10 shows USB cabling rules.

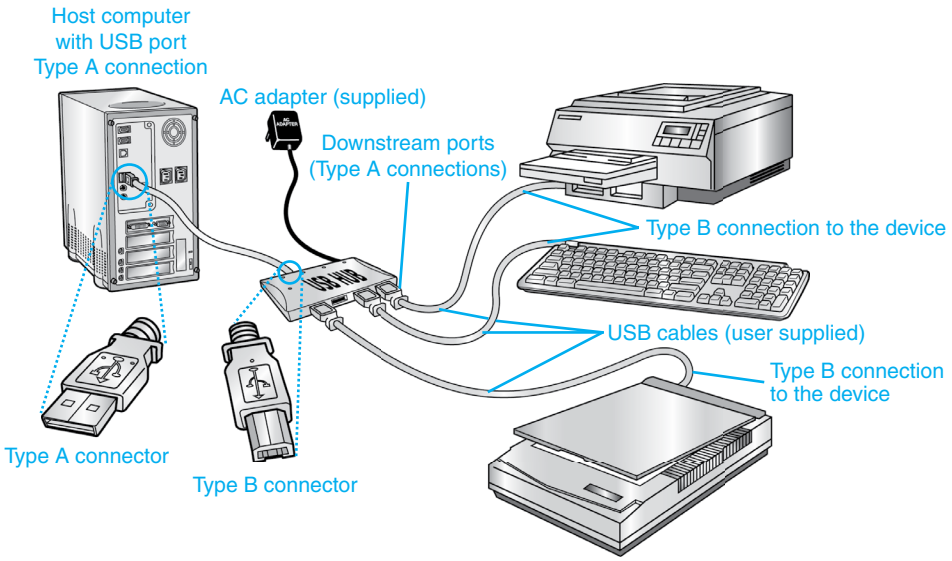
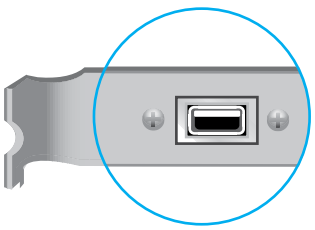


FIGURE 2.9 USB hub connectivity



USB cabling rules

- 5 hubs maximum (total max range of 88.5 feet or 27 meters)
- 127 devices maximum connected to up to 5 hubs
- Maximum distance between 2 USB hubs
  - high-speed devices – 16.4 feet or 5 meters
  - low-speed devices – 9.8 feet or 3 meters

FIGURE 2.10 USB cabling rules

USB ports have always been able to provide power to unpowered devices, such as flash drives. A **charging USB port** is a port designed to be able to provide power and charge attached devices. Note that not all USB devices can be powered on while charging. With a **sleep-and-charge USB port**, the port provides power to charge the device even when the computer is powered off. See the computing device's specifications to see if a USB port supports this feature. Table 2.1 summarizes USB types, alternate names, speeds, port colors, and cable requirements.

TECH TIP

Safely removing USB devices

To properly remove a USB device, do not simply unplug it from the port. Instead, click on the *Safely Remove Hardware and Eject Media* from the notification area on a Windows device and then select the USB device to remove. On a Mac, right-click the desktop icon for the device and select *Eject x* (where *x* is the device name) or drag the desktop icon to the trash can. In Ubuntu Linux, locate the device in Files or File Explorer. Click the small eject icon or right-click the name of the device and select *Eject*. The operating system will notify you when it is safe to unplug the device. Following these steps helps prevent data loss and ensures that your device is properly disconnected.

TABLE 2.1 USB port summary

Port type and alternate name	Maximum transmission speed	Port color	Cable type/length and alternate name
USB 1.x	1.5 Mb/s and 12 Mb/s	Usually white	9.8" (3 m) Type-A 1.0 low speed 1.1 full speed
USB 2.0	480 Mb/s	Black	9.8" (3 m) Type-A Hi-Speed
USB 3.0	5 Gb/s	Blue	9.8" (3 m) Type-A or Type-C SuperSpeed
USB 3.1 Gen 1	5 Gb/s	Blue	9.8" (3 m) Type-A or Type-C SuperSpeed
USB 3.1 Gen 2	10 Gb/s	Teal	9.8" (3 m) Type-C SuperSpeed+
USB 3.2 Gen 1 (3.2 Gen 1x1 1 lane) (3.2 Gen 1x2 2 lanes)	5 Gb/s and 10 Gb/s	Red	9.8" (3 m) Type-C SuperSpeed USB 5Gbps SuperSpeed USB 10Gbps
USB 3.2 Gen 2 (3.2 Gen 2x1 1 lane) (3.2 Gen 2x2 2 lanes)	10 Gb/s and 20 Gb/s	Red	9.8" (3 m) Type-C SuperSpeed USB 10Gbps SuperSpeed USB 20Gbps
USB4 Gen 2 (2 lanes)	20 Gb/s	N/A	9.8" (3 m) Type-C
USB4 Gen 3 (2 lanes)	40 Gb/s	N/A	9.8" (3 m) Type-C
USB sleep-and-charge	N/A	Yellow, orange, or red	N/A

USB Converters

USB converters have become more popular for modern laptops and tablets that focus on being thin and lightweight. Many of these devices don't include traditional ports, making it challenging to connect to external displays or wired Ethernet networks. Whether you need to connect to an Ethernet network, hook up an external monitor, or use a different type of connector, USB converters provide a flexible solution, as shown in Figure 2.11.

FIGURE 2.11 USB-to-Ethernet converter

Installing Extra USB Ports

Sometimes people want more USB ports and do not want to add an external hub. Many motherboards support adding two or more USB ports by using a cable that attaches to an internal USB connector on the motherboard, also known as a USB header. The term **header** simply means a set of motherboard pins for a specific purpose, like USB, SATA, eSATA, RGB LEDs (lights), and TPM (Trusted Platform Module). The headers associated with ports mount in an expansion slot space, but they do not have a card that plugs into an expansion slot. Even if the motherboard has such pins, the ports and cable assembly might have to be purchased separately. Figure 2.12 shows sample USB ports that attach to a motherboard.

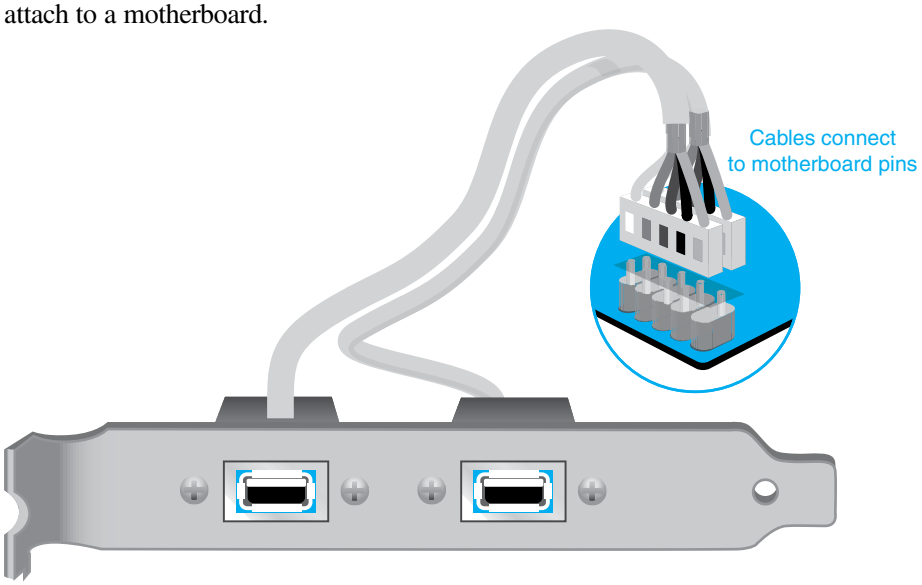


FIGURE 2.12 Installing extra USB ports

Thunderbolt

Thunderbolt ports are versatile connectors that are mainly used for video but that can also transfer power, audio, and data to external devices like hard drives. The Thunderbolt interface

was developed by Intel with support from Apple. The Thunderbolt port used on Apple computers has the same connector as the mini-DisplayPort; however, Thunderbolt 3 uses the USB Type-C connector.

Thunderbolt 3 is notable because it's the first version to support USB devices. It offers incredibly fast data transfer speeds of up to 80 Gb/s, allowing you to move large files quickly. Additionally, you can daisy-chain up to six devices together through a single Thunderbolt port, making it easy to connect multiple monitors or peripherals without cluttering your workspace. Figure 2.13 shows a Thunderbolt port and cable. Look back at Figure 2.6 to see the Type-C connector and cable that Thunderbolt 3 and 4 use.

FIGURE 2.13 Thunderbolt cable and port

TECH TIP

Can a Thunderbolt 3 or 4 device work in a USB-C port?

While Thunderbolt 3/4 devices use the same USB-C connector, their compatibility isn't always straightforward. A Thunderbolt device can physically connect to a USB-C port, but performance is not guaranteed. If it does work, it will operate at the slower USB-C speeds rather than Thunderbolt speeds.

On the other hand, USB-C devices can typically connect to Thunderbolt 3/4 ports without any issues. These devices will function normally and often at full USB-C speeds. It's important to understand that while the ports look identical, the underlying technology differs.

Lightning

The **Lightning port**, developed by Apple, is an 8-pin port that accepts the cable connector with either side facing up (that is, it is reversible). The Lightning port can carry data and power from mobile devices to other devices, such as cameras, external monitors, and external storage devices. The Lightning port supports USB data and USB charging, but the Lightning port and cable are not compatible with USB-C ports and connectors. The Lightning port is being phased out, and Apple is now using USB-C connectors instead. Figure 2.14 shows a Lightning cable. Table 2.2 shows a comparison of the three multipurpose ports.

FIGURE 2.14 Lightning cable

TABLE 2.2 Multipurpose port comparison

Port type	Maximum transmission speed	Type of connector	Platforms	What it carries
USB4 Gen 3	40 Gb/s	USB Type-C 24-pin reversible connector	Found on Apple and PCs	Data and power
Thunderbolt 4	80 Gb/s	USB Type-C 24-pin reversible connector	Intel and Apple developed	Data and power
Lightning	Speeds up to USB 3.0, but normally 480 Mb/s	8-pin reversible connector	Apple proprietary	Data and power

Video Ports

Video ports are used to connect displays, like monitors or TVs, to computers and other devices. Video output can be the older method of an **analog signal** (varying levels, such as seen with an audio signal) or the newer output that uses a **digital signal** (1s and 0s).

Most modern computers use digital signals because they are more efficient. Digital video doesn't need to be converted from analog, which helps maintain better image quality. This is relevant because there are still video ports around that are designed for analog signals. Figure 2.15 shows the difference between analog and digital signals.

The most common video ports used today are VGA, DVI, DisplayPort, and HDMI. USB-C is also used for displays today. Let's dive into the ports and cables.

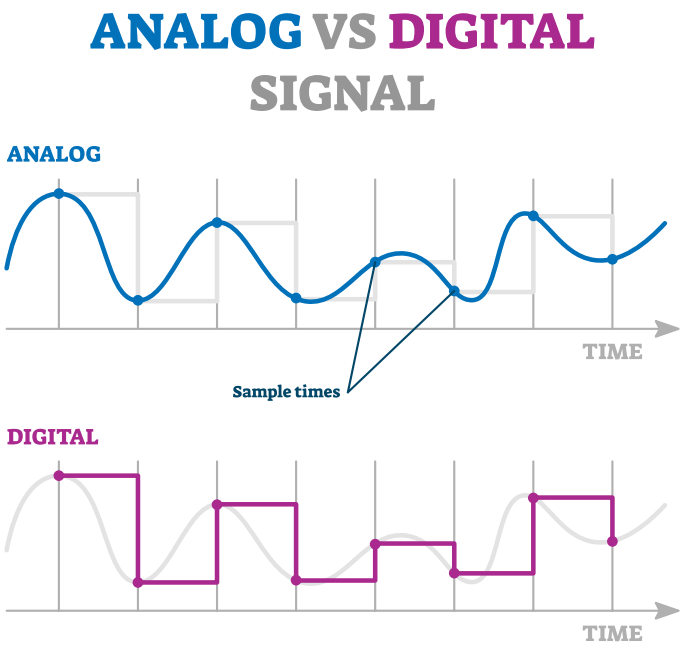


FIGURE 2.15 Analog and digital signals

Video Graphics Array (VGA)

The video graphics array port, or **VGA port**, was designed for analog output to an old cathode ray tube (CRT) monitor. VGA ports are easy to identify because they have three rows of holes—15 in total. Ports that have holes are known as female ports. The VGA port is sometimes seen in documentation as an HD15, DE15, or D-sub (DB) port. The *D* in these names comes from the VGA connector being a d-shell connector. Look at the VGA port in Figure 2.17 and imagine that port turned sideways so it looks like the letter D. The VGA cable has a DB15 male end that attaches to the DE15 female port.

Digital Visual Interface (DVI)

Another port is the Digital Visual Interface port, or **DVI port**, which has three rows of square holes. The DVI port was designed to provide high-quality digital video transmission, delivering superior image quality compared to older analog connections. There are several types of DVI connectors, and the one used depends on the type of display attached.

Terms used with these DVI connectors are single link and dual link. A single link connection allows lower video resolutions than a dual link connection because a dual link port has more pins. The two major types of connectors are DVI-D and DVI-I. DVI-D is used for digital video connectivity only. DVI-I can be used for both digital and analog monitors, and it is the most common. A less common type is DVI-A, which is used for analog connectivity (and is not shown in Figure 2.16 with the other DVI connectors). Figure 2.17 shows both a DVI cable and a VGA cable.

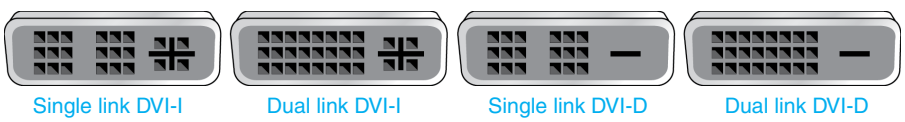


FIGURE 2.16 DVI connectors

FIGURE 2.17 DVI and VGA cables

Some monitors can also connect to the older VGA ports. Some video adapters also enable you to connect to a video device (such as a television) that has an **S-Video port**. Figure 2.18 shows a video adapter with a DVI port as the left connector, an S-Video port in the center, and a VGA port on the right.

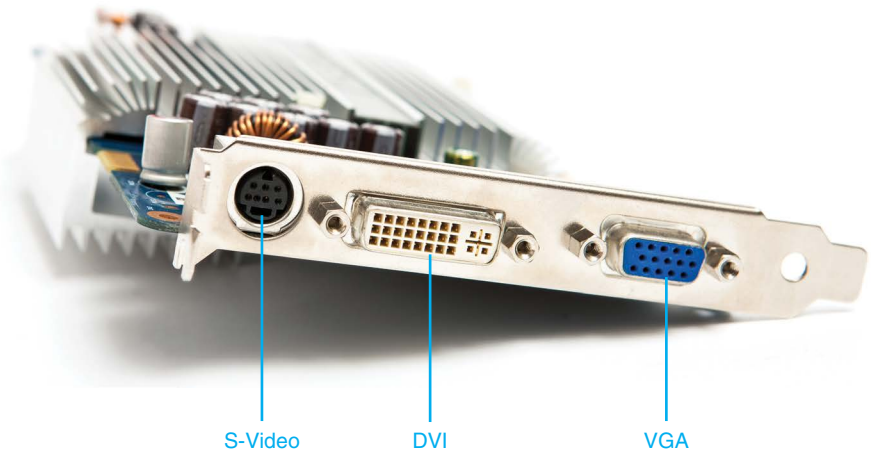


FIGURE 2.18 S-Video, DVI, and VGA ports

TECH TIP

Matching a monitor to the port type

Be careful when installing a monitor. For example, ensure that the video port matches the DVI connection type for the monitor. Converters can be purchased to adapt to a monitor with a different type of video port.

DisplayPort

The **DisplayPort** (DP) can send and receive video, audio, or both types of signals simultaneously. Its main benefit is its ability to support higher resolutions and fast screen refresh rates, making it ideal for high-performance computer monitors, gaming setups, and professional graphics work. The port is designed to primarily output to display devices, such as monitors, televisions, and home theaters. Figure 2.19 shows a DisplayPort and a cable that would connect to this port.

FIGURE 2.19 DisplayPort

HDMI

Another upgrade over DVI is High-Definition Multimedia Interface (**HDMI**), a digital interface that can carry audio and video over the same cable. Its key benefit is its widespread compatibility and prevalence in consumer electronics. HDMI ports are found on cable TV boxes, televisions, video adapters, laptops, desktops, and tablets. Smaller mini-HDMI or micro-HDMI connectors are used with devices such as cameras, tablets, and smartphones. Figure 2.20 shows an HDMI port and cable. Table 2.3 describes the different HDMI ports.

FIGURE 2.20 HDMI port and cable

TABLE 2.3 HDMI ports

HDMI connector type	Description
A	19-pin port found on a TV or PC that can have a Category 1 (standard) or Category 2 (high-speed) cable attached
B	29-pin port used with very high-resolution displays
C	19-pin mini-HDMI port found on mobile devices
D	19-pin micro-HDMI port found on mobile devices

Figure 2.21 shows a video card that would be used in a gaming computer. On top is a dual link DVI-D port. On the bottom, from left to right, are a DisplayPort, an HDMI port, and a dual link DVI-I port. Table 2.4 summarizes important PC video ports.

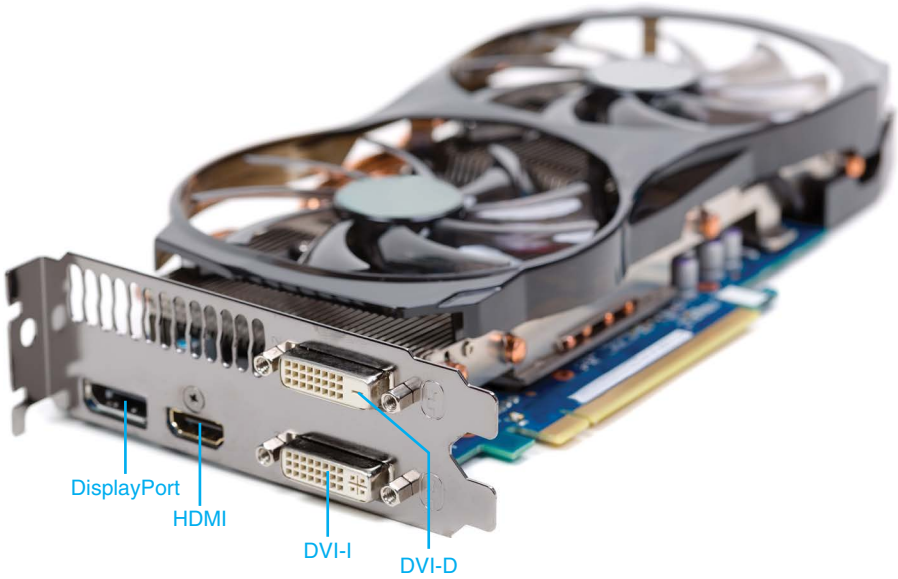


FIGURE 2.21 Video ports, including a DisplayPort, an HDMI port, and two DVI ports

TABLE 2.4 Video port summary

Port type	Analog, digital, or both	Max transfer speed	Carries audio?	Maximum cable lengths
VGA	Analog	N/A	No	Depends on resolution
DVI-D	Digital	Dual link 7.92 Gb/s	No	Up to 15 feet (4.57 m) for display resolutions up to 1920×1200
DVI-I	Both	Single or dual link	No	Not in the standards, but a general rule of thumb is up to 15 feet (4.57 m) for display resolutions up to 1920×1200
DisplayPort	Digital	80 Gb/s	Yes	9.8 feet (3 m) for passive and 108 feet (32.9 m) for active
HDMI	Digital	48 Gb/s	Yes	Generally up to 16 feet (4.88 m) for standard cable and up to 100 feet (30 m) for high-speed, good-quality cable/connectors
Thunderbolt	Digital	80 Gb/s	Yes	Up to 9.8 feet (3 m)
USB-C (DisplayPort, HDMI, or Thunderbolt over USB-C)	Digital	Varies	Yes	13 feet (4 m) for passive and 6.5 feet (2 m)

Video Adapters and Converters

Converters can be purchased for video ports to convert from one of the major types to another type. For example, Figure 2.22 shows a **DVI-to-HDMI adapter** (with both ends visible).

FIGURE 2.22 DVI-to-HDMI adapter

Audio Ports

A **sound card** (sometimes called an audio card) converts digital signals from a computer into sound and vice versa. While many computers have built-in sound ports integrated into the motherboard, some people choose to install a separate sound card for improved audio quality. This can enhance the overall listening experience, especially for music, gaming, and other audio applications. The most common sound ports include a port for a microphone, MP3 player, or other audio device and one or more ports for speakers. The ports can accept analog or digital signals. (Refer to Figure 2.15 to see the difference between analog and digital signals.)

The traditional analog sound ports are 3.5 mm (see Figure 2.23). The newer Sony/Phillips Digital interface (**S/PDIF**) in/out ports, on the left in Figure 2.23, are used to connect to various devices, such as digital audio tape players/recorders, DVD players/recorders, and external disc players/recorders. There are two main types of S/PDIF connectors: an RCA jack (last port on the left) used to connect a coaxial cable and a fiber-optic port for a TOSLINK cable connection (two optical ports beside the RCA/Digital Out jack in Figure 2.23).

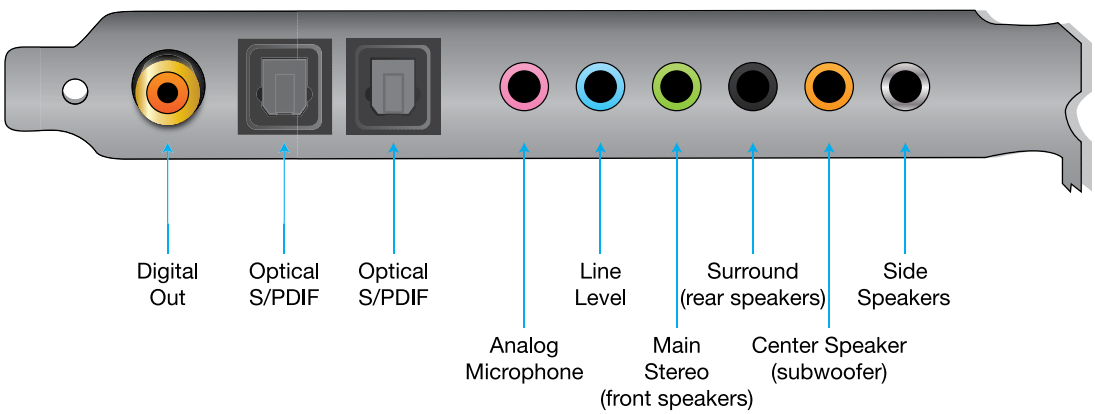


FIGURE 2.23 Sound card ports

eSATA Ports

SATA connections are commonly used for storage devices. A 7-pin nonpowered External Serial AT Attachment, or **eSATA**, port is used for connecting external storage such as hard drives or optical drives. However, eSATA ports have become increasingly rare on modern laptops, largely replaced by USB 3.0 or newer connectivity options. A desktop motherboard typically has a SATA

header so that an eSATA port can be easily added. eSATA can transfer data at 6 Gb/s. Devices can connect at a maximum of approximately 6.6 feet (2 m).

A variation of the eSATA port is the **eSATAp port**, which is also known as eSATA/USB, or power over eSATA. This variation can accept eSATA or USB cables and provides power when necessary. Figure 2.24 shows a standard **eSATA cable**, eSATA port, and eSATAp (eSATA/USB combination) port.

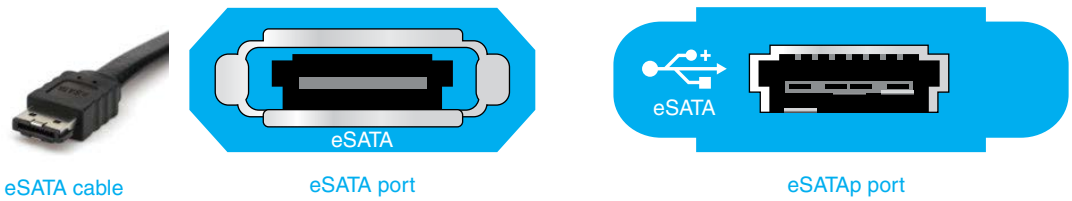


FIGURE 2.24 eSATA cable and eSATA/eSATAp ports

Modem and Serial Ports

A modulator/demodulator, or **modem**, connects a digital computer to a different type of network, such as a phone line or an internet connection. An internal modem used to connect a computer to a phone network is an adapter that has one or two **RJ11** phone jack ports The RJ11 port labeled *Line* is for the connection to the wall phone jack; the one labeled *Phone* is to attach a phone, if needed. Figure 2.25 shows an internal modem with two RJ11 ports.

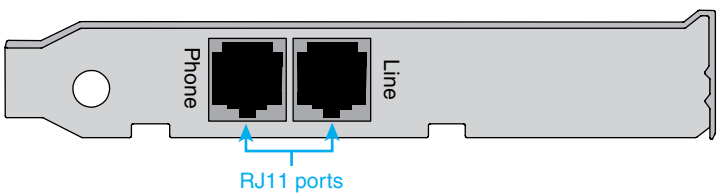


FIGURE 2.25 An internal modem with two RJ11 ports

The RJ11 port, which has 4 conductors, is used in some home setups for both internet and phone connections. This type of port connects a modem to the internet, allowing users to go online. It can also be used to connect a regular landline phone. Figure 2.26 shows such a port, labeled as Phone Lines 1&2.

Serial ports are found on older modems and motherboards, network equipment, alarm systems, automation systems, communication systems, single-board systems, and point of sale (POS) terminals. Serial ports are 9-pin male (they have pins instead of holes) and are sometimes called **DB9** or RS-232 ports. Figure 2.27 shows the DB9 serial ports on an older computer. Figure 2.28 shows an example of a **serial cable**. The DB9 female connector would attach to the DB9 male connector on a device or motherboard. Figure 2.29 shows a USB-to-serial converter cable, which you might need to connect an external modem to a modern motherboard.

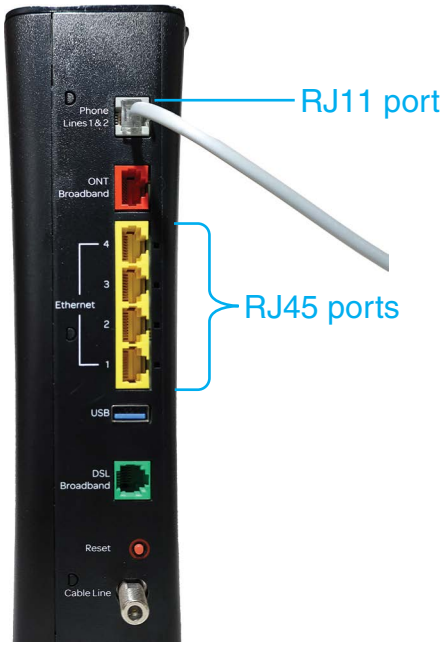


FIGURE 2.26 Cable modem with RJ11 port

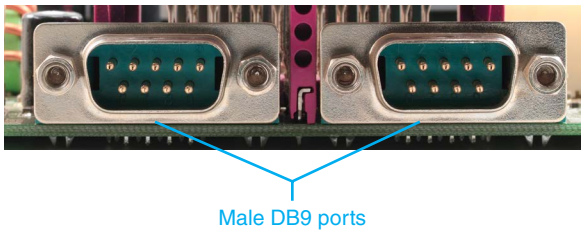


FIGURE 2.27 DB9 serial ports

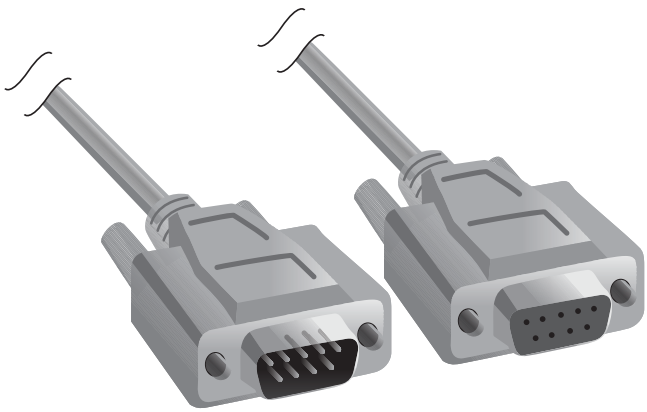


FIGURE 2.28 Serial cable ends

FIGURE 2.29 USB-to-serial port converter

Network Ports

A **network port** is used to connect a device such as a computer or printer to a network. The most common type of network port is an **Ethernet port**, also known as an **RJ45 port** (see Figure 2.30). A network cable inserts into the Ethernet port to connect the computing device to the wired network. A network port is sometimes called a **NIC** (network interface card/controller).

FIGURE 2.30 An RJ45 Ethernet port

An RJ45 port looks very similar to an RJ11 phone jack (see Figures 2.25 and 2.26). However, the RJ45 connector has 8 conductors (wires) instead of 4. Look closely at the connectors in Figure 2.31 to see the difference. The RJ11 connector is on the left.

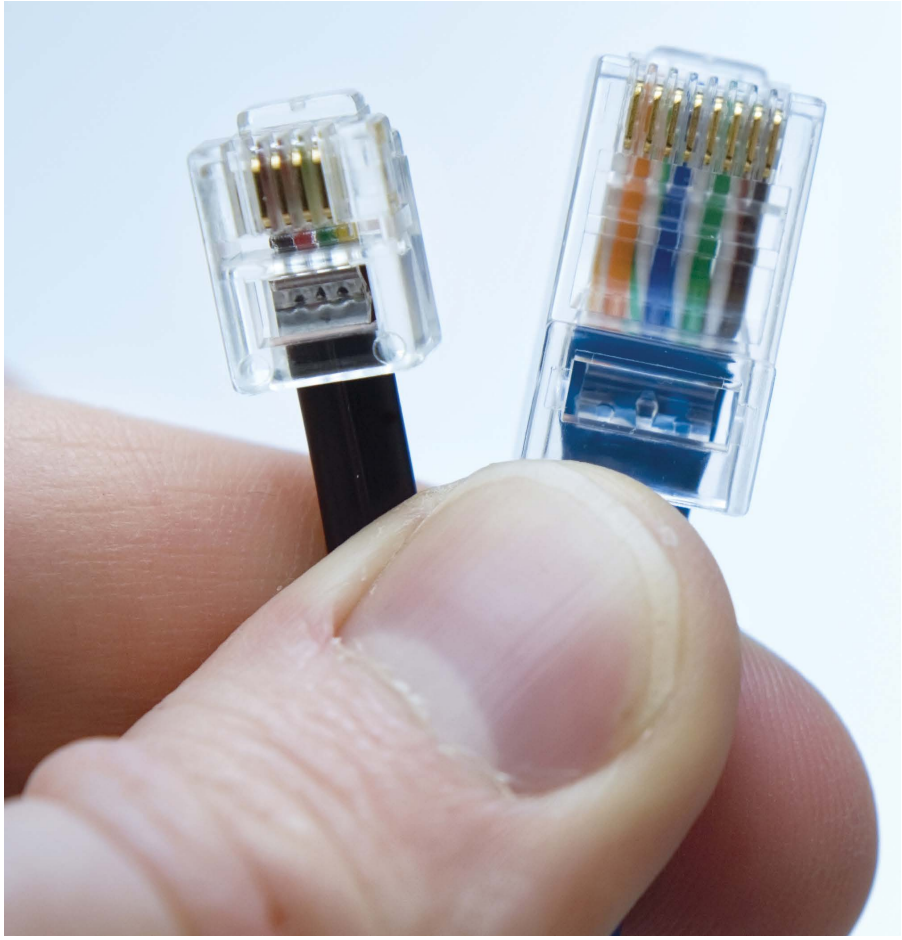


FIGURE 2.31 RJ11 and RJ45 connectors

TECH TIP

Ethernet port symbols

An Ethernet port commonly has LEDs on top or near the port to indicate data activity. An Ethernet port may also have one of the following symbols:

Network Cabling

People who work in IT have all types of devices—including PCs, printers, servers, projectors, and displays—that connect to the network. This is a good time to make sure you know what type of cable might be used. We will start with **copper cabling** that sends electrical pulses to create the digital 1s and 0s and then look at fiber-optic cabling, which uses light instead.

Coaxial

Copper coaxial cable is commonly used for transmitting signals in various applications, such as telecommunications and broadcasting. It consists of a center conductor made of copper wire, surrounded by an insulating layer and a shield of copper braid, a metallic foil, or both, as shown in Figure 2.32, to protect the center conductor from outside noises called electromagnetic interference (EMI).

A type of connector you might see associated with video, but more likely with cable TV or when attaching a wireless network antenna to a connector, is a Bayonet Neill–Concelman (BNC) connector. A **BNC connector** is used with a **coaxial** cable to provide a secure connection for transmitting video signals. These connectors are often found in professional video equipment and surveillance systems. Figure 2.33 shows the front of a BNC connector already put onto the coax cable.

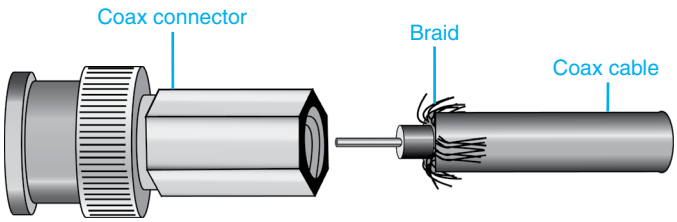


FIGURE 2.32 Coaxial cable with a BNC connector

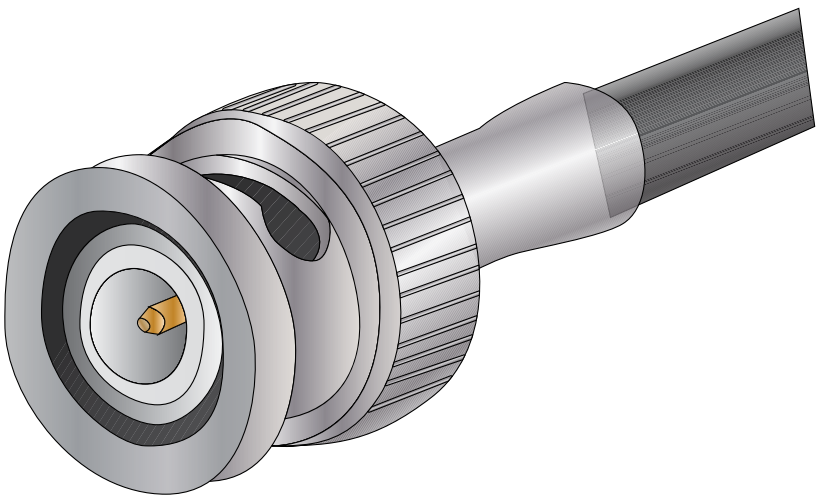


FIGURE 2.33 BNC connector

Another widely used connector is the **F-type** connector, which is primarily used for cable TV and satellite connections. Unlike BNC connectors, F-type connectors screw onto the receiving device, providing a secure connection for transmitting signals. While BNC connectors are favored in professional settings for their quick-connect feature and simplicity, F-type connectors are more common in homes and offices due to their ease of use and affordability. Figure 2.34 shows two popular coax connectors: BNC and F. Notice that the BNC connector has a notched side to turn and twist onto the receiving connector. The F-type connector simply screws onto the receiving connector.

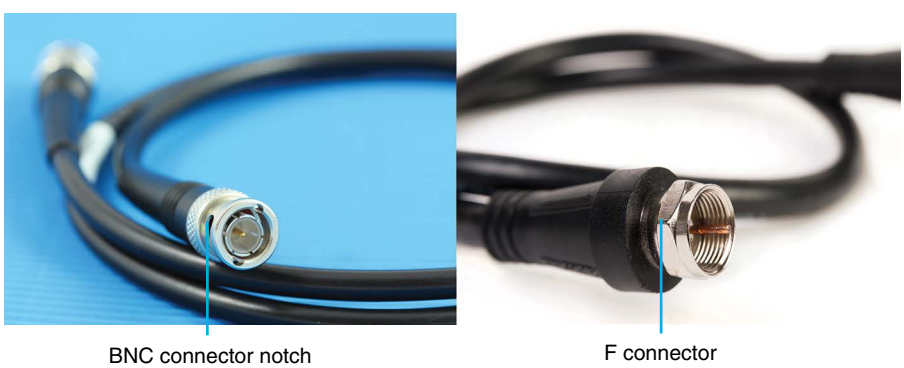


FIGURE 2.34 Coaxial BNC and F connectors

Coaxial cable is rated according to whether it will be used in an interior or exterior space. It's important to use the appropriate cable type for the installation (see Table 2.5). Be careful when bending coaxial cables, as sharp bends can damage the cable and affect signal quality. If you have a problem with your coaxial cable setup and you are using the correct type of cable and connector, the issue may be that the coax connector is not attached properly.

TABLE 2.5 Coax cable types

Coax cable type	Description
RG-6*	This is the type of cable least likely to be used in a network. It is a 75-ohm cable suitable for distributing signals for a cable TV, satellite dish, or rooftop antenna. It has better shielding than RG-59, so it is larger in diameter. Typical distances are 1,000 feet (305 m) to 1,500 feet (457 m). It can carry frequencies up to 2,200 MHz.
RG-59	This type of 75-ohm cable is not used in LANs but is used in video installations. Typical distances are 750 feet (225 m) to 1,000 feet (305 m). It can carry frequencies up to 1,000 MHz.

*RG stands for radio grade.

Ethernet Cable

Ethernet is the most common type of wired network in homes and in companies. An Ethernet cable attaches to an RJ45 Ethernet port. The most common type of network cable is **unshielded twisted pair (UTP)**. UTP comes in several types: **Cat 5**, **Cat 5e**, **Cat 6**, and **Cat 6a**. Cat 7 and Cat 8 are also available. The *Cat* in these cable names is short for *category*.

UTP cable has 8 wires that are twisted to prevent data that is traveling along one wire from interfering with an adjacent wire—which is called crosstalk. Figure 2.35 shows a Cat 5e cable and a Cat 6 cable. Cat6 cables often include an internal separator to further reduce signal interference. Cat 6a has more cable twists to reduce crosstalk (data from one wire interfering with the data in an adjacent wire). Cat 6a cabling might also have a thicker conductor and jacket. Table 2.6 shows a comparison of the cable types.

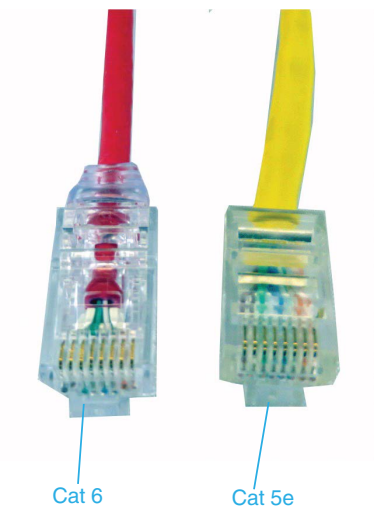


FIGURE 2.35 Cat 6 and Cat 5e cable

TABLE 2.6 Ethernet cable comparison

Ethernet cable type	Maximum transmission speed	Bandwidth	Distance limitation
Cat 5	100 Mb/s	100 MHz	328 feet (100 m)
Cat 5e	1000 Mb/s, or 1 Gb/s	100 MHz	328 feet (100 m)
Cat 6	1000 Mb/s, or 1 Gb/s*	250 MHz	328 feet (100 m)
Cat 6a	10,000 Mb/s, or 10 Gb/s	500 MHz	328 feet (100 m)
Cat 7	10,000 Mb/s, or 10 Gb/s	600 MHz	328 feet (100 m)
Cat 8	25,000/40,000 Mb/s or 25/40 Gb/s	2,000 MHz	328 feet (100 m)

*Cat 6 can support speeds of 10 Gb/s at lengths up to 165 feet (55 m).

The alternative to UTP is **shield twisted pair (STP)** cable, which is used between buildings and in manufacturing, security alarm systems, audio connections, and harsh environments where the cabling needs a little more shielding to keep the data intact. The shielding is provided by a foil wrapped around all the cables as well as around each grouping of two cables, which makes STP cabling thicker than UTP. Cat 7 and Cat 8 cabling use this type.

STP is also used with direct burial and underground cable in an outdoor environment. **Direct burial cable** is designed to be used underground without any extra protection provided—like tubing, piping, or extra covering—because this type of cabling has extra insulation, cover, and waterproofing added. UTP direct burial cable is also available and designed to protect against moisture.

Both UTP and STP use the RJ45 connector, which has a tang on one side. To remove a cable from an Ethernet port, press on the tang to release the cable from the port. When inserting the cable, ensure that the cable is oriented properly and then push the cable firmly into the port until you hear the click when the tang fits snuggly into the port. Figure 2.36 shows the top and bottom of an Ethernet cable connector.

FIGURE 2.36 Ethernet RJ45 connector with tang

Ethernet cabling in a corporate environment makes use of a patch panel to terminate cabling from one part of a building to another. On the back of a patch panel is a **punchdown block** that is also found in traditional phone networks. Figure 2.37 shows a technician using a **punchdown tool** to firmly attach a wire into the punchdown block.

A special type of UTP or STP cable is **plenum cable**. A plenum is a building's air-circulation space for heating and air-conditioning systems. Plenum cable is treated with Teflon or alternative fire-retardant materials to reduce the fire risk. Plenum cable produces less smoke and is less toxic when it burns than is regular networking cable.

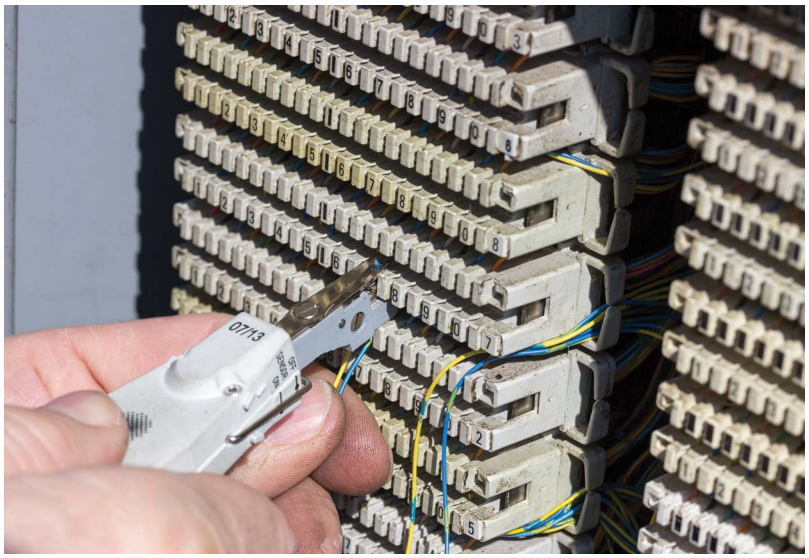


FIGURE 2.37 Connecting a wire on the punchdown block using a punchdown tool

An alternative to plenum cable is polyvinyl chloride (**PVC**) cable, which has a plastic cable insulation or jacket. PVC is cheaper than plenum cable, and it can have flame-retardant chemicals added to make it compliant with building codes. PVC is usually easier to install than plenum cable.

To avoid extra troubleshooting time, most businesses install their network cable according to the ANSI/TIA/EIA-568-A or 568-B (commonly shown as **T568A** and **T568B** or **568A/B**) standard. These standards specify how far the cable can extend, how to label it, what type of connectors to use, and so forth. Figure 2.38 shows that the colored wires within a connector must be in a particular order. Chapter 13, "Networking," shows how to make cables according to the T568A and T568B standards.

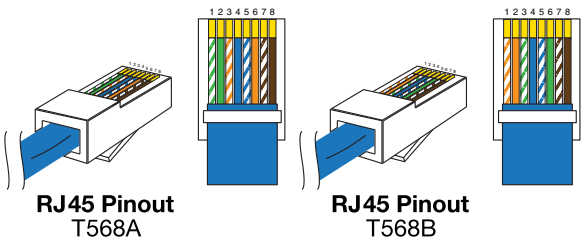


FIGURE 2.38 ANSI/TIA/EIA T568A and T568AB wiring standards

Fiber Media

Fiber cable, also known as **optical cable** or fiber-optic cable, is made of glass or a type of plastic fiber and is used to carry light pulses. Fiber cable can be used to connect a workstation to another device, but in industry, the most common uses of fiber-optic cable are to connect networks forming the network backbone, networks between buildings, service provider high-speed networks, and homes to a service provider. Figure 2.39 shows fiber connections.

There are many different types of fiber connectors, and some of them are proprietary. Four of the most common connectors used with fiber-optic cable are the Mechanical Transfer Registered Jack, or MT-RJ (common in home installations), **straight tip (ST) connector**, **subscriber connector (SC)**, and **Lucent connector (LC)**. Figure 2.40 shows three of these connectors.

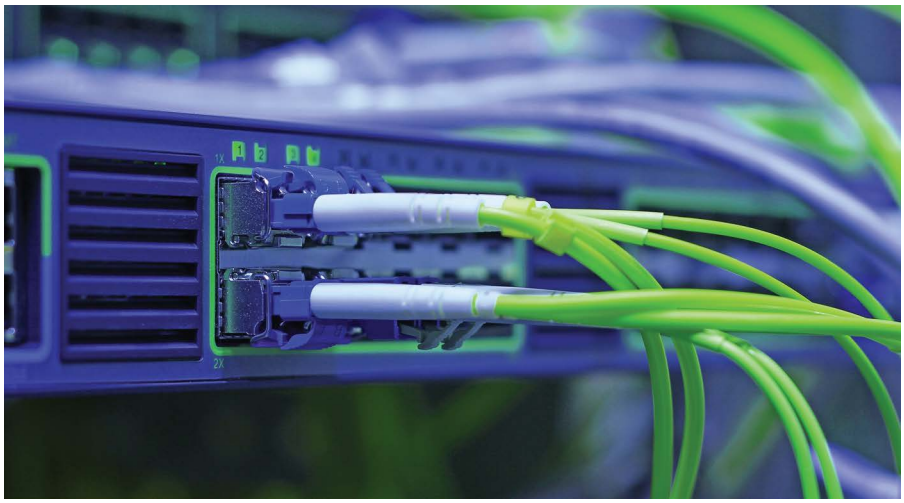


FIGURE 2.39 Fiber connections

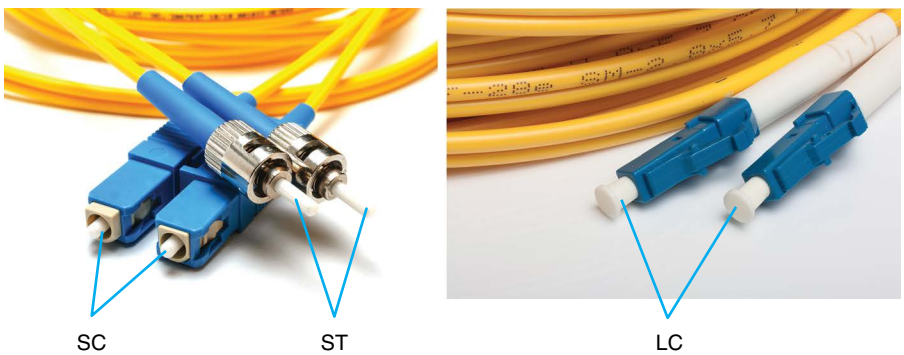


FIGURE 2.40 Fiber-optic connector types

The two major classifications of fiber are single-mode and multi-mode fiber. **Single-mode fiber** cable has only one light beam sent down the cable. **Multi-mode fiber** allows multiple light signals to be sent along the same cable. Table 2.7 describes the characteristics of the two types. (Note that fiber's maximum speeds keep increasing as technology keeps changing.)

TABLE 2.7 Fiber cable speed and transmission characteristics

Type	Characteristic
Single-mode	Classified by the size of the fiber core and the cladding. Common sizes include 8/125 to 10/125 microns, where the first number represents the size of the core, and the second number is the size of the cladding. Single-mode cable allows for distances more than 50 miles (80 km) at speeds more than 100 Gb/s.
Multi-mode	Sizes include 50/125 and 62.5/125 microns. Can support distances more than 1 mile (2 km) and speeds up to 10 Gb/s. ST connectors are used more with multi-mode fiber than with single-mode.

TECH TIP

Choosing the correct fiber type

Multi-mode fiber is less expensive and more commonly used than single-mode fiber and is good for shorter-distance applications; however, single-mode fiber can easily transmit a signal 40 times farther than multi-mode and supports the highest bandwidth.

Integrated Motherboard Ports

An integrated motherboard provides expandability because ports are built in and do not require separate adapters. If a motherboard includes USB, network, sound, keyboard, mouse, and video ports, there is more space available for other adapters. The number of available expansion slots in a system depends on the motherboard manufacturer. Figure 2.41 shows integrated motherboard ports including ports to attach two Wi-Fi 6 wireless antennas.

FIGURE 2.41 Integrated motherboard ports

Ports built into a motherboard are faster than those on an expansion board. All adapters in expansion slots run more slowly than the motherboard components. Computers with integrated ports on the motherboard are easier to set up because you do not have to install an adapter or configure the ports. Normally, systems with integrated motherboard ports are easier to troubleshoot because the components are on one board. The drawback is that when one port goes bad, you have to add an adapter that has the same type of port as the one that went bad. Furthermore, ports on an adapter might be of higher quality or might have more capabilities than integrated ports. See Figure 2.42.

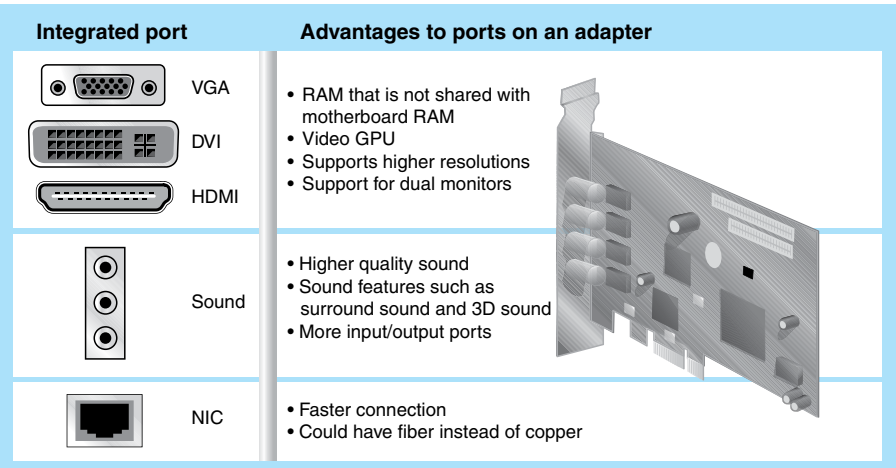


FIGURE 2.42 Advantages of adapters

Getting to Know Ports

Being able to identify ports quickly and accurately is a critical skill in computer repair. Table 2.8 lists the most common computer ports.

TABLE 2.8 Common ports

Port	Usage	Port color code	Common connector
PS/2 mouse	Mouse	Green	6-pin mini-DIN
PS/2 keyboard	Keyboard	Purple	6-pin mini-DIN
VGA	Video for an analog monitor	Blue	3-row 15-pin female D-shell or mini-VGA port
DVI	Video for a DVI digital or analog monitor	White	3-row 18- or 24-pin female DVI, mini-DVI, or micro-DVI
DVI-D	Video for a DVI digital monitor	White	3-row 18- or 24-pin female DVI, mini-DVI, or micro-DVI
DVI-A	Video for a DVI analog monitor	White	3-row 18- or 24-pin female DVI, mini-DVI, or micro-DVI
HDMI	Digital audio and video monitor	N/A	19- or 29-pin HDMI, mini-HDMI, or micro-HDMI
DisplayPort	Digital audio and video monitor	N/A	20-pin DisplayPort or mini-DisplayPort
USB	Multipurpose port for data, video, audio, and power	Black, blue, teal, or red	USB Type-A, Type-B, Type-C, mini-USB, micro-USB
Thunderbolt	Multipurpose port that can carry data, video, audio, and power	N/A	20-pin DisplayPort, mini-DisplayPort, or USB Type-C connector
Lightning	Multipurpose port for Apple devices that can carry data and power	N/A	8-pin connector
Audio	Analog audio input	Light pink	1/8 inch (3.5 mm) jack
Audio	Analog line level audio input	Light blue	1/8 inch (3.5 mm) jack
Audio	Analog line level audio output from main stereo signal	Lime green	1/8 inch (3.5 mm) jack
Audio	Analog line level audio for right-to-left speaker	Brown	1/8 inch (3.5 mm) jack
S/PDIF	Audio input/output	Orange	RCA jack (coax) or TOSLINK (fiber)
RJ45	UTP Ethernet network	N/A	8-conductor
RJ11	Internal/external modem or phone	N/A	4-conductor
DB9	RS232 serial port found on older computers and some networking equipment	N/A	9-pin port
eSATA	External storage devices	N/A	7-pin non-powered port
eSATAp	External devices	N/A	Combination eSATA/USB port

Wireless Connectivity for Input Devices

Many input devices, such as keyboards, mice, game pads, touchpads, and headphones, have wireless connectivity. Technologies used to connect without a cord include infrared, radio, Bluetooth, and near field communication (NFC). Many computing devices, especially smartphones and other mobile devices, have cordless connectivity integrated into the device; otherwise, a transceiver is connected to a USB port to allow connectivity to the computing device. Figure 2.43 shows a wireless presenter used with a computing device and a projector.

FIGURE 2.43 Wireless presenter

Table 2.9 summarizes the various wireless technologies used with input and output devices.

TABLE 2.9 Wireless input/output technologies

Technology	Description
Infrared (**IR**)	Used for very short distances. Cheaper than other technologies.
Radio	Works in the 27 or 900 MHz or 2.4, 5, 6, or 60 GHz radio frequency ranges. Longer distances are supported than with infrared.
Bluetooth	Includes 128-bit security and works in the 2.4 GHz range. There are four classes of devices, with ranges up to 1.6 feet (0.5 m), 3 feet (1 m), 33 feet (10 m), and 328 feet (100 m). Note that Bluetooth 5 supports a connection between two devices up to 800 feet (242 meters) away. Up to eight devices can be connected in a central/peripheral relationship, with only one device being the central.
Near field communication (**NFC**)	Used to print from a phone or a camera or to transfer data between two smartphones that are positioned very close to one another (less than 6 inches [15.24 cm]). Also used in payment systems. Works in the 13.56 MHz range at transfer speeds up to 424 kb/s.

SOFT SKILLS: USING APPROPRIATE TITLES

The internet and mobile devices have brought new methods of communication. In today's social media world, communication tends to be more casual, with people using colloquialisms, slang, and other language habits that aren't necessarily professional. In addition, some people regularly use acronyms, such as HAGD, LOL, BTW, NRN, TYVM, and YMMD, to communicate in emails, notes, text messages, and memos.

Many places of business are returning to fundamental principles of customer service, and they expect IT professionals to adopt professional communication methods. People expect the IT department to use more professional communication skills, which is why there is greater emphasis on improved soft skills during the hiring process. For example, IT personnel are expected to use appropriate titles and designations, such as Dr., Mr., Professor, and Ms., when talking to non-IT personnel, including external vendors. In the work environment, you should use a person's title, sir, or ma'am until the person you are addressing tells you otherwise. Figure 2.44 shows a couple of examples.

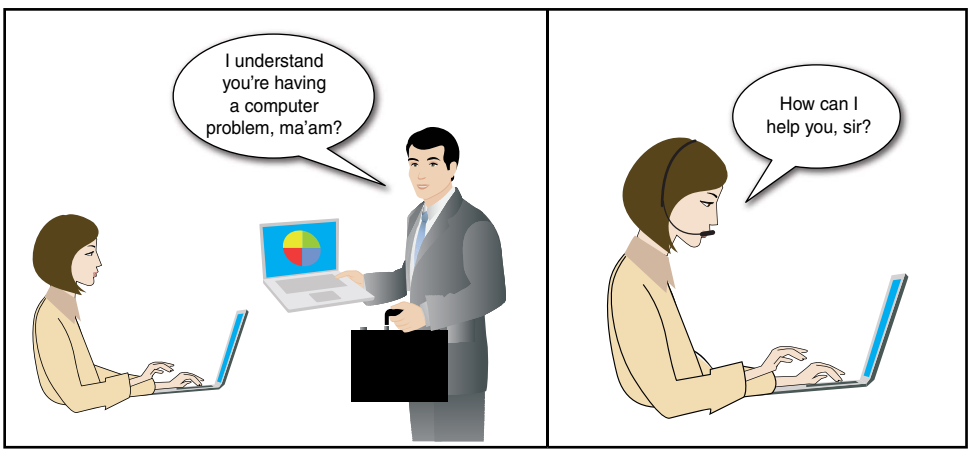


FIGURE 2.44 At work, use appropriate salutations

Chapter Summary

- A technician must be able to identify a variety of ports, including mouse and keyboard PS/2, VGA, DVI, HDMI, DisplayPort, Thunderbolt, Lightning, USB, RJ45, RJ11, 3.5 mm sound jack, TOSLINK, RCA, DB9, eSATA, and eSATAp ports.
- USB is the most popular method for adding devices to desktops, laptops, and tablets.
- USB provides power: 10W, 18W, 36W, 60W, and 100W. All USB4 ports support charging of USB devices.
- Add additional USB ports by connecting a hub that can be self-powered or bus powered. Up to five hubs can be daisy-chained to one port.
- Connect an internal USB cable from the motherboard connector to a metal plate that mounts in an empty expansion slot for more USB ports.
- Adapters are available to convert between different types of display ports, such as DVI and VGA or DVI and HDMI.
- Converters are available for USB ports, such as **USB-to-Ethernet**, which you might need if the Ethernet port goes bad on a computer.
- Audio ports can be analog or digital. S/PDIF ports are digital. There are two types of S/PDIF ports: TOSLINK and fiber.

- Ethernet ports have RJ45 connectors. RJ11 ports are found on modems and devices used to connect to the internet.
- DB9 ports can be found on modems, single-board computers, and networking equipment.
- An Ethernet port usually has a Cat 5e, 6, or 6a cable attached. Ethernet cables can be unshielded twisted pair or, if additional shielding is needed, shielded twisted pair. Plenum cabling is made of fire-retardant materials. A cheaper type of cable is PVC. Ethernet cables adhere to the T568A or T568B standard.
- Fiber cabling carries data over longer distances, and coaxial (coax) cabling is used for video networks.
- Input devices can connect to a computer by using four wireless technologies: IR, radio, Bluetooth, or NFC.
- When speaking with others, use appropriate professional titles when appropriate.

A+ CERTIFICATION EXAM TIPS

- ✓ Be able to identify the following connectors: RJ11, RJ45, BNC, F-type, ST, LC, SC, USB 2.0, USB 3.0, microUSB, miniUSB, USB-C, DB9, and Lightning. (On 3×5 cards, write the names of ports you have a hard time remembering. Put a picture of the port on one side and the name of the port on the other. Also include the type of connector each type of cable attaches to, such as RJ45 for a network cable. Practice until you know them all.)
- ✓ Be able to recognize a punchdown block and explain where you would see one.
- ✓ Be able to describe the following network cables, including features of each one: Ethernet (Cat 5, Cat 5e, Cat 6, Cat 6a, plenum, shielded twisted pair, unshielded twisted pair, and T568A/B standard cables), fiber, and coaxial. Know that direct burial STP cable is used between buildings without having to be inside piping or a special conduit. (Make a chart of key characteristics for each of these types of cable. Have someone quiz you on them.)
- ✓ Be able to explain the following video cables, features, and their purposes: VGA, HDMI, DisplayPort, DVI, and USB-C. (Do a web search of images for video ports and see if you can recognize these ports.)
- ✓ Be able to explain the features and purposes of the following cables: serial, Thunderbolt, USB 2.0, and USB 3.0. (Make a chart for each of these cables and characteristics of each.)
- ✓ The following communication and professionalism skills are part of the 220-1202 exam: Be culturally sensitive and use appropriate professional titles when applicable.

Key Terms

568A/B, analog signal, Bluetooth, BNC connector, Cat 5, Cat 5e, Cat 6, Cat 6a, charging USB port, coaxial, copper cabling, DB9, digital signal, direct burial cable, DisplayPort, DVI port, DVI-to-HDMI adapter, eSATA, eSATA cable, eSATAp port, Ethernet port, F-type, fiber cable, HDMI, header, IR, keyboard port, Lightning port, Lucent connector (LC), microUSB, mini-DIN, miniUSB, modem, mouse port, multimode fiber, network port, NFC, NIC, optical cable, PD, plenum cable, port, PS/2 port, punchdown block, punchdown tool, PVC, radio, RJ11, RJ45, S/PDIF, S-Video port, serial cable, shielded twisted pair (STP), single-mode fiber, sleep-and-charge USB port, sound card, straight tip (ST) connector, subscriber connector (SC), T568A, T568B, Thunderbolt port, unshielded twisted pair (UTP), USB, USB 2.0, USB 3.0, USB-C, USB-PD, USB-to-Ethernet converter, USB Type-A, USB Type-B, USB Type-C, VGA port

Review Questions

1. Match each port to the correct description.

___ DVI	a. Ethernet
___ VGA	b. TOSLINK
___ Thunderbolt	c. Up to 127 devices
___ USB	d. Daisy chain up to 6 devices
___ NIC	e. Older monitor
___ S/PDIF	f. Digital signals to monitor

2. Which connectors are used with fiber-optic cabling? (Select all that apply.)

   [BNC | DVI | ST | Lightning | LC | Thunderbolt | UTP]

3. What is a visual indication that a port is USB version 3.0?

   _____

4. Which port uses an RJ45 connector?

   [modem | Ethernet | Lightning | S/PDIF]

5. What feature does an eSATAp port have that makes it different from an eSATA port?

   _____

6. When considering VGA, HDMI, DVI, and DisplayPort, which video port can output both digital audio and video signals and is the most technologically advanced?

   [DisplayPort | DVI | HDMI | VGA]

7. What is the most common DVI port?

   [DVI-A | DVI-D | DVI-C | DVI-I]

8. Which has the faster transfer time, a USB 3.0 or 1,000 Mb/s Ethernet port?

   [USB 3.0 | 1,000 Mb/s Ethernet]

   _____

9. What is the maximum cable length for an Ethernet UTP cable?

   [100 meters | 150 meters | 200 meters | 1000 meters]

10. Which color of sound port would be used to attach a speaker?
    [black | green | pink | white]

11. List two titles that might be used in the workplace that are not sir or ma'am.

    _____

12. You see a port on a computer that you have never seen before. There are no markings. How can you determine the purpose of the port?

    _____

13. What type of port uses an RJ11 connector?

    [Ethernet | internet router | display | keyboard]

14. Which port is more commonly found on an Apple computer than any other type of PC?

    [Ethernet | RJ45 | Thunderbolt | USB-C]

15. On which type of cable would you find an F-type connector?

    [VGA | Thunderbolt | Lightning | coaxial]

16. On which type of card would a DB9 connector be found?
    [serial | NIC | video | audio]

17. Which cable can carry video and audio signals and can be used to connect external storage devices?

    [Type-A | DVI-I | Thunderbolt | mini-DIN]

18. In which of the following situations would Bluetooth most likely be used?

    a. To connect to a corporate wireless network

    b. To connect a keyboard to a PC

    c. To connect a PC to a phone line

    d. To connect a flash drive to a camera

19. List one advantage of having an adapter rather than an integrated motherboard port.

    _____

20. What are two commonly used connectors on coaxial cable that are used in video distribution systems? (Choose two.)

    [RG-6 | RG-11 | RG-59 | RJ11 | RJ45]

Exercises

Exercise 2.1 Identifying Computer Ports

Objective: To identify various computer ports correctly

Procedure: Identify each computer port in Figure 2.45.

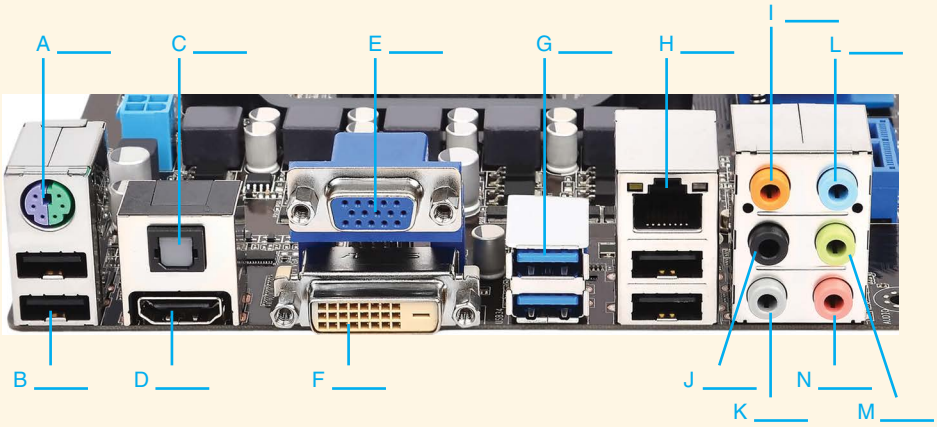


FIGURE 2.45 Identify motherboard ports

A. _____	**H.** _____
B. _____	**I.** _____
C. _____	**J.** _____
D. _____	**K.** _____
E. _____	**L.** _____
F. _____	**M.** _____
G. _____	**N.** _____

Exercise 2.2 Identifying More Computer Ports

Objective: To identify various computer ports using graphics

Procedure: Identify each computer port in Figure 2.46.

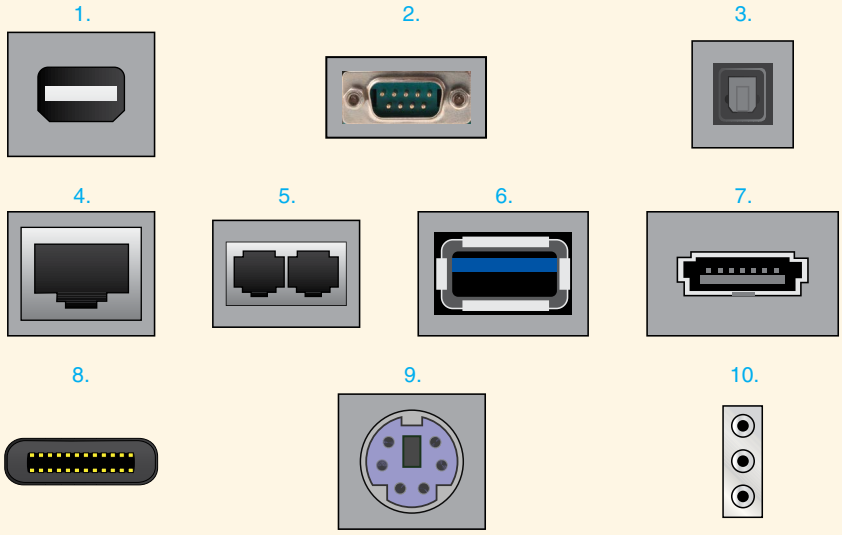


FIGURE 2.46 Identify computer ports

1. _____
2. _____
3. _____
4. _____
5. _____
6. _____
7. _____
8. _____
9. _____
10. _____

Exercise 2.3 Identifying Display Ports

Objective: To identify various display ports correctly

Procedure: Identify each display port in Figure 2.47.

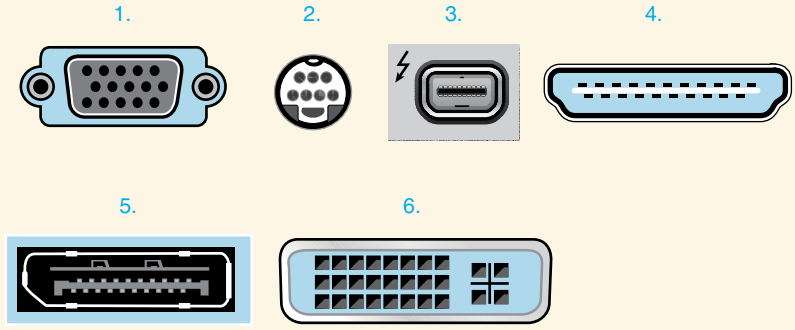


FIGURE 2.47 Identify video ports

1. _____
2. _____
3. _____
4. _____
5. _____
6. _____

Exercise 2.4 Identifying USB Ports

Objective: To identify various USB ports correctly

Procedure: Identify each USB port in Figure 2.48.

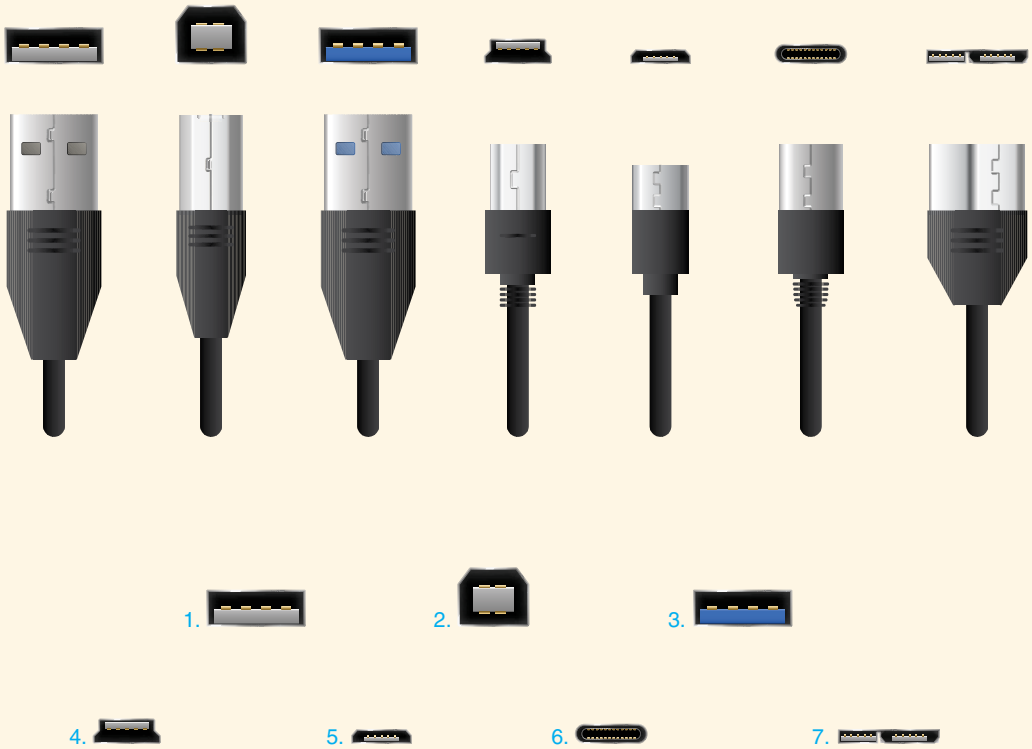


FIGURE 2.48 Identify USB ports

1. _____
2. _____
3. _____
4. _____
5. _____
6. _____
7. _____

Exercise 2.5 Identifying Cables

Objective: To identify various cables

Procedure: Identify each cable in Figure 2.49.

FIGURE 2.49 Identify cables

1. _____
2. _____
3. _____
4. _____
5. _____
6. _____
7. _____
8. _____
9. _____
10. _____

Activities

Internet Discovery

Objective: To obtain specific information from the internet regarding a computer or its associated parts

Parts: Computer with internet access

Procedure: Complete the following procedure and answer the accompanying questions.

Questions: For Questions 1–4: Obtain technical information about a particular computer (maybe your own computer or a model number given by the instructor). Answer the following questions based on the information. You may need to obtain more documents, or you may need to select a different computer model to answer questions. Please use only one computer model.

1. Which ports are available on the front of the computer?

_____

2. Which ports are available on the back of the computer?

_____

3. How many drive bays are available to install devices such as hard drives, optical drives, tape drives, and so on?

_____

4. Are the photos in the documentation clear enough to differentiate between the different ports? If not, explain what is wrong.

_____

5. Create a list of 10 acronyms along with their meanings. These acronyms should be suitable for texting a family member but inappropriate for communication (even texting) with an employee from a non-IT department who is not a close friend but a professional acquaintance. Also, provide the URL(s) where this information is found.

_____

6. Using the internet, list one fact about NFC that was not in the chapter and provide the URL for the site where you found this information.

_____

Soft Skills

Objective: To enhance and fine-tune a future technician's ability to listen, communicate in both written and oral forms, and support people who use computers in a professional manner

Procedure:

1. In teams of two, one student writes a professional note that contains internet acronyms that are commonly used for texting. The other student tries to guess what the acronyms mean. Together, rewrite the note so it is more professional.
2. Draft an email to a pretend computer customer that you just met for the first time yesterday. You did not have the part needed to repair the computer, but now the part has come in. Be sure you use professionalism in your email.

Critical Thinking Skills

Objective: To analyze and evaluate information as well as apply learned information to new or different situations

Procedure:

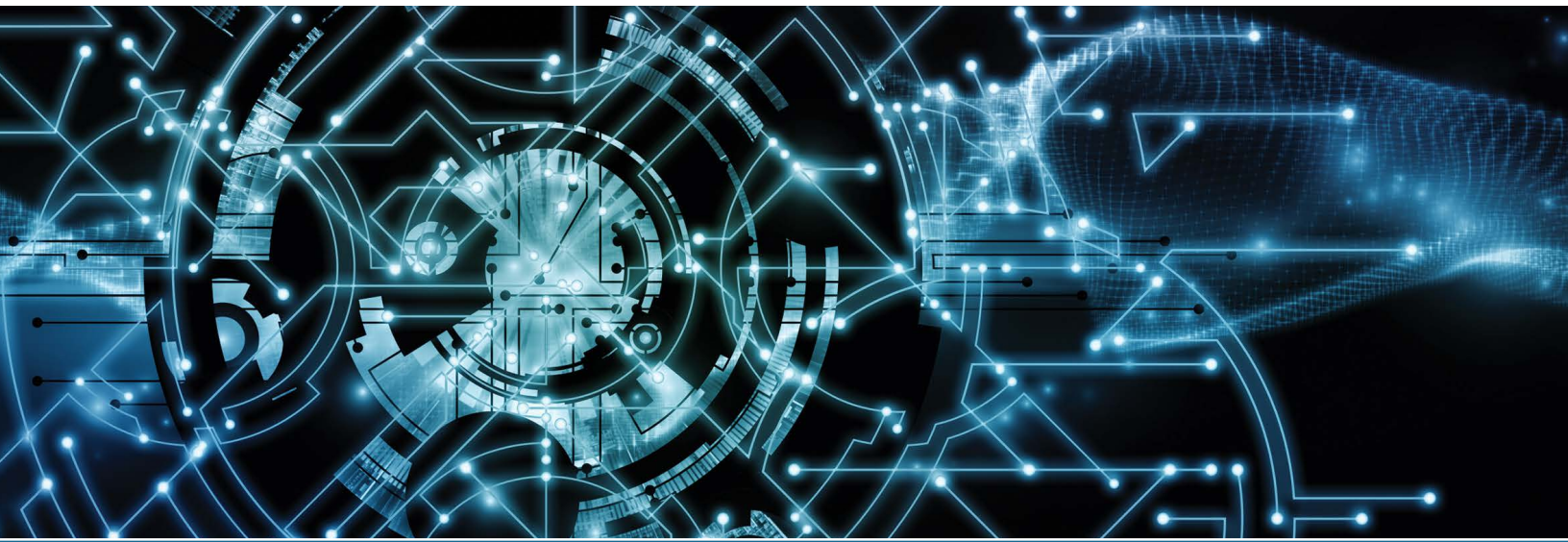
1. Find an advertisement for a computer in a local computer flyer, in a newspaper, in a magazine, in a book, or on the internet. List which ports you know in one column and the ports you do not know in the other column. Select one port you do not know and research that component. Write the new information and share it with at least one other person.
2. Work in groups of three. As a group, do you think future computers will only have wireless connections or continue to have both wired and wireless connectivity? Why do you think this? What might be some hindrances to future computers having only wireless connections?
3. Provide five tips that might help someone identify the different computer ports. If possible, each person in the class should state a tip without duplicating someone else's tip.

_____

_____

This page intentionally left blank

3 On the Motherboard



In this chapter you will learn:

- How to recognize and identify important motherboard parts
- The basics of how a processor works
- Issues to consider when upgrading or replacing a motherboard or processor
- Information regarding GPUs
- How to add cards to computers
- The differences between PCI and PCIe adapters and slots
- Motherboard technologies such as multicore configurations, NPU, cooling, and cache memory
- Motherboard form factors and security options
- Symptoms of motherboard and CPU problems
- The benefits of active listening

CompTIA Exam Objectives:

- ✓ 1201-3.5 Given a scenario, install and configure motherboards, central processing units (CPUs), and add-on cards.
- ✓ 1201-5.1 Given a scenario, troubleshoot motherboards, RAM, CPU, and power.
- ✓ 1202-4.7 Given a scenario, use proper communication techniques and professionalism.

Introduction to the Motherboard

The motherboard is a crucial component found in most electronic devices, including computers, and is important to any type of device. Figure 3.1 shows some of the key motherboard components we will be covering.

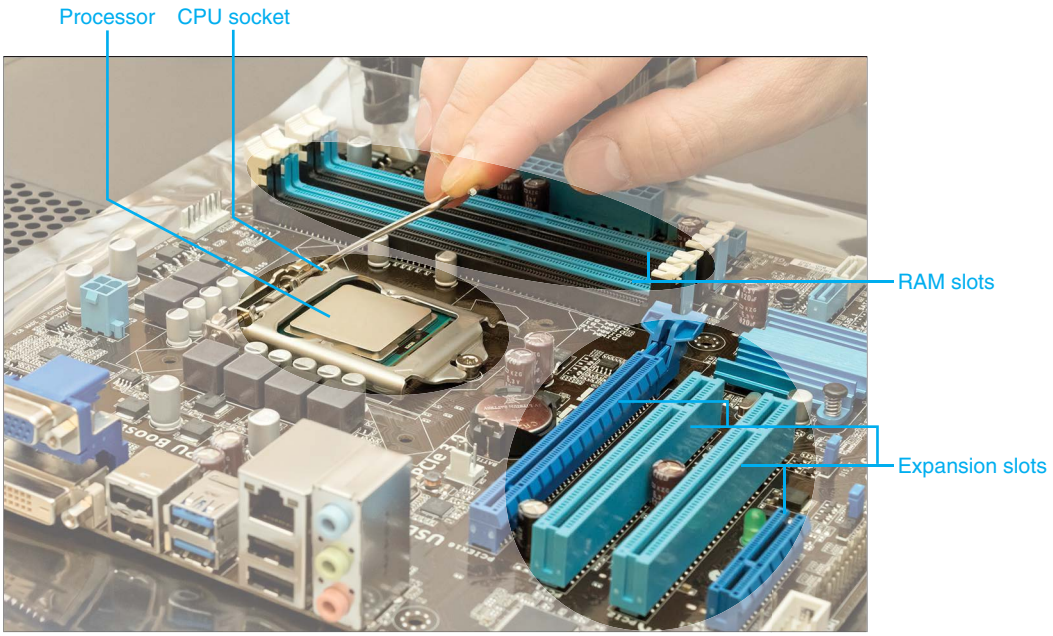


FIGURE 3.1 Key motherboard components

Processor Overview

At the heart of every computer is the **processor**, which determines, to a great extent, the performance of the computer. The processor is also called the central processing unit (**CPU**), or microprocessor. The processor executes instructions, performs calculations, and coordinates input/output operations. Each motherboard has chips that work with the CPU and that are designed to exact specifications. Whether these other components can keep up with the processor depends on the individual component's specifications. The major processor manufacturers today are Intel, VIA, Samsung, NVIDIA, Apple Inc., Qualcomm, and AMD (Advanced Micro Devices, Inc.). **Intel** and **AMD** are the predominant manufacturers of desktop and laptop processors. A term you might hear related to Intel and AMD CPUs is x86-64. The **x86** relates back to the Intel 8086 processor, and the 64, or **x64**, is an updated 64-bit version. Intel and AMD each have their own patented CPU architecture, called Intel 64 and AMD64.

ARM processors are used on mobile devices like smartphones, tablets, and laptops. ARM used to be an acronym for Acorn RISC (reduced instruction set computing) Machine and then Advanced RISC Machines, but today it is just an architecture used in processors and microcontrollers. ARM processors can be 32- or 64-bit processors and are frequently used on mobile devices like smartphones, tablets, digital cameras, and laptops, but they can also be used for desktops and servers. ARM processors take less power, produce less heat, and cost less than AMD or Intel processors.

A similar device is a system on a chip (**SoC**), which has everything to run the computer on a single chip, including the CPU, RAM, graphics processor, ports, etc. SoCs are used in desktops and mobile devices like tablets, smartphones, and laptops.

A motherboard accepts the processors of one or more specific manufacturers; for example, a motherboard that accepts an Intel processor will not support an AMD processor. Figure 3.2 shows the front and back of a processor.

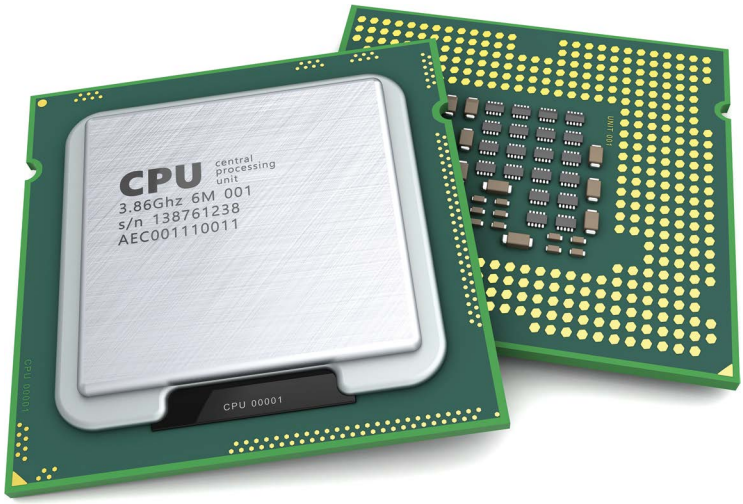


FIGURE 3.2 Intel processor

Processor Basics

Processors come in a variety of speeds, measured in **gigahertz** (GHz). Hertz is a measurement of cycles per second. One hertz, written 1 Hz, equals 1 cycle per second. One gigahertz, or 1 GHz, is 1 billion cycles per second. Today's processors can run at speeds near 6 GHz.

Buses

Processors operate on 1s and 0s. The 1s and 0s must travel from one place to another inside the processor, as well as outside to other chips. To move the 1s and 0s around, electronic lines called a **bus** are used. The electronic lines inside the CPU are known as the internal data bus.

For a CPU to communicate with devices in the outside world, such as a printer, the 1s and 0s travel on the external data bus. An external data bus is also known as an external data path. You can see the external data lines by looking between the expansion slots on the motherboard. Today's processors have 64- and 128-bit external data paths. Figure 3.3 shows internal and external data buses.

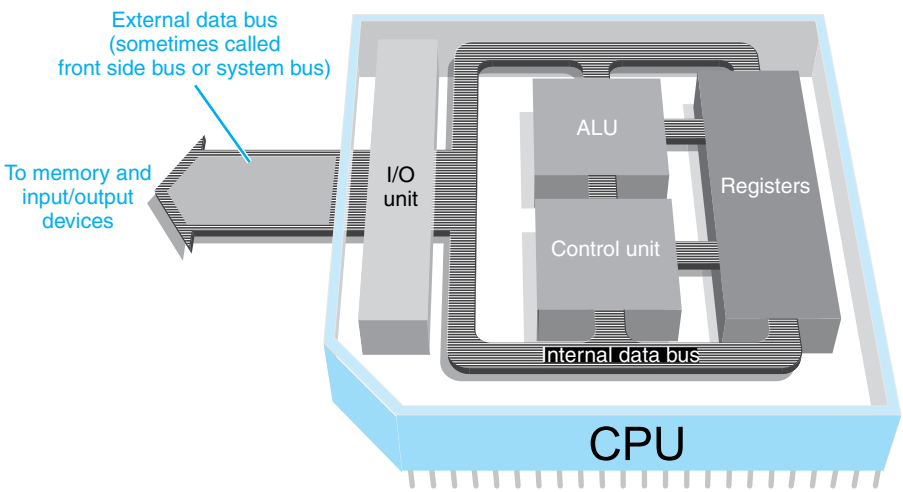


FIGURE 3.3 Internal and external data buses

Processing Data

To understand how a computer processes data, consider a letter typed on a computer that starts out *DEAR MOM*. To the computer, each letter of the alphabet is a different combination of eight 1s and 0s. For example, the letter *D* is 01000100, and the letter *E* is 01000101. Figure 3.4 demonstrates that the size of the bus greatly increases performance on a computer much the way increasing the number of lanes of a highway decreases congestion.

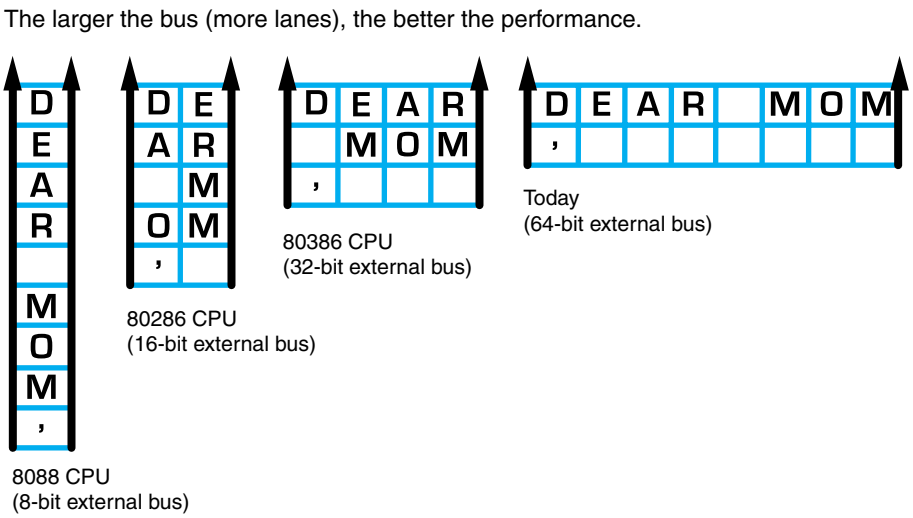


FIGURE 3.4 Bus performance

Speeding Up Processor Operations Overview

You can determine the speed of a processor by looking at the model number on the chip, but processors frequently have a cooling product attached to them, which makes it difficult to see the writing on the chip. A processor usually operates below its maximum speed to save power or prevent overheating. Also, a processor does not always function at its maximum potential for a lot of reasons, including coding used within an application, the user switching from application to application, inadequate bus width, or the amount of RAM installed. A processor can also operate beyond its rated specifications to handle periods of increased workload.

TECH TIP

Locating processor speed

An easy way to check the processor speed with Windows is to go to Windows File Explorer and right-click *This PC* and select *Properties*. On a Mac, use the Activity Monitor tool.

We've explored how increased bus width can enhance performance, but several other technologies also contribute to making processors more efficient. We will begin by defining key terms related to this topic and associate those terms to relevant concepts and technologies. Table 3.1 lists some terms related to speed.

TABLE 3.1 Motherboard speed terms

Term	Explanation
Clock or **clock speed**	The speed of the processor's internal clock, measured in gigahertz.
Front side bus (**FSB**)	The speed (commonly called motherboard speed) between the CPU and some of the motherboard components, sometimes listed in megatransfers per second, or MT/s. With MT/s, the speed of the FSB is considered, and so is the number of processor transfers that occur each clock cycle. A 266 MHz FSB that can do four transfers per second could be listed as 1,064 MT/s.
Back side bus	The speed between the CPU and the L2 cache is located outside the main CPU but on the same chip.
PCI bus speed	The speed used to deliver data on the PCI bus. Common speeds for the PCI bus are 33 and 66 MHz, allowing bandwidths up to 533 MB/s.
PCIe bus speed	The speed used to deliver data on the PCIe bus. Common data transfer rates follow: > PCIe 3.x: 8 GT/s > PCIe 4.x: 16 GT/s > PCIe 5.x: 32 GT/s > PCIe 6.x: 64 GT/s > PCIe 7.x: 128GT/s To find the total throughput, multiply the transfer rate by the number of lanes. For example, with a PCIe 5.x transfer rate of 32.0 GT/s (gigatransfers per second), the throughput on a 1x card is 3.2 GB/s and on a 16x card is 512 GB/s.
CPU speed	The speed at which the CPU operates; it can be changed on some motherboards.
CPU throttling	Reducing the clock frequency to slow the CPU in order to reduce power consumption and heat. This is especially useful in laptops and mobile devices.

Cache

An important concept related to processor speed is keeping data flowing into the processor. The data or instruction the CPU needs to process is usually found in one of four places: cache memory, motherboard memory (main memory), a solid-state drive (SSD, which is also memory), or the hard drive.

Cache memory is a very fast type of memory that is designed to increase the speed and efficiency of processor operations. Cache provides the fastest access. If the information is not in cache memory, the processor looks for the data in motherboard RAM. If the information is not there, it is retrieved from the hard drive and placed into the motherboard memory or the cache. Hard drive access is the slowest of the three. Table 3.2 lists the types of cache. Figure 3.5 shows the hierarchy of where the CPU looks for data.

TABLE 3.2 Types of cache

Type	Explanation
L1 cache	Cache memory integrated into the processor; the fastest type
L2 cache	Cache in the processor packaging but that is not part of the CPU; also called on-die cache
L3 cache	Usually found in more powerful processors and can be located in the CPU housing (on-die) or on the motherboard

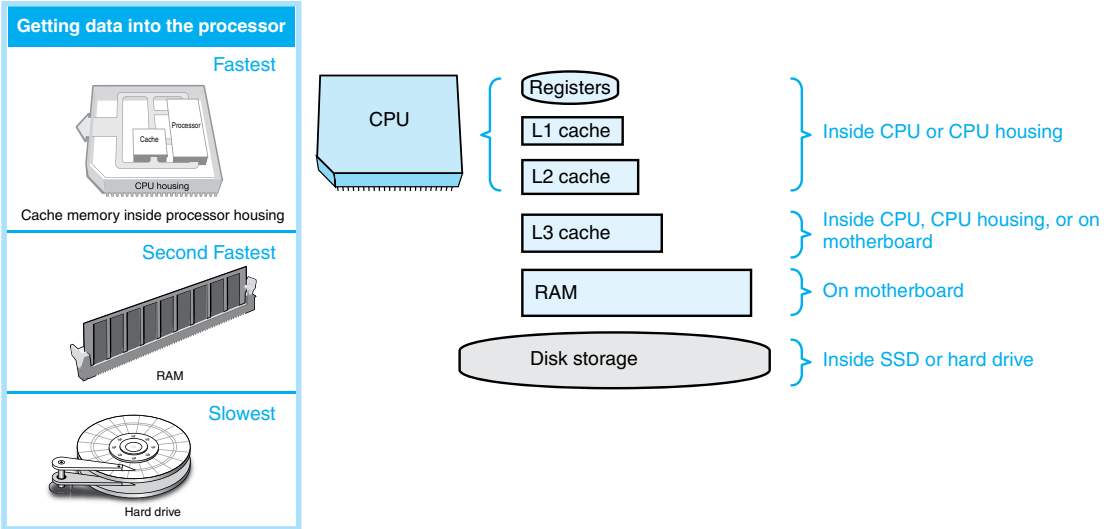


FIGURE 3.5 CPU data sources and data access hierarchy

Connecting to the Processor

In older computer systems, a performance bottleneck occurred because the CPU used a single bus to communicate with multiple components. This shared bus was used for accessing L2 cache, RAM, and other motherboard components, which limited the speed of data transfer between these elements and the CPU. The solution to this problem is to use two buses: a back side bus and a front side bus. The back side bus connects the CPU to the L2 cache. The front side bus (see Figure 3.6) connects the CPU to the motherboard components. The front side bus is considered the speed of the motherboard.

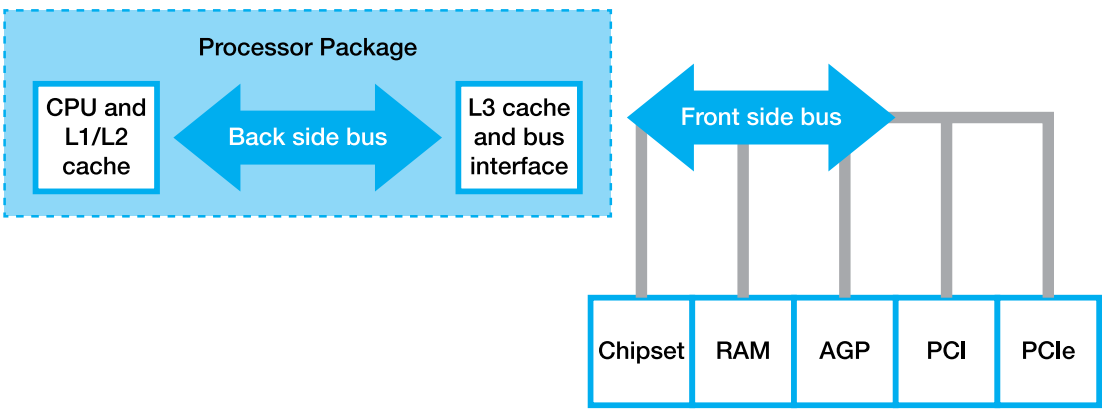


FIGURE 3.6 Front side bus and back side bus

Many people think that the higher the CPU speed, the faster the computer. This is seldom true. Several factors contribute to speed of a computer. One factor is bus speed. Bus speed describes how fast the CPU can communicate with motherboard components, such as memory, the chipset, or the PCI/PCIe bus. Another important factor is the chipset, which determines the maximum amount of memory, the type of memory chips, the number and type of USB ports, etc. The chipset motherboard component looks like a processor and may have a heat sink on top of it.

Intel and AMD have technologies to replace the front side bus in some parts. AMD's solution is to have the processor cores connect directly to memory, to the other motherboard components such as the expansion slots, and to other processor cores by using a high-speed bus called **HyperTransport**. AMD is upgrading HyperTransport to Infinity Fabric. Intel has Quick Path

Interconnect (QPI), Ultra Path Interconnect (UPI), Serial Peripheral Interface (SPI), and Direct Media Interface (DMI), which are point-to-point connections between the processor and one or more motherboard components.

Multicore Processors

A single-core processor is just one processor. Both Intel and AMD provide **multicore** processors, which means more than one CPU in the same housing (see Figure 3.7). Each core can execute programs or threads. One Intel Core 9 CPU has up to 24 cores, and AMD's Ryzen Threadripper has 96 cores and 192 threads.

A **thread** is a small piece of an application process. Each thread can share resources, such as the processor or cache, with other threads. Hyperthreading allows a single processor to handle two separate sets of instructions simultaneously. A computer using hyperthreading shows more logical cores than physical cores. Figure 3.7 illustrates how multiple Intel processors connect. Figure 3.8 shows how each AMD CPU accesses RAM (through the memory controllers) with multicore machines. Notice the neural processing unit (**NPU**) box in Figure 3.8. This is part of the architecture when the computer can be used to do artificial intelligence (**AI**) tasks or calculations.

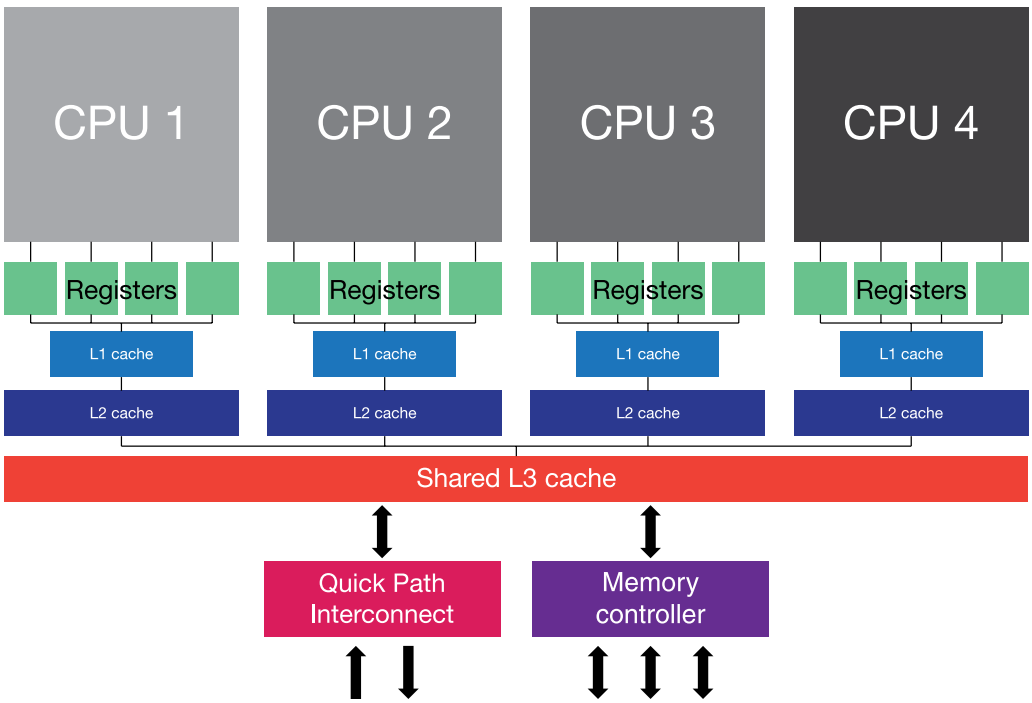


FIGURE 3.7 Intel multicore architecture

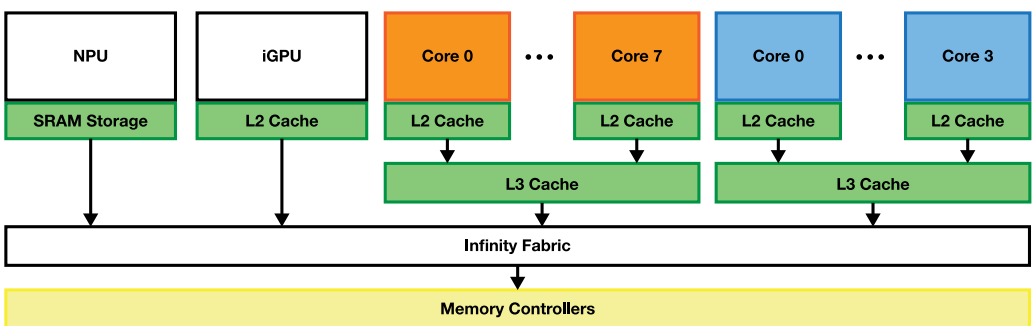


FIGURE 3.8 AMD multicore memory access

TECH TIP

How many cores and threads do you have?

Right-click on Windows taskbar > *Task Manager* > *Performance* tab > *CPU* > look for *Cores, Logical processors,* and *Threads*.

A logical processor can execute its own set of instructions, allowing multiple tasks to be handled simultaneously. All applications can take advantage of the multicore technology and the background processes that are associated with the operating system and applications. This potentially improves operations when multitasking or when running powerful applications that require many instructions to be executed, such as drawing applications and games.

TECH TIP

A+ core configurations

On the CompTIA A+ exam, a key term is **core configurations**. To understand core configurations, you need to know that (1) processors can have multiple cores and how to tell what they have, (2) each computer has a specific clock speed that affects the speed at which the computer runs, and (3) the number of cores for a particular system needs to be based on what the customer plans on doing with the computer.

Graphics Processing Unit (GPU)

Another bottleneck for computer performance is video. Computer users who want better video performance buy a separate video adapter that contains a dedicated GPU. Both Intel and AMD offer a CPU with an integrated graphics processing unit (**GPU**) on some of their processor models. An integrated GPU (**iGPU**), sometimes called an integrated graphics processor (IGP), eliminates the need for an external video card. It processes graphical data quickly, with reduced power consumption. Today's CPUs contain multicore processors, and GPUs contain hundreds of smaller core processors. GPUs can also be used for other purposes that are not directly related to graphics but that increase system performance. These GPUs are sometimes referred to as general-purpose GPUs (GPGPUs). Figure 3.9 shows how an IGP is within the same housing as the CPU cores.

AMD uses the term accelerated processing units (**APUs**) for its processors that have GPUs integrated with the CPUs. Intel uses the terms Intel HD Graphics and Intel Iris Graphics for its processors that have GPUs integrated with the CPUs.

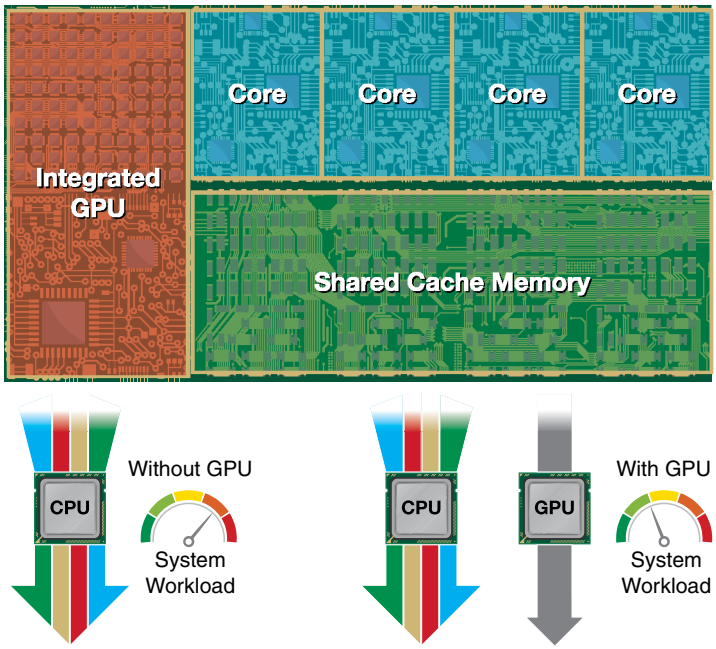


FIGURE 3.9 CPU vs. GPU

Introduction to Virtualization Support

One advantage of having multiple processor cores is that they allow both home and business computers to take advantage of virtual technology. **Virtualization** allows you to have one or more virtual machines (**VMs**) on the same computer. Virtualization software, such as VMware Workstation, Oracle VM VirtualBox, or Microsoft Hyper-V, enables one computer to act as if it were two or more computers. The computer can have two or more operating systems installed through the use of the virtualization software. Each operating system has no knowledge of the other operating system(s) on the computer (see Figure 3.10).

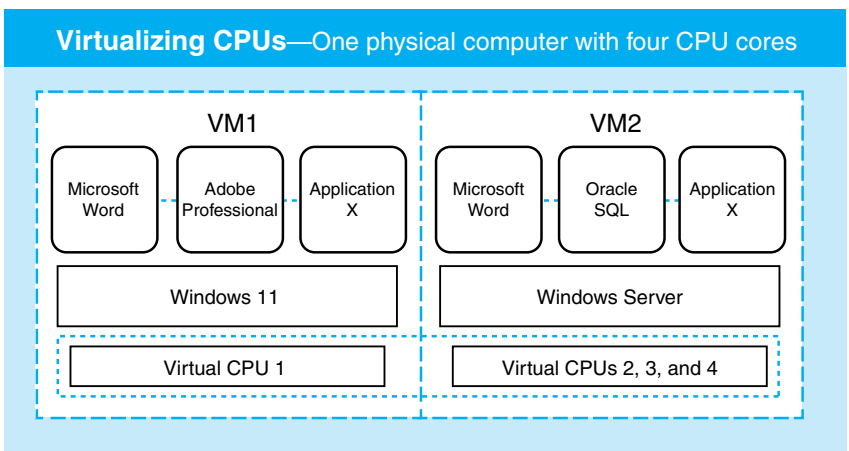


FIGURE 3.10 The concept of virtualization

Windows has Hyper-V, which allows an application to run in a virtual environment as if an older operating system were installed. Businesses often use virtualization so they can use legacy software on newer machines but keep it separate from the main operating system or another VM on the same computer. Reduced costs and physical space are benefits of virtualization. Home computer users can install multiple operating systems in separate VMs within the same physical box, and each VM is seen as a separate computer.

TECH TIP

A+ virtualization

To better prepare for the CompTIA A+ certification exam, you could install VMs running Windows and/or Linux.

Selecting a motherboard and processor is important when in a virtual environment. Refer to the virtualization software documentation to determine whether the CPU used is supported. Be sure to enable **virtualization support** in the firmware (covered in Chapter 4, "Introduction to Configuration"). Another issue regarding processors and virtualization is licensing. For virtualization software that must be purchased (that is, is not freeware), the software manufacturer may charge on a per-processor or per-socket license basis or on a per-core basis.

Intel Processors

Traditionally, Intel has rated its processors by GHz, and people have compared processors based on speed alone. Now Intel arranges its products by family numbers. Within a family of processors, you can compare attributes such as speed and the amount of cache memory and other technologies. Table 3.3 shows Intel's processor families. Figure 3.11 shows a close-up of a processor installed into a motherboard. Figure 3.12 shows how to decipher Intel processor models.

TABLE 3.3 Intel processor families

Processor family*	Comments
Xeon	CPU for servers and professional PCs that needs large amounts of ECC memory, larger cache, more cores, and multiple sockets.
Core Ultra *x*	Processor with 8 to 24 cores (at press time) in the Core 5, 7, and 9 families that allows better graphics and supports AI processing.
Core 9	Powerful multicore processor for gaming and intensive content creation as well as megatasking.
Core 7	Multicore processor with cache memory shared between cores and an on-board memory controller. Good for virtualization, graphic/multimedia design and creation, and gaming.
Core 5	Midrange dual- and quad-core processor. Used for video, photos, email, and internet access.
Core 3	Low-end desktop and mobile processor used for common tasks such as word processing and internet access.

*Intel is constantly upgrading processors. For more information, visit www.intel.com.

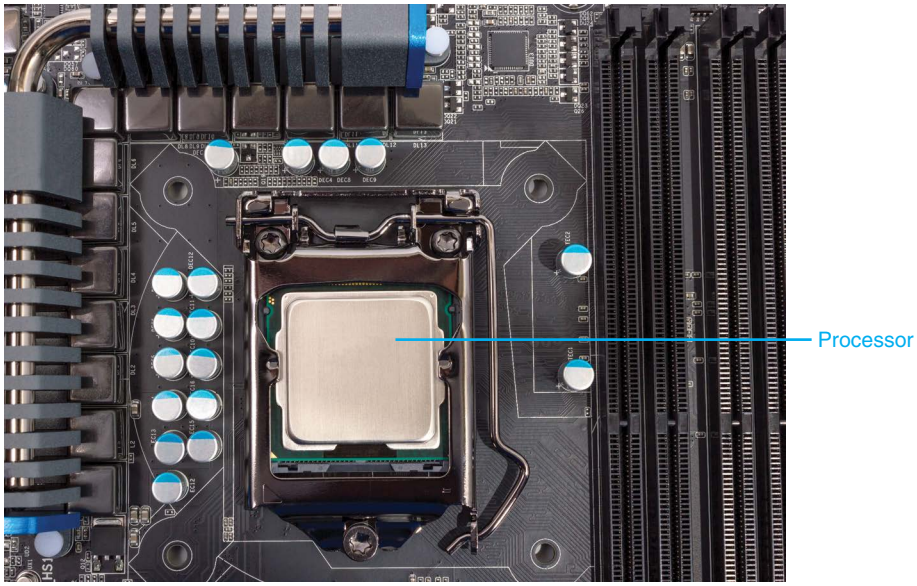


FIGURE 3.11 Installed processor

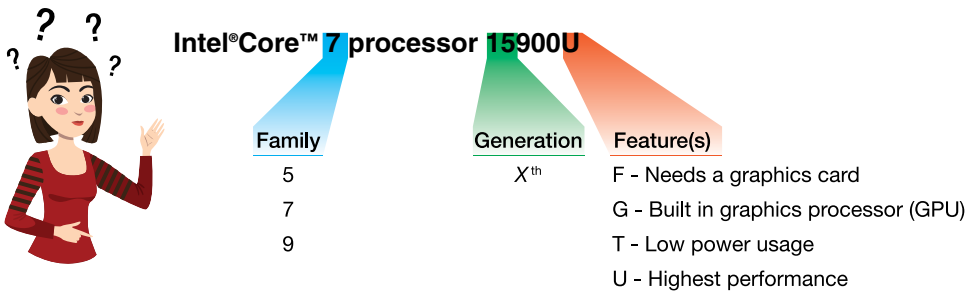


FIGURE 3.12 Deciphering Intel processor model numbers

AMD Processors

AMD is Intel's largest rival in computer processors. Table 3.4 lists the AMD processor families, and Figure 3.13 shows how to make sense of the AMD CPU model numbers.

TABLE 3.4 AMD processor families

Processor family	Comments
Ryzen AI	Up to 12 cores and 24 MB cache. Used for AI-based tasks.
Ryzen Threadripper	12 to 96 cores, 24 to 192 threads, and up to 384 MB cache. For extremely high-end desktop processor.
Ryzen 9	12 to 16 cores, up to 32 threads, and up to 64 MB cache.
Ryzen 7	8 cores, 16 threads, and 96 MB cache. For gaming, high-end content creation, and megatasking.
Ryzen 5	6 cores, 12 threads, and 16 MB cache. For workplace or home computing use.
Ryzen 3	4 cores, 8 threads, and 8 MB cache for standard computing use.

*AMD is constantly upgrading processors. For more information, visit www.amd.com.

Ryzen 7 3700X

Family	Generation	Performance Level	Feature(s)
3	1st	1-3	X - High performance
5	2nd	4-5	WX - High core count workstation
7	3rd	6-7	G - Desktop + IGP
9	4th	8	E - Low-power desktop
THREADRIPPER	5th	9	GE - Low-power desktop + IGP
			XT - Extreme

FIGURE 3.13 Deciphering AMD processor model numbers

CPU Sockets

A processor inserts into a **CPU socket** on the motherboard. There are different types of sockets, but each socket has a specific number of pins and accepts only specific CPUs. A motherboard that can take more than one CPU shows in the documentation/specifications as a **multisocket** motherboard. These are typically found in servers, which are powerful computers used in network environments. Figure 3.14 shows a desktop motherboard CPU socket.

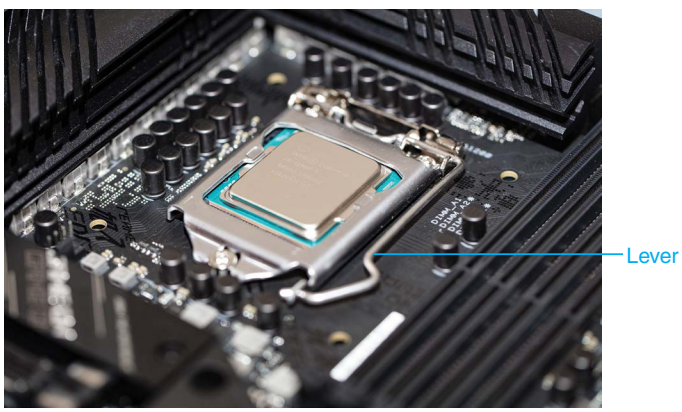


FIGURE 3.14 CPU socket

Processor sockets are also called zero insertion force sockets, or **ZIF sockets**, and they come in different sizes. The socket has a small lever to the side that, when lifted, brings the processor slightly up and out of the socket holes. When installing a processor, you align the CPU over the socket and press the lever down to bring the processor into the socket with equal force. In Figure 3.14, notice the lever beside the socket that is used to lift the metal cover.

TECH TIP

Buying the right CPU

If you buy a motherboard and processor separately, it is important to ensure that the motherboard CPU socket is the correct type for the processor:

> **Intel desktop sockets:** LGA 1151, 2066, 1200, 1700, and 1851

> **AMD sockets:** AM4, AM5, TR4, sTRX4, and sWRX8

Processor Cooling

Keeping a CPU cool is critical. Both Intel and AMD have technologies that reduce processor energy consumption (and heat) by turning off unused parts of the processor or slowing down the processor when it starts to overheat. But these measures alone are not enough. Today's systems use one or more of the methods listed in Table 3.5. Figure 3.15 shows a heat sink and a fan. The largest chip on the motherboard with a fan or a heat sink attached is easily recognized as the processor.

TABLE 3.5 Processor cooling methods

Method	Description
Heat sink	A heat sink is a block of metal (usually aluminum or copper), metal bars, or metal fins that attach to the top of the processor or other motherboard components. Heat from the processor is transferred to the heat sink and then redistributed to be pushed out the computer case.
Fan	Fans can be attached to the processor, beside the processor, and in the case.
Thermal paste or **thermal pad**	Thermal paste, compound, or grease can be applied to the top of a processor before a heat sink is attached. Some heat sinks and fans have thermal paste pre-applied. A thermal pad provides uniform heat dispersion and lies between the processor and the heat sink.
Liquid cooling	Liquid is circulated through the system, including through a heat sink that is mounted on the CPU. Heat from the processor is transferred to the cooler liquid. The now-hot liquid is transported to the back of the system, converted to heat, and released outside the case. CPU temperature remains constant, no matter the usage. Some systems require the liquid to be periodically refilled.
Phase-change cooling (vapor cooling)	This expensive option uses a technique similar to a refrigerator: A gas is converted to a liquid that is converted back to gas.

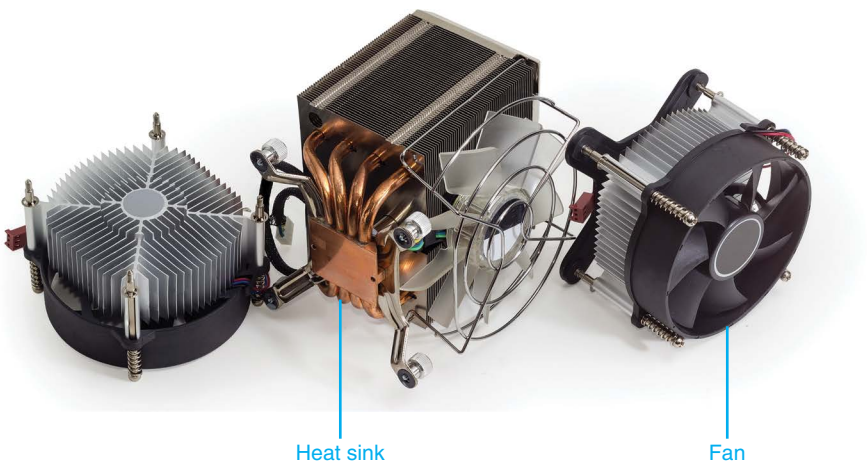


FIGURE 3.15 Heat sinks and fans

TECH TIP

Cooling the CPU

Do not apply power to a computer until the CPU and the heat sink, fan, and/or cooling unit are installed. Running the CPU without installing appropriate cooling mechanisms will cause the CPU to overheat, which will destroy or weaken it.

Additional motherboard components can also have heat sinks attached. They are normally the chipset and/or the I/O (input/output) controller chips. Figure 3.16 shows a motherboard with these cooling elements.

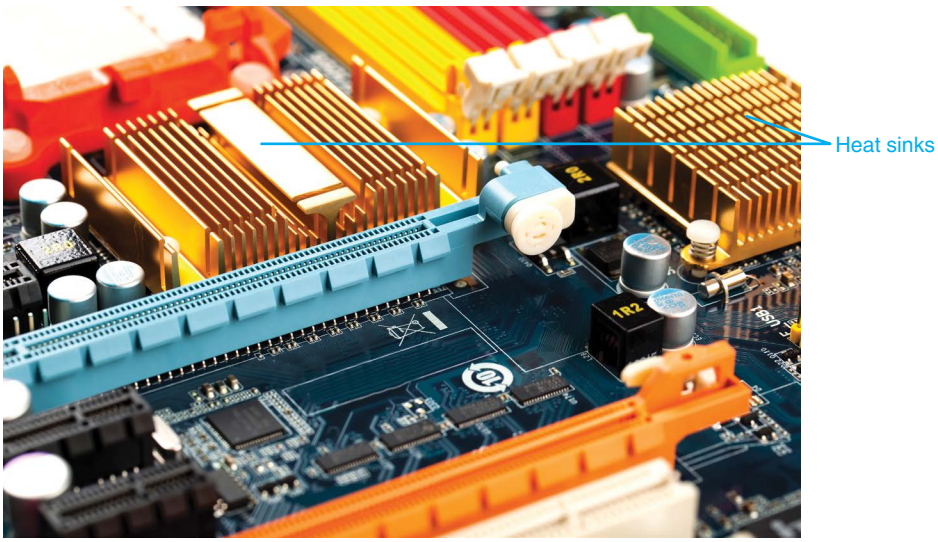


FIGURE 3.16 Motherboard heat sinks

TECH TIP

When thermal paste acts like glue

Over time, thermal paste can act like glue, making a processor hard to separate from a heat sink. You can use a thermal paste cleaner, acetone, or denatured alcohol to separate the two parts. Do not pry them apart!

Installing a Processor

Processors are sold with installation instructions. In addition, motherboard manuals (or other documentation) include the steps to upgrade or install the CPU. The following are the parts and the general steps for installing a processor:

Parts: Appropriate processor for the motherboard (refer to motherboard documentation)
Antistatic materials

Step 1. Ensure that power to the computer is off and the computer is unplugged.

Step 2. Place an antistatic wrist strap around your wrist and attach the other end to a ground or unpainted metal part of the computer. Alternatively, use an antistatic glove.

Step 3. If a retention lever is present, push the retention lever down and outward to release the CPU retention plate. Move the handle backward until the retention plate is fully open. Do not touch the CPU socket. *If a plastic cover is installed in the CPU socket, remove it.*

Step 4. Remove the processor from the packaging, taking care to hold it by the edges and never touch the bottom metal portion of the processor. Remember that a CPU fits only one way into the socket. Look at the processor and the socket before inserting the chip to ensure proper alignment. A socket and CPU normally have a triangle marking or dot to indicate pin 1, as shown in Figure 3.17. The processor also has notches on each side

that align with the socket. Insert the CPU into the socket by aligning it with the socket and lowering it until it is flush with the socket, as shown in Figure 3.18. (Do not force it and do not power on the computer until a thermal solution has been applied! See "Installing CPU Thermal Solutions," later in the chapter.)

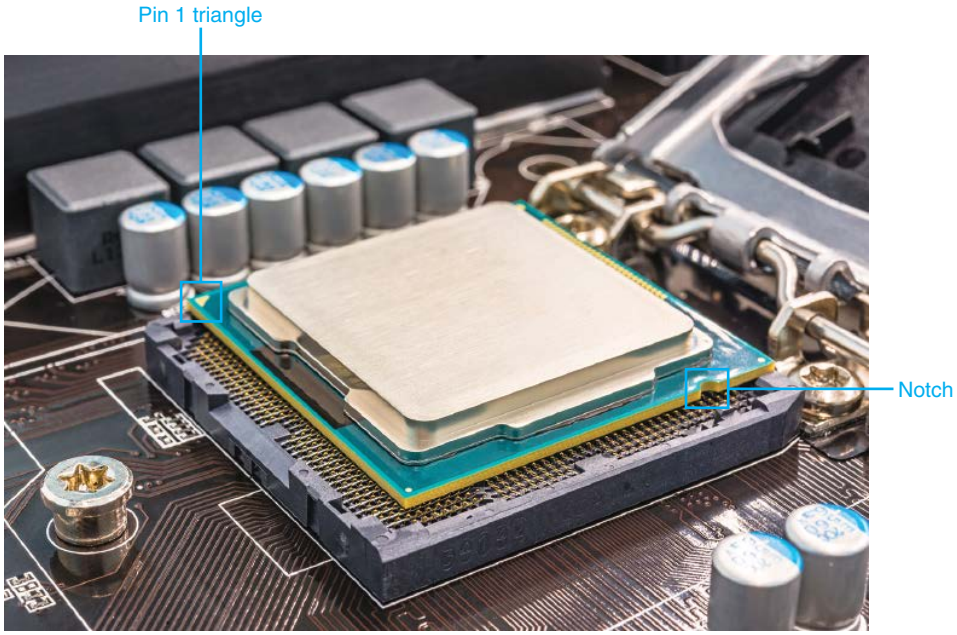


FIGURE 3.17 Pin 1 and notch on a processor

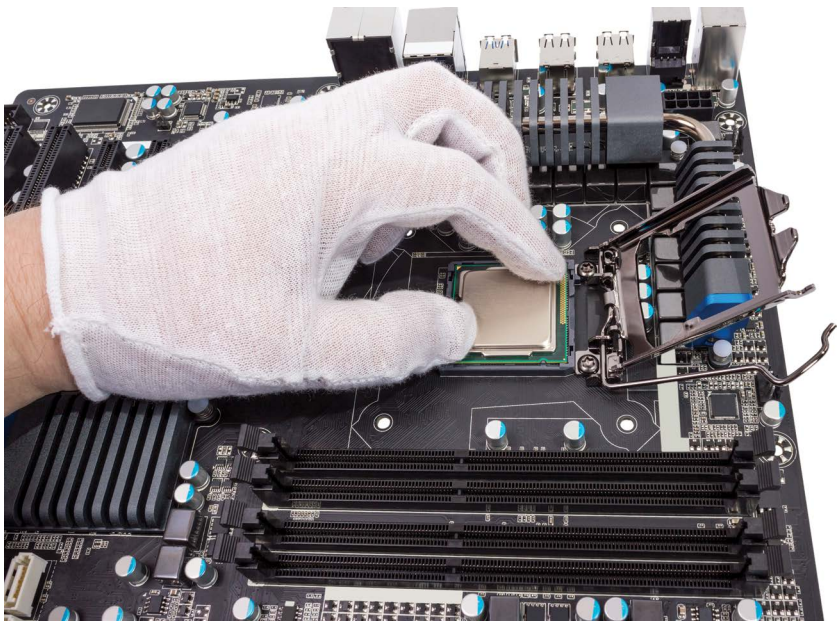


FIGURE 3.18 Installing a CPU

TECH TIP

Handling the CPU

Always hold the CPU by the edges to avoid bending or touching the pins underneath. Do not touch the CPU until you are ready to install it in the socket.

Upgrading Processors

Two common questions asked of technicians are "Can a computer be upgraded to a higher or faster processor?" and "Should a computer be upgraded to a higher or faster processor?" Whether or not a computer can be upgraded to a higher or faster processor depends on the capability of the motherboard. When a customer asks if a processor should be upgraded, the technician should ask, "What operating system and applications are you using?" The newer the operating system, the more advanced the processor should be. Some games and applications that must perform calculations, as well as graphic-oriented applications, require faster, more advanced processors. Refer to the motherboard documentation to determine whether the motherboard can accept a faster processor.

TECH TIP

Upgrading a CPU

Do not upgrade a processor unless the documentation or manufacturer states that the motherboard supports a newer or faster processor.

Upgrading components other than the processor can also increase speed in a computer. Installing more memory or a larger, faster storage device may improve a computer's performance more than installing a new CPU. All devices and electronic components must work together to transfer the 1s and 0s efficiently. The processor is only one piece of the puzzle. Many people do not realize that upgrading only one computer component does not necessarily make a computer faster or better.

Overclocking Processors

Overclocking involves changing the front side bus speed and/or multiplier to boost CPU and system speed. Overclocking has some issues:

- The processor, motherboard, memory, and other components can be damaged by overclocking.
- Applications may crash, the operating system may not boot, and/or the system may hang (lock up) when overclocking.
- You may void the warranty on some CPUs if you overclock.
- When you increase the speed of the CPU, the processor's heat increases. Extra cooling, using fans and larger heat sinks, is essential.
- Attached devices may not react well to overclocking.
- Memory chips may need to be upgraded to be able to keep up with the faster processing.
- You need to know how to reset the system BIOS/UEFI in case the computer will not boot properly after you make changes. This process is covered in Chapter 4.

Throttle management, on the other hand, is the process of controlling the speed of a CPU by slowing it down when it is not being used heavily or when it is hot. Usually this feature is controlled by a system BIOS/UEFI setting and/or the Windows *System* > *Power* Settings option.

TECH TIP

Being ready to cool

The primary problem with overclocking is insufficient cooling. Make sure you purchase a larger heat sink and/or extra fans before starting the overclocking process.

Many motherboard manufacturers do not allow changes to the CPU, multiplier, and clock settings. For the motherboard manufacturers that do allow CPU setting changes, the changes are made through BIOS/UEFI Setup or a manufacturer-provided tool/app. Keep in mind that overclocking is a trial-and-error situation. There are websites geared toward documenting specific motherboards and overclocked CPUs.

Installing CPU Thermal Solutions

A CPU may come with a thermal solution such as a heat sink and/or fan. The thermal solution commonly comes with a pre-applied thermal paste or an attached thermal pad. Heat sinks and fans attach to a processor using different methods, such as screws and clips. Clips can involve retaining screws, pressure release, or a retaining slot. The type of heat sink and/or fan installed must fit the processor and case. Additional hardware may have to be installed on the motherboard to be able to attach a CPU thermal solution. Figure 3.19 shows a CPU heat sink and fan being installed.

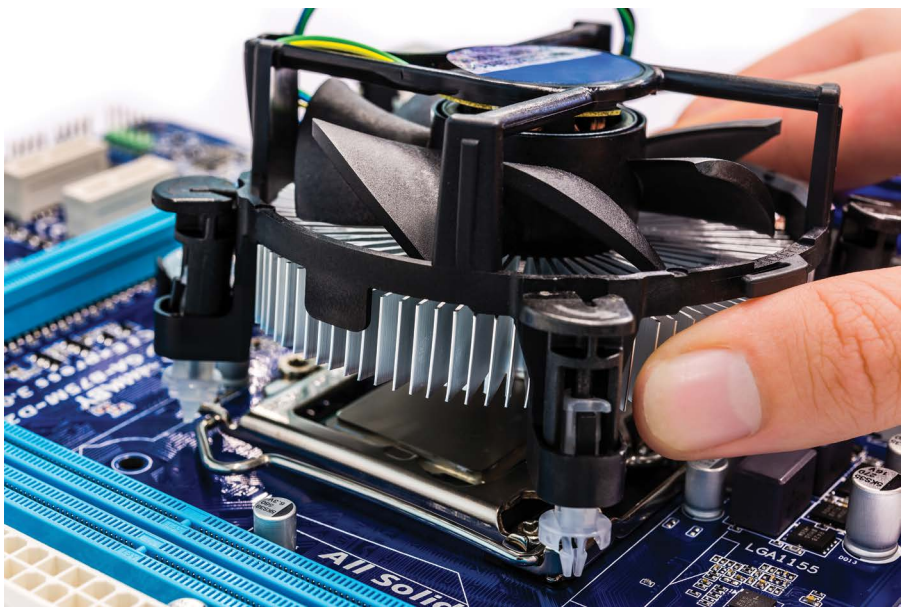


FIGURE 3.19 CPU heat sink/fan installation

TECH TIP

Take a photo of the CPU

Before attaching a heat sink and/or fan to the CPU, take a picture of the markings on top. You might need to use these if you ever need technical support and need the exact specifications. Techs often take pictures to document motherboard replacement and wiring.

If a thermal solution is being installed, the thermal pad or old thermal paste should be removed and new thermal paste applied. Do not scratch the surface of a heat sink. Use a plastic scribe or tool to remove a thermal pad or old paste. Use a thermal paste cleaner, acetone, or denatured or isopropyl alcohol with a lint-free cloth.

When installing thermal paste, you should apply the prescribed amount in the center of the processor. Spread the compound evenly in a fine layer over the portion of the center of the CPU that comes in contact with the heat sink. Consider using an old credit card to do the spreading. When the heat sink is attached to the processor, the thermal compound will spread more (hopefully not over the edges). Always follow the heat sink installation directions.

A CPU fan is likely to have a 3- or 4-pin cable that attaches to the motherboard. The motherboard might have a 3- or 4-pin connector. A 3-pin fan can be attached to a 4-pin motherboard connector, and a 4-pin fan cable can be connected to a 3-pin motherboard connector, as shown in Figure 3.20. However, it is important to note that when a 3-pin cable attaches to a 4-pin connector, the fan runs continuously at full speed and cannot be controlled. In contrast, a 4-pin fan connected to a 4-pin motherboard connector allows for speed control based on temperature and system demands.

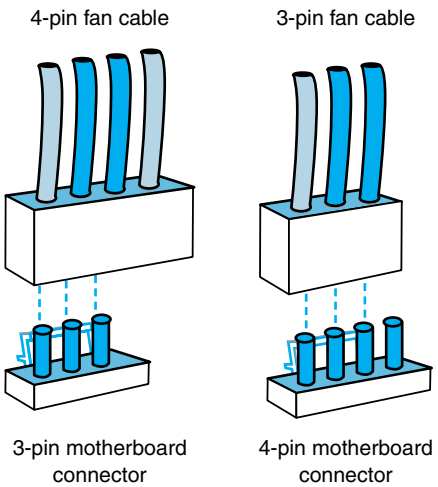


FIGURE 3.20 CPU fan connectivity

Troubleshooting Processor Issues

Processor issues can appear in different ways, as illustrated in Figure 3.21.

Use your senses when troubleshooting processor problems.

- Nothing on the screen (and the power supply and monitor work)
- System powers on, but turns off quickly
- BSOD (blue screen of death)
- An error code that the documentation shows as a CPU problem

- Hear the fan(s) going frantically, but the system won't boot or boots and then shuts off
- System powers on briefly, but then shuts off
- A series of beeps that the manual shows as a CPU problem

- Smell something burning (fan might be out, causing the CPU to shut down)

FIGURE 3.21 Detecting processor problems

The following tips can help you solve CPU issues:

> The number-one issue related to processor problems is heat. Ensure that all fans work. Listen for **unusual noise**, which can indicate that something is caught in the fan or the fan is going bad. Adding fans costs very little compared to replacing a processor and/or a motherboard. Ensure that the computer has adequate circulation/cooling. Vacuum dust from the motherboard/CPU. Cool the room more.
> Check for an overheated CPU. Many BIOS/UEFI apps show the CPU temperature. (This is covered in more detail in Chapter 4.)
> Research any visual codes shown on the motherboard LEDs and listen for audio beeps as the computer beeps. Refer to the computer or motherboard manufacturer's website.

Troubleshooting processor issues can be challenging, as it is often difficult to determine whether the problem lies with the CPU or the motherboard. If the system has power (that is, the power supply has power coming out of it), the hard drive works (try it on a different computer), and the monitor works (try it on a different computer), then the motherboard and/or CPU should be considered as potential causes of the problem.

Expansion Slots

If a computer is to be useful, the CPU must communicate with the outside world, including other motherboard components and adapters that are plugged into the motherboard. An expansion slot is used to add an adapter to the motherboard. Figure 3.22 shows expansion slots on a motherboard.

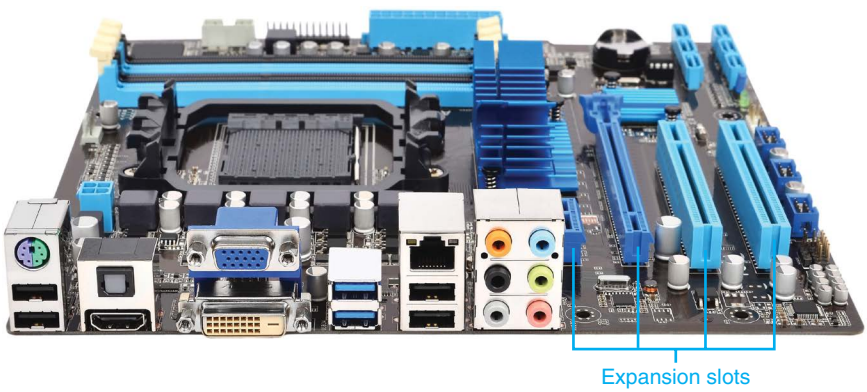


FIGURE 3.22 Motherboard expansion slots

A technician must be able to distinguish between adapters and expansion slots and be able to identify the adapters/devices that use expansion slots. A technician must also realize the abilities and limitations of each type of expansion slot when installing upgrades, replacing parts, and making recommendations. Let's start with the oldest type and move forward.

PCI (Peripheral Component Interconnect)

A previously popular expansion slot is Peripheral Component Interconnect (**PCI**). PCI comes in four varieties: 32-bit 33 MHz, 32-bit 66 MHz, 64-bit 33 MHz, and 64-bit 66 MHz. There was also an upgrade to the PCI bus called PCI-X that was commonly found in servers and is not covered except in comparison here. Figure 3.23 shows the most common type of PCI expansion slot.

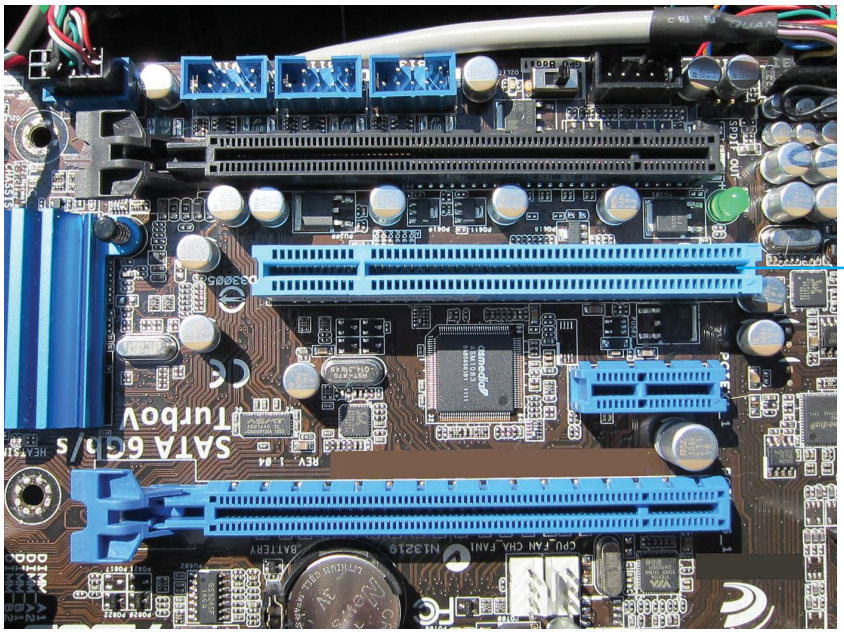


FIGURE 3.23 PCI expansion slot

PCIe (Peripheral Component Interconnect Express)

PCI and Accelerated Graphics Port (**AGP**, which was used exclusively for video cards) have been replaced with **PCIe** (PCI Express). PCIe outperforms all other types of expansion slots. Figure 3.24 shows PCI expansion slots, and Table 3.6 lists the different PCIe versions.

FIGURE 3.24 PCIe expansion slots

TABLE 3.6 PCIe versions

PCIe version	Speed (per lane per direction)
1.0	2.5 GT/s (gigatransfers per second) or 250 MB/s
2.0	5 GT/s or 500 MB/s
3.0	8 GT/s or ~1 GB/s
4.0	16 GT/s or ~2 GB/s
5.0	32 GT/s or ~4 GB/s
6.0	64 GT/s or ~8 GB/s
7.0	128 GT/s or ~16 GB/s

The older PCI standard is half-duplex bidirectional, which means that data is sent to and from the PCI card using only one direction at a time. PCIe sends data full-duplex bidirectionally; in other words, it can send and receive at the same time.

TECH TIP

Other types of cards in PCIe slots

Older PCI and AGP adapters will not work in any type of PCIe slots.

Another difference between PCI and PCIe is that PCIe slots come in different versions, depending on the maximum number of lanes that can be assigned to the card inserted into the slot. For example, an x1 slot can have only one transfer lane used by the x1 card inserted into the slot; x2, x4, x8, and x16 slots are also available. The standard supports an x32 slot, but these slots are rare because of the length. An x16 slot accepts up to 16 lanes, but fewer lanes can be assigned. Figure 3.25 shows the concept of PCIe lanes. Notice that one lane has two unidirectional communication channels. Also note that only seven lanes are used. PCIe has the capability to use a reduced number of lanes if one lane experiences a failure or a performance issue.

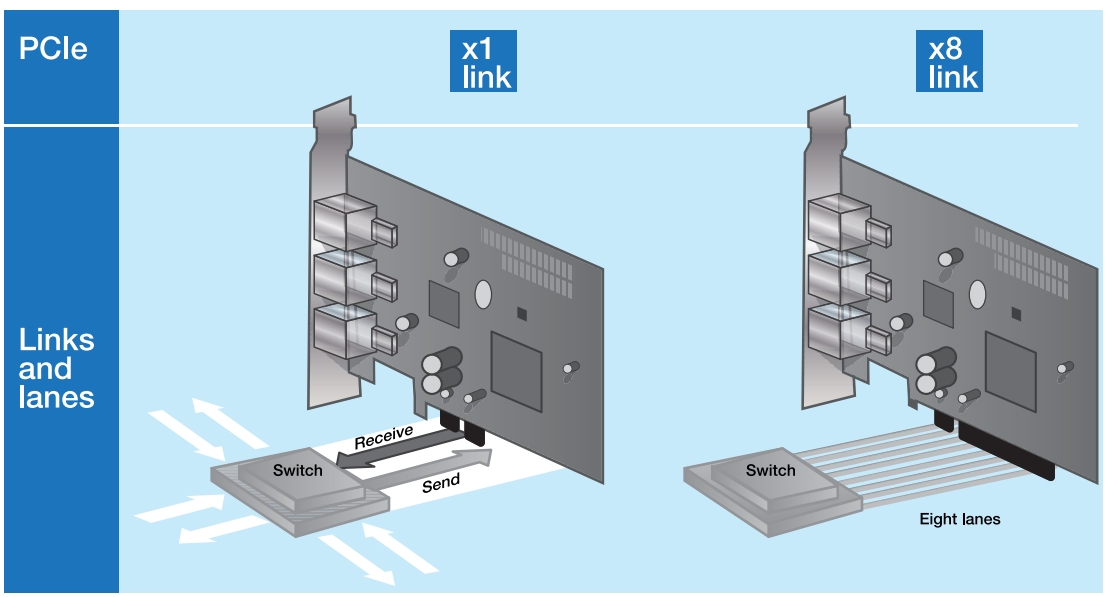


FIGURE 3.25 PCIe lanes

TECH TIP

Beware of the PCIe fine print

Some motherboard manufacturers offer a larger slot size (such as x8), but the slot runs at a slower speed (x4, for example). This keeps the cost down. The manual would show such a slot as x8 (x4 mode) in the PCIe slot description.

A PCIe x1 adapter can fit in an x1 or higher slot. A larger card, such as a PCIe x16, cannot fit in a lower-numbered (x8, x4, x2, or x1) slot. Figure 3.26 shows this concept.

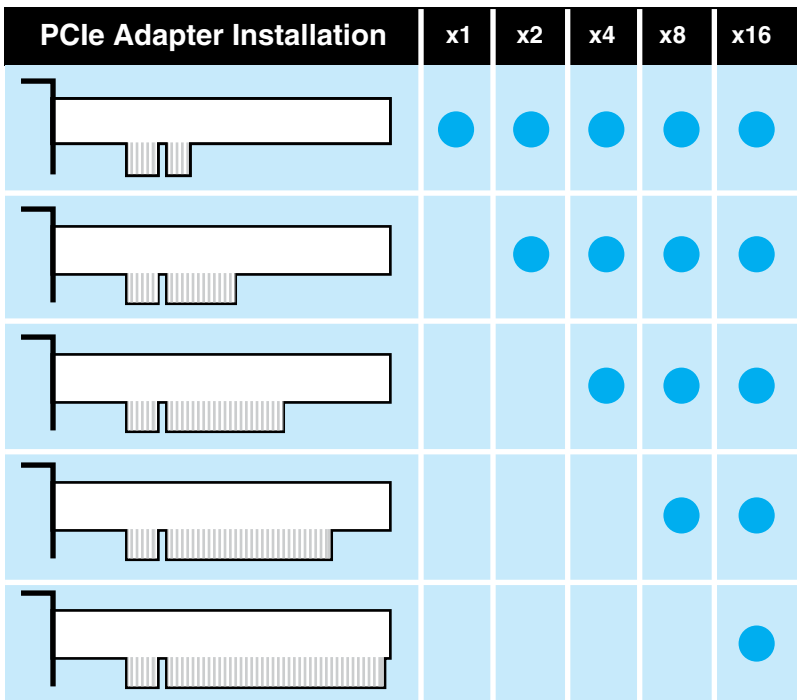


FIGURE 3.26 Correct slots for PCIe cards

Removing an adapter is normally just a matter of removing a retaining screw or lifting a retention plate and lifting the adapter out of the slot. Some AGP and PCIe expansion slots have retention levers. You move the retention lever to the side in order to lift the adapter from the expansion slot. Figure 3.27 shows an example of the PCIe adapter removal process. Figure 3.28 shows a motherboard with two PCIe x1, two PCIe x16, and three PCI expansion slots. Notice that each PCIe x16 slot has a retention lever at the rear of the slot to make the installation and removal process easier and more secure. These levers ensure that the adapter is correctly seated in the slot, which is essential for maintaining a stable connection and optimal performance.

TECH TIP

Removing PCIe adapters

PCIe x16 adapters commonly have release levers. You must press the lever while pulling the adapter out of the expansion slot, or you may damage the adapter (and possibly the motherboard).

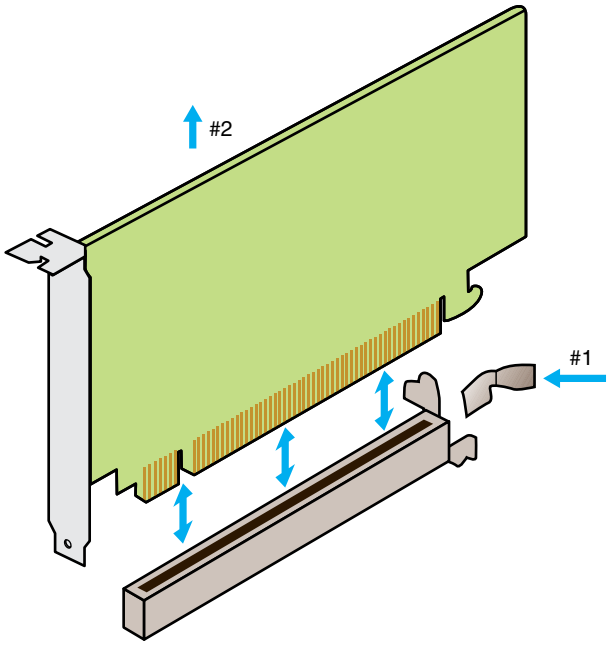


FIGURE 3.27 PCIe adapter removal

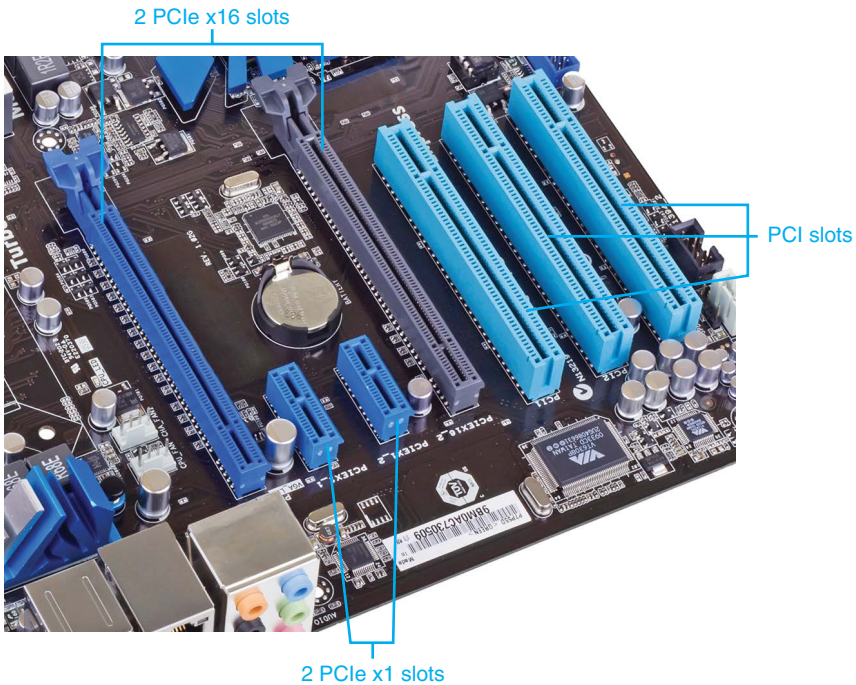


FIGURE 3.28 Motherboard with PCIe and PCI slots

Motherboard Security Options

Motherboards can contain options that provide more security for applications and data. The motherboard might contain a Trusted Platform Module (**TPM**) or a slot to install one. A TPM can be used when securing data, storing digital security certificates, storing passwords, or checking the integrity of operating system files. Microsoft Windows 11 requires that a TPM be installed before the operating system will function. The TPM is enabled and configured through the BIOS/UEFI, as discussed in Chapter 4. Figure 3.29 shows a TPM.

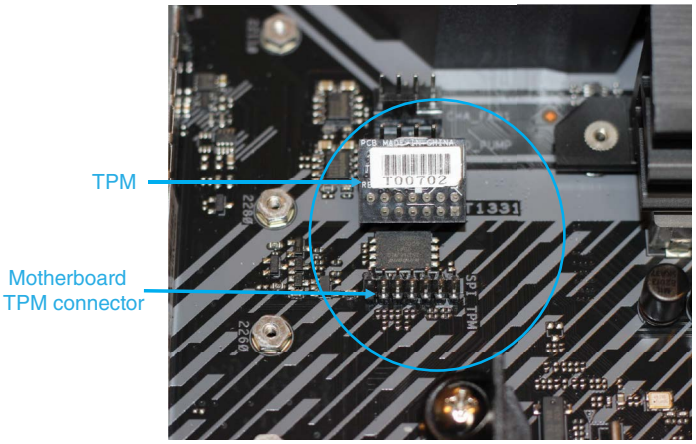


FIGURE 3.29 TPM

Another similar security option is an **HSM** (hardware security module), which can be installed as an adapter to do some of the same functions as the TPM. An HSM has a cryptoprocessor or other chips that are used to create, manage, and store security keys and used in encryption of data and storage devices.

Types of Motherboards

Motherboards come in different sizes, known as **form factors**. The most common desktop motherboard form factor is Advanced Technology Extended (**ATX**), which comes in several varieties, including **microATX** (sometimes written µATX or mATX), mini-ATX, FlexATX, EATX, WATX, nano-ATX, pico-ATX and mobileATX. A drawback to these designs is that the airflow is not as good as it could be.

A smaller form factor is Information Technology eXtended (**ITX**), which comes in mini-ITX, nano-ITX, and pico-ITX sizes. Figure 3.30 shows some of the motherboard form factors, and Table 3.7 provides consolidated information on the main form factors. Figure 3.31 shows a motherboard with many of the motherboard components labeled.

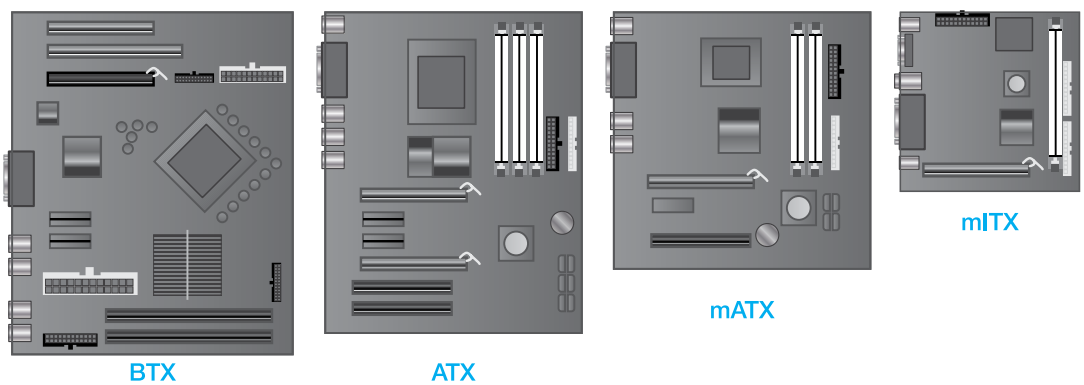


FIGURE 3.30 Motherboard form factors

TABLE 3.7 Motherboard form factor comparison

Form factor	Description	Size
ATX	Used in desktop computers	12×9.6 inches (30.5×24.4 cm)
mATX	MicroATX, a smaller motherboard used in desktop computers	9.6×9.6 inches (24.4×24.4 cm)
ITX or mITX	Used in very small computers and set-top boxes	6.7×6.7 inches (17×17 cm)

TECH TIP

Matching the motherboard form factor and case

The case used for a computer must match the motherboard form factor. Some cases can accommodate different form factors, but you should always check. When you are building a computer or replacing a motherboard, it is important to obtain and verify the correct form factor.

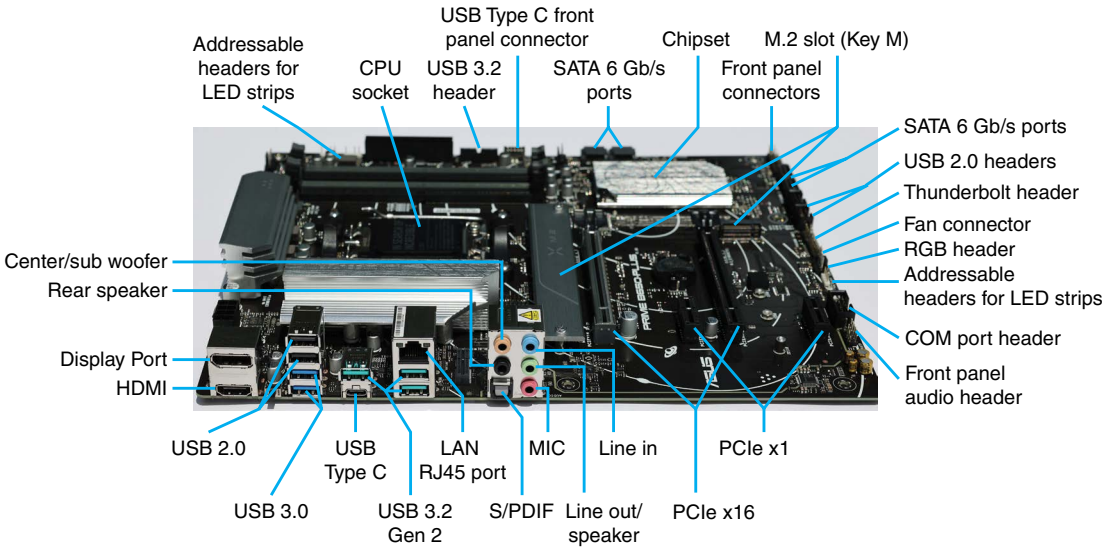


FIGURE 3.31 Gaming motherboard components

A manufacturer may design a case so that it requires a proprietary motherboard. With such a design, a replacement motherboard must be purchased from the original manufacturer and is usually more expensive than a generic option.

Upgrading and Replacing Motherboards

The following list guides you through making the decision (or helping a customer make the decision) about whether to upgrade a motherboard:

- Why is the computer being upgraded? Upgrading the motherboard may not help if the other computer components are not upgraded. If software access is slow, the solution might not be a new motherboard but a faster and larger hard drive, new/high-capacity SSD, or more RAM.
- Which type of expansion slot (PCI, AGP, or PCIe) and how many adapters of each type are needed from the old motherboard? Does the new motherboard have the required expansion slots?
- Is the new motherboard compatible? Check which CPU manufacturer and models are supported. Will the new motherboard fit in the current computer case, or is a new one required?
- If upgrading the CPU, will the motherboard support the new CPU?
- Will the old memory chips work on the new motherboard or with the new CPU?

TECH TIP

Motherboards in other types of devices

Note that server motherboards, laptop motherboards, and other mobile device motherboards tend to be proprietary, and you have to buy a replacement from the manufacturer.

Before replacing a motherboard, it is important to do all the following:

- Remove the CPU and CPU fan.
- Remove adapters from expansion slots.
- Remove memory chips from expansion slots.
- Disconnect power connectors.
- Disconnect ribbon cables.
- Disconnect external devices such as mouse, keyboard, and monitor.

Replacement motherboards do not normally come with RAM, so the old modules are removed from the bad/older motherboard. A motherboard usually does not come with a CPU. When upgrading any component or an entire computer, remember that the older part can be donated to a charity or an educational institution.

TECH TIP

Use good antistatic measures when installing a motherboard

When replacing a motherboard, place the motherboard on a nonconductive surface such as an antistatic mat or the antistatic bag that came with the motherboard.

Motherboard Troubleshooting

Common symptoms of motherboard issues are similar to the symptoms of CPU problems: The system has a **blank screen on bootup** (which could mean the video cable is not attached well or the system is not powered/turned on); an error code appears; one or more beeps occur; the system experiences **random shutdown**; the system might do **continuous reboots**; or one or more of the ports, expansion slots, or memory modules fails. Note that random shutdowns and continuous reboots can also be symptoms of a CPU or power supply problem.

Motherboard problems and power problems are probably the most difficult issues to troubleshoot. Because various components are located on the motherboard, many things can cause errors. **POST** (power-on self-test) is one of the most beneficial aids for troubleshooting a motherboard and may include a series of **POST beeps**. The meaning of any code that appears on the screen should be researched. If multiple POST error codes appear, you should troubleshoot them in the order in which they are presented. Chapter 11, "Computer Design and Troubleshooting Review," contains descriptions of common beeps and errors, but note that manufacturers could have their own **proprietary crash screens** and errors.

The following list helps with motherboard troubleshooting:

- Is the motherboard receiving power? Check the power supply to see if the fan is turning. If the CPU or motherboard has a fan, see if it is turning. Check voltages going from the power supply to the motherboard. See Chapter 5, "Disassembly and Power," for directions.
- Check the BIOS/UEFI settings (covered in Chapter 4) for accuracy.
- Check for **overheating**, which might point to a problem with the CPU or motherboard. Is the motherboard hot to the touch or emitting a **burning smell**? Power down the computer and allow the computer to cool. Power on the computer with the cover off. See if the CPU fan is turning.
- Check the motherboard for **capacitor swelling**—small components that might appear to be bulging. If you look again at Figure 3.28, you can see the metal cylinders (which are capacitors) in the bottom-right corner and beside the expansion slots. If you see that such a capacitor is bulging, replace the motherboard as soon as possible.

- Reseat the CPU, adapters, and memory chips.
- Remove unnecessary adapters and devices and boot the computer.
- Plug the computer into a different power outlet and circuit, if possible.
- Check to determine whether the motherboard is shorting out on the frame.
- Check the CMOS battery. (See Chapter 5 for how to take voltage readings.)
- With a motherboard that has diagnostic LEDs, check the output for any error code. Refer to the motherboard documentation or online documentation for the problem and possible solution.

TECH TIP

These concepts relate to Apple computers, too

Even though this book focuses on PCs, concepts related to CPUs, motherboards, expansion slots, cache, and chipsets also apply to Apple computers. Apple computers and PCs have similar CPU and memory requirements.

SOFT SKILLS: ACTIVE LISTENING

Active listening is participating in a conversation where you focus on what the other person is saying—in other words, listening more than talking. For a technician, active listening has the following benefits:

- Enables you to gather data and symptoms quickly
- Enables you to build customer rapport
- Improves your understanding of the problem
- Enables you to solve the problem more quickly because you understand the problem better
- Provides mutual understanding between you and the customer
- Provides a means of having a positive, engaged conversation rather than having a negative, confrontational encounter
- Focuses on the customer rather than the technician
- Provides an environment in which the customer might be more forthcoming with information related to the problem

Frequently, when a technician arrives onsite or contacts a customer who has a technical problem, the technician is (1) rushed; (2) thinking of other things, including the problems that need to be solved; (3) assuming that they know exactly what the problem is, even though the user has not finished explaining the problem; or (4) more interested in the technical problem than in the customer and the issues. Active listening changes the focus from the technician's problems to the customer's problems.

A common but ineffective service call involves a technician doing most of the talking and questioning, using technical jargon, acronyms, and a flat or condescending tone. A customer who feels vulnerable experiences a heightened anxiety level. Active listening changes this scenario by helping you build a professional relationship with your customers. Figure 3.32 shows a technician actively listening. The lists that follow outline some measures that help you implement active listening.

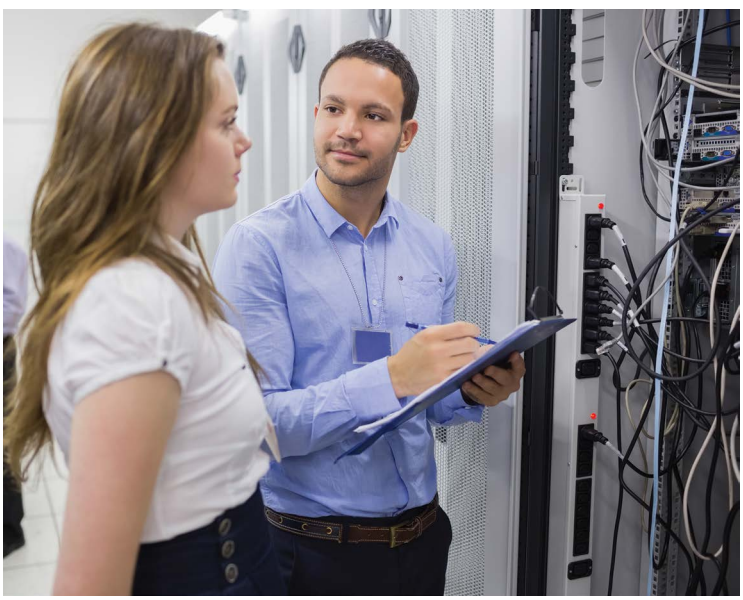


FIGURE 3.32 Active listening

Have a positive, engaged professional attitude when talking and listening to customers:

- Leave your prejudices behind; be polite and aware of other cultures and customs; be open-minded and nonjudgmental.
- Have a warm and caring attitude.
- Do not fold your arms in front of your chest because doing so distances you from the problem and the customer.
- Do not blame others or talk badly about other technicians.
- Do not act as if the problem is not your responsibility.

Focus on what the customer is saying:

- Turn off or ignore your electronic devices.
- Maintain eye contact; don't let your mind wander.
- Allow the customer to finish explaining the problem; do not interrupt; avoid arguing with the customer or being defensive.
- Stop all irrelevant behaviors and activities.
- Mentally review what the customer is saying.
- Refrain from talking to coworkers unnecessarily while interacting with customers.
- Avoid personal interruptions or distractions.

Participate in the conversation in a limited but active manner:

- Maintain a professional demeanor (suspend negative emotions); do not minimize or diminish the customer's problem.
- Acknowledge that you are listening by occasionally nodding and making comments such as "I see."
- Use positive body language such as leaning slightly forward or taking notes.
- Observe the customer's behavior to determine when it is appropriate to ask questions.

Briefly talk with the customer:

- Speak using a positive tone; use a tone that is empathetic and genuine, not condescending.
- Restate or summarize points made by the customer.
- Ask nonthreatening, probing questions related to the customer's statements or questions.
- Do not jump between topics.
- Do not use technical jargon.
- Clarify the meaning of the customer's situation.
- Identify clues to help solve the problem and reduce your troubleshooting time by listening carefully to what the customer says.
- Follow up with the person at a later date to ensure that the problem is solved and to verify their satisfaction.
- Offer different repair or replacement options, if possible.

Chapter Summary

- Important motherboard parts include the following: CPU, RAM slots, RAM, expansion slots (PCI, PCIe, and AGP), and cooling devices.
- ARM processors are popular in mobile devices (but can be used for desktops and servers), take less power, produce less heat, and cost less than Intel or AMD processors. Desktop processors can be multicore and can contain very fast cache memory: L1, L2, and L3.
- Processors must be kept cool with fans and/or heat sinks. A thermal paste or pad is applied between a heat sink and a processor. Never turn on a computer without some type of cooling installed.

- The clock speed refers to the processor's internal clock. This is not the same as the FSB or bus speed.
- CPU throttling slows down the processor to prevent overheating.
- PCI is a 32- and 64-bit parallel bus. PCI and AGP have been replaced with serial PCIe bus.
- PCIe slots have a specific number of bidirectional lanes that are the maximum a card can use. A PCIe adapter can fit in a slot with the same number of lanes or a slot that has the ability to process a higher number of lanes.
- An integrated GPU is on-die with the CPU and processes graphics-related functions.
- When replacing a motherboard, ensure that the form factor, CPU socket, and number/types of expansion slots are appropriate.
- A TPM or an HSM increases security by storing digital security certificates and passwords and securing data.
- Use POST in troubleshooting motherboard or CPU issues. Symptoms of CPU or motherboard issues include swollen capacitors, random shutdowns, blank screen on bootup, continuous reboots, and overheating.
- Active listening is an important skill for a technician. Avoid getting distracted by people or technology. Take notes, make good eye contact, and ask directed questions when appropriate.

A+ CERTIFICATION EXAM TIPS

- ✓ Know the following motherboard connector types: PCI, PCIe, eSATA, socket types (including the term multisocket), and headers. Know that server and mobile motherboards are frequently proprietary items.
- ✓ Know the following CPU architecture features: x64/x86, core configurations, advanced RISC ARM, and virtualization support.
- ✓ Be able to recognize the different sizes of PCIe expansion slots. Use the internet to view motherboards to see if you can determine the type of expansion slot. Do the same for other motherboard components, including the processor. The exam has graphics that are unlabeled.
- ✓ Know that Intel and AMD are two prominent CPU manufacturers that require an appropriate motherboard and socket in order to install the processor.
- ✓ Review the types of CPU cooling methods: fan, heat sink, liquid, and thermal paste/pads.
- ✓ Be able to install a CPU and cooling system. Know how and where to connect a CPU fan.
- ✓ Know the differences between and be able to identify ATX, microATX, and ITX motherboard form factors.
- ✓ Know the differences between a TPM and an HSM.
- ✓ Know symptoms of processor and motherboard issues: swollen capacitor, random shutdowns, blank screen on bootup, continuous reboots, overheating, or a burning smell. Use POST codes to help with troubleshooting.

Key Terms

active listening, AGP, AI, AMD, APU, ARM processor, ATX, blank screen, burning smell, bus, cache memory, capacitor swelling, clock, clock speed, continuous reboot, CPU, CPU socket, CPU speed, CPU throttling, core configurations, fan, form factor, FSB, gigahertz, GPU, heat sink, HSM, HyperTransport, iGPU, Intel, ITX, L1 cache, L2 cache, L3 cache, liquid cooling, microATX, multicore, multisocket, NPU, overclocking, overheating, PCI, PCIe, POST, POST beeps, processor, proprietary crash screen, random shutdown, SoC, thermal pad, thermal paste, thread, throttle management, TPM, unusual noise, virtualization, virtualization support, VM, x64, x86, ZIF socket

Review Questions

1. Which component can be located both on a video card and on a motherboard?

   [TPM | PCIe expansion slot | PCI expansion slot | GPU]

2. Which expansion slot is *best* for a video card in a new desktop computer?

   [PCIe | PCI | USB | AGP]

3. A motherboard has a PCIe x16 expansion slot. Which PCIe adapter size(s) will fit in this slot? (Choose any that apply.)

   [x1 | x2 | x4 | x8 | x16 | x32]

4. Match each motherboard part with the correct description.

____ L1 cache	**a.** Mounted on top of the CPU
____ CPU	**b.** Memory found in the CPU
____ FSB	**c.** Executes software instructions
____ heat sink	**d.** Bus between the CPU and motherboard components
____ SoC	**e.** Slows the CPU to cool it
____ throttling	**f.** Single chip that has CPU, RAM, and ports

5. What is the front side bus?

   a. The internal data bus that connects the processor core to the L1 cache

   b. The internal data bus that connects the processor core to the L2 cache

   c. The external data bus that connects the processor to the motherboard components

   d. The external data bus that connects the processor to the L2 cache

6. A customer wants to upgrade the L2 cache. Which of the following does this definitely require?

   a. A motherboard purchase

   b. A CPU purchase

   c. A video card purchase

   d. A RAM module purchase

7. Match the expansion slot to its definition. Each answer is only used one time.

____ PCIe x16	**a.** 32- or 64-bit parallel bus
____ PCI	**b.** commonly used for video cards
____ PCIe	**c.** has a varying number of lanes

8. List three things that would indicate that the processor or motherboard needs to be replaced.

   _____

   _____

   _____

   _____

9. What should a technician do if a swollen capacitor is found on a motherboard?

   a. Replace the capacitor.

   b. Replace the motherboard.

   c. Check the voltages coming from the power supply.

   d. Replace the power supply.

10. Which of the following statements is true regarding PCIe?
    - **a.** A PCIe slot will not accept a PCI card.
    - **b.** PCIe is a parallel bus technology.
    - **c.** PCIe is a 32- or 64-bit bus technology.
    - **d.** PCIe is being replaced by PCI-X.
11. [T | F] A PCIe x8 adapter always transmits using eight lanes.
12. What is the significance of a motherboard specification that states the following: 1 PCIe x16 (x8 mode) slot?
    - **a.** The slot accepts x8 or x16 cards.
    - **b.** The slot can transmit traffic using 8 or 16 lanes.
    - **c.** The slot can transmit in bursts of 8 or 16 bytes at a time.
    - **d.** The slot accepts x16 cards but uses only 8 lanes.
13. What are two security options that would help with password management and encryption? (Choose two.)

    [CPU | TPM | PCIe standard | GPU | HSM]
14. A technician for a college is going to repair a problem in another building. A professor stops the technician to talk about her slow computer. The technician gives a little eye roll but then stops and listens to the professor. The professor comments, "I can't get my email or even type my tests. The computer takes at least 20 minutes just to boot." The technician looks around, a little exasperated, and says, "Uh huh." "I logged this problem over a week ago," continues the professor, "and no one has dropped by." "Uh huh," replies the technician again. "Do you know when you folks might get to that issue or have an idea about what might be the problem?" the professor asks. The technician looks at the professor and says, "It is probably a virus that has been going around. Jim was supposed to get to those. We will get to you as soon as we can." The technician's phone rings, and he walks away to get to the phone.

    List three active listening techniques and good customer support procedures that would lead to a better interaction.

    _____

    _____

    _____

    _____

    _____
15. Explain how a technician might be culturally insensitive.

    _____

    _____

    _____
16. Which component can be adjusted to overclock?

    [heat sink | CPU | expansion slot | chipset]
17. [T | F] When installing a CPU, orient pin 1 to pin 1 on the socket and align the other pins. Lower the ZIF socket lever and lock. Power on the computer to ensure that the CPU works. Power down the computer and install the heat sink and/or fan.
18. What is applied between a processor and a heat sink to increase heat dissipation?

    [a capacitor | thermal paste | a fan | cache memory]
19. When looking over the specifications for the motherboard, you see LGA 2066. Which component is being referenced?

    [RAM | HSM | processor | expansion slot]
20. Which method is not used to cool a processor?

    [CPU fan | case fan | heat sink | thermal tank]

Exercises

Exercise 3.1 Identifying ATX Motherboard Parts

Objective: To identify various motherboard parts

Parts: None

Procedure: Identify each of the ATX motherboard parts in Figure 3.33.

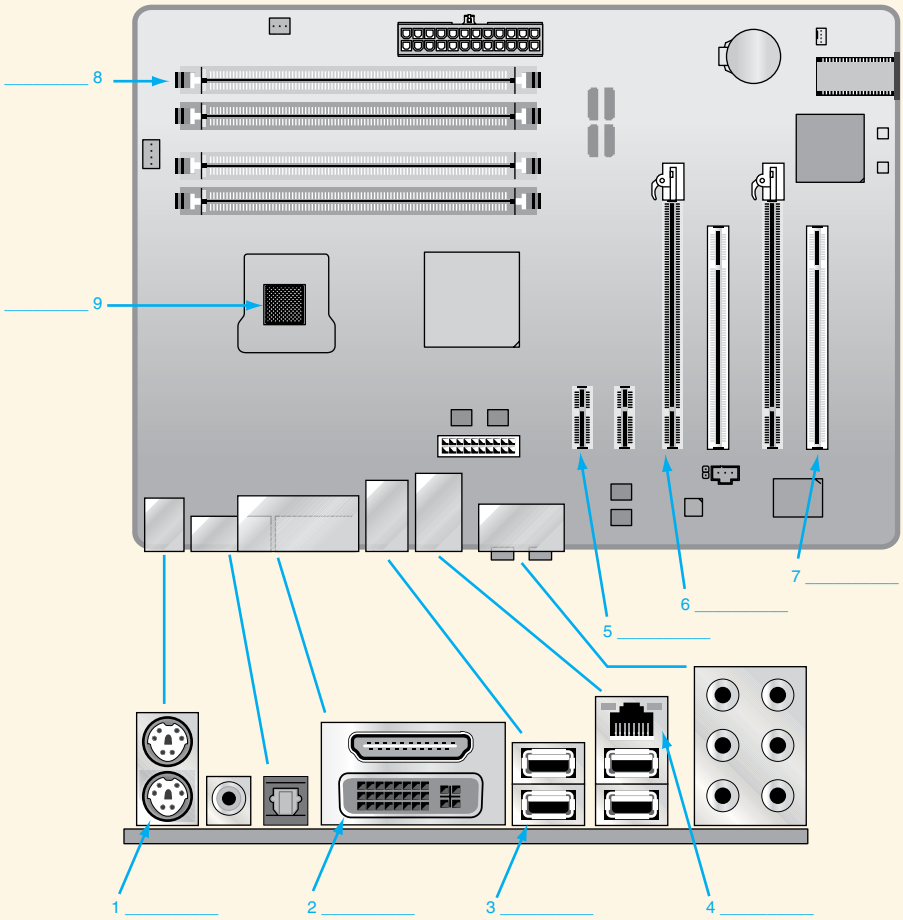


FIGURE 3.33 Motherboard ports, slots, and parts

1. _____
2. _____
3. _____
4. _____
5. _____
6. _____
7. _____
8. _____
9. _____

Exercise 3.2 Motherboard Analysis

Objective: To identify various motherboard parts

Parts: None

Procedure: Using the information you learned in this chapter and related to the specifications found in Figure 3.34, answer the questions that follow.

XYZ Motherboard Specifications

Form factor	ATX
Power connector	1 x 24-pin main power 1 x 8-pin 12V power
CPU	
Power connector	LGA 1200
CPUs supported	Core-X 10000 / 9000 / 78xx
Chipset	Intel B560
Memory	
Memory	4x288-pin
Memory	DDR4 4266 (OC) / 4000 (OC), 3600 (OC) / 3200 / 3000 / 2933 / 2800 / 2666
Memory	128GB
Memory	Dual channel
Expansion slots	
PCIe 4.0 x 16	1
PCIe 3.0 x 16	1 (x4 mode)
PCIe 3.0 x 2	2
Onboard LAN	
Max LAN speed	1 x RJ-45 port 1Gbps
Wireless LAN	802.11 a/b/g/n/ac/ax
Rear ports	
PS/2	1 x PS/2 keyboard/mouse port
Video	1 x D-sub + 1 x DVI-D ports
HDMI	1 x HDMI
DisplayPort	1 x DisplayPort
USB 3.2 Gen 1	4 ports
USB 1.1/20	2 ports
S/PDIF out	1 x optical
Audio	6 ports

FIGURE 3.34 Desktop motherboard advertisement

1. If you were buying this motherboard, what type of case would you need to purchase?

   _____

2. What does LGA 1200 tell you about this motherboard?

   _____

3. Does this motherboard come with a CPU installed?

   [Yes | No | Cannot tell from the information presented]

4. What motherboard component controls the maximum number of USB 3.0 ports this motherboard could have?

   [CPU | RAM | chipset | FSB]

5. What manufacturer makes the processor(s) that this motherboard accepts?

   _____

6. What do you think the letters O.C. after some of the memory chips mean in relationship to this motherboard?

   _____

   _____

7. What is the most significant difference between a version 3.0 PCIe slot and a version 4.0 PCIe expansion slot?

   _____

8. What does the PCIe 3.0 x16 line that states "1 (x4 mode)" mean?
   a. The adapter that goes into this slot can use a single lane that goes at x16 speeds or two lanes that go at x4 speeds.
   b. One single x16 adapter and/or one single x4 adapter can go into the expansion slots.
   c. One x16 adapter can go into one of the version 3.0 slots, but it can transfer only four lanes at a time at version 3.0 speeds.
   d. A single x16 adapter can be installed in one of the version 3.0 slots, or two x4 adapters can be installed in the two version 3.0 slots.
9. What device cable can be inserted into the PS/2 port? (Choose the best answer.)

   [speaker | mouse or keyboard | display | external storage]
10. Which type of video port is described as a D-sub in this documentation?

    [DisplayPort | DVI | HDMI | VGA]
11. What is an advantage of having an integrated GPU in a CPU?

    _____
12. What is the most likely reason this motherboard manufacturer chose to include two PCI expansion slots?

    _____

    _____
13. How many different video port types does this motherboard have? List them.

    _____
14. What is the purpose of the S/PDIF out port?
    [video | audio | wireless networking | input device connectivity]
15. Is this motherboard a multisocket motherboard? How can you tell?
    [yes | no]

Activities

Internet Discovery

Objective: To obtain specific information on the internet regarding a computer or its associated parts

Parts: A computer with internet access

Procedure: Locate documentation on the internet for a Gigabyte TRX50 AERO D sTR5 motherboard to answer Questions 1–12. Continue your internet search to answer Questions 13 and 14.

Questions:

1. Does the motherboard support an Intel processor or an AMD processor?

   _____
2. Which chipset is used?

   _____
3. How many adapter expansion slots are on the motherboard?

   _____
4. Which form factor does this motherboard use?

   _____
5. Which processors can be used on this motherboard?

   _____

6. Does the motherboard support having an integrated GPU in the CPU? How can you tell whether it does or not?

_____

_____

_____

7. Which type of CPU socket does the motherboard have?

_____

8. How many and what type of PCIe slots does it have?

_____

9. Are there any other type of slots on this motherboard? If so, what type(s)?

_____

10. Does this motherboard have at least one integrated USB Type-C port that can be used for a monitor?

_____

11. What are the maximum number and type of USB ports available on the rear of the motherboard?

_____

_____

_____

12. Write the URL where you found the motherboard information.

_____

_____

13. Find a vendor for an Intel motherboard that uses the LGA 1851 socket and supports the 14th-generation Intel desktop processors. Document the motherboard model and vendor.

_____

_____

14. Find an internet site that describes the dimensions of the extended ATX motherboard form factor. List the dimensions and the website or AI generator you used to discover this information.

_____

_____

Soft Skills

Objective: To enhance and fine-tune a future technician's ability to listen, communicate in both written and oral forms, and support people who use computers in a professional manner

Activities:

1. On a piece of paper or an index card, list three ways you can practice active listening at school. Share this information with your group. Consolidate ideas and present five of the best ideas to the class.
2. In a team environment, come up with two examples of situations you have experienced in which a support person (a PC support person, sales clerk, checkout clerk, person being asked directions, and so on) could have provided better service if they had been actively listening. Share your findings with the class.
3. In teams of two, have one person tell a story and the other person practice active listening skills. The person telling the story should critique the listener. The pair should then change roles.

Flip the CLASSROOM

Critical Thinking Skills

Objective: To analyze and evaluate information and to apply learned information to new or different situations

Activities:

1. Find an advertisement for a computer in a local computer flyer, newspaper, magazine, book, or on the internet. Determine all the information about the motherboard and ports that you can from the ad. Write down any information you do not understand. Research this information and share your findings with a classmate.

   _____

2. Your parents want to give you a new computer as a present. The one they are considering has a GPU integrated into the CPU. List at least one argument you might use for getting a different computer model.

   _____

   _____

   _____

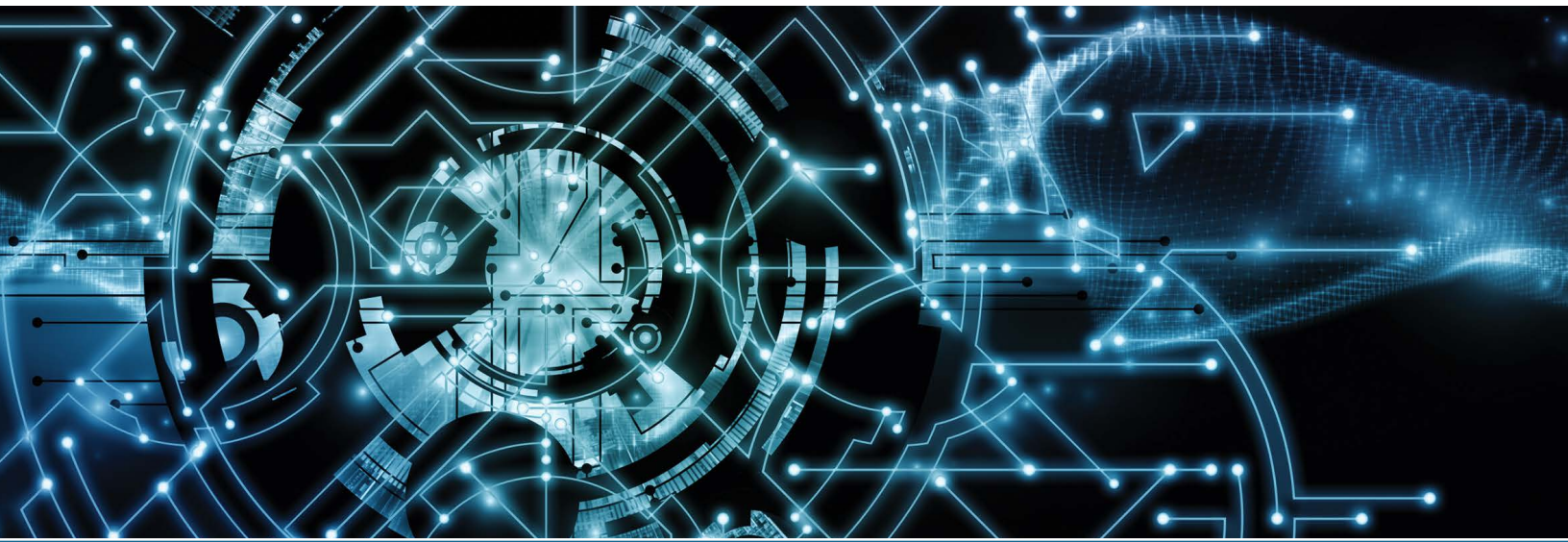
3. Why do you think a motherboard has different buses that operate at different speeds?

   _____

   _____

This page intentionally left blank

4 Introduction to Configuration



In this chapter you will learn:

- The importance of BIOS/UEFI
- How to replace a motherboard battery
- What system resources are and how to view/change them
- Basics steps needed to install, configure, and verify common peripheral devices and USB, eSATA, and network cards
- How to troubleshoot configuration and device issues

CompTIA Exam Objectives:

- ✓ 1201-3.2 Summarize basic cable types and their connectors, features, and purposes.
- ✓ 1201-3.5 Given a scenario, install and configure motherboards, central processing units (CPUs), and add-on cards.
- ✓ 1201-5.1 Given a scenario, troubleshoot motherboards, RAM, CPUs, and power.
- ✓ 1201-5.2 Given a scenario, troubleshoot drive and RAID issues.

Configuration Overview

Configuration can mean a lot of things, but this chapter focuses on using the system BIOS/UEFI Setup program and looking at configurations that might need to be done when installing adapters. We are going to start off with the system **Setup** program, which enables you to configure the motherboard, power, and devices. It also allows you to adjust BIOS/UEFI-level performance settings.

BIOS Overview

The basic input/output system (BIOS) is an important motherboard component that is commonly soldered to the motherboard, as shown in Figure 4.1. BIOS is also known as the Unified Extensible Firmware Interface (UEFI) and sometimes simply as EFI, BIOS/UEFI, or UEFI/BIOS. UEFI is covered in the next section. **BIOS** generically has the following functions:

- Holds and executes power-on self-test (**POST**)—a program that identifies, tests, and initializes basic hardware components.
- Holds a basic routine called a bootstrap program that locates an operating system and launches it, allowing the operating system to then control the system.
- Holds Setup, which is a program that allows viewing and management of settings related to the display, date/time, processor, memory, and drives. Other names used for Setup include BIOS (or UEFI) Setup, System Setup, and CMOS Setup.
- Optionally, turns over control to an adapter's onboard BIOS so that the card can initialize during the computer boot process.

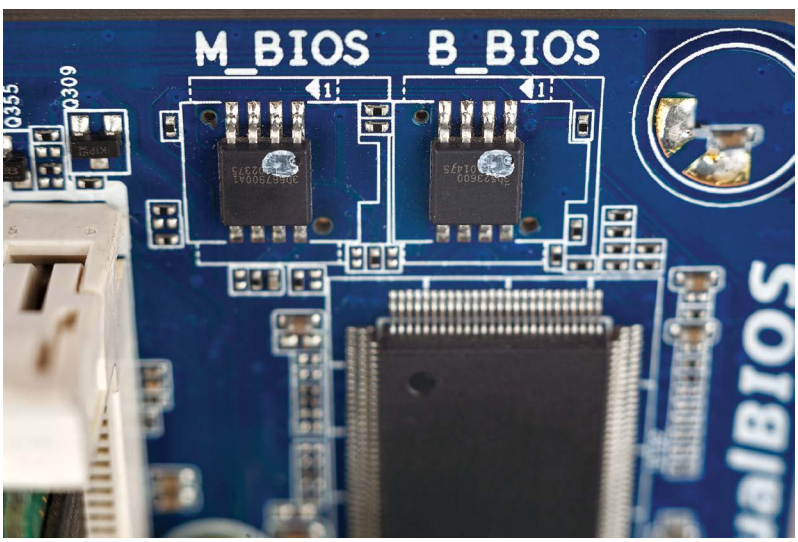


FIGURE 4.1 Motherboard BIOS

POST performs basic tests of individual hardware components. POST runs when a cold boot is performed (powering on the computer). An indication that POST is running is that the indicator lights on the keyboard momentarily flash on and then off. In contrast, restarting the computer is known as a warm boot. A warm boot does not execute POST.

TECH TIP

Speed up boot time

BIOS can be configured to limit the number of devices checked by POST, thus reducing boot time.

There are two main ways to configure a system or an adapter: through the Setup program held in system BIOS and through the operating system. Let's examine using the Setup program method first.

TECH TIP

What if you can't get into Setup?

If nothing appears on the monitor and the display has power and a good connection to the video port, check the motherboard for any LEDs (CPU, RAM, display/VGA, boot, etc.) and research what it means if the particular LED stays on. Check CPU, CPU fan, and RAM installation.

Flash BIOS

Flash BIOS allows you to upgrade (or downgrade) the BIOS without installing a new chip or chips. Common computer BIOS/UEFI manufacturers include AMI (American Megatrends, Inc.), Phoenix Technologies, Byosoft (Nanjing Byosoft Co., Ltd.), and Insyde Software. Many companies, like Dell, HP, and ASUS, customize their own BIOS chips or subcontract with a BIOS manufacturer to customize them.

To determine the current BIOS version, you can do one of the following:

- Watch the computer screen as it boots. Note that you might be able to press the Pause/Break key to freeze the frame and better see the boot information.
- Enter BIOS Setup using a particular keystroke during the boot process.
- From within Windows, access BIOS/UEFI Setup.

TECH TIP

Accessing BIOS Setup from Within Windows 10/11

To access BIOS Setup in Windows, go to Windows *Settings* > Windows 10 *Update and Security*/ Windows 11 *System* > *Recovery* > *Advanced Startup Restart Now* button. Then, use *Troubleshoot* > *Advanced Options* > *UEFI Firmware Settings*.

An upgrade of the BIOS normally involves removing all BIOS software and settings stored in CMOS. Some manufacturers provide utilities that enable you to save the current CMOS settings before upgrading the BIOS. Two things should be done before upgrading the flash BIOS, if possible: Back up current CMOS settings and back up the current BIOS.

UEFI

Unified Extensible Firmware Interface (**UEFI**) is a modern technology that serves as a bridge between a computer's operating system and its firmware. It can either work alongside the traditional BIOS or completely replace it. The traditional BIOS always checks for certain things, such as a keyboard, before allowing the system to boot. Traditional BIOS made configuring kiosks and other touch screen technologies difficult. UEFI addressed these limitations by providing a more flexible and customizable boot process.

Setup Program

Computers have Setup software built into the system BIOS/UEFI chip on the motherboard that you can access with specific keystrokes (such as Esc, Insert, Del, F1, F2, F10, or the key combination Ctrl+Alt+some other key) determined by the BIOS manufacturer. During the boot process, most

computers display a message stating which keystroke(s) will launch the Setup program. The message shown is usually in one of the four screen corners (see Figure 4.2).

FIGURE 4.2 Setup keystrokes

With UEFI, you can boot into a special environment, but unlike with the original BIOS environment, you can use your mouse and possibly connect to the internet, run applications, run a virus scan, use a GUI, execute utilities, or perform a backup or a restore—a lot more configuration options in a much easier-to-use environment. From within Windows, use the search function to launch the *System Information* tool > locate *BIOS Mode* to see if your computer is running in UEFI mode or legacy mode. Figure 4.3 shows an example of a UEFI environment.

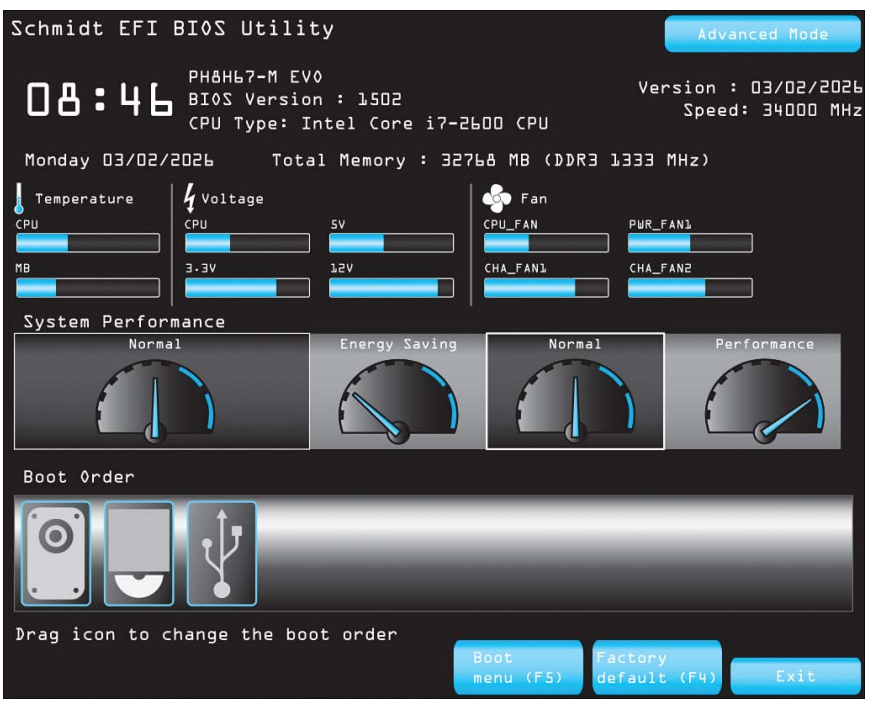


FIGURE 4.3 Sample UEFI main menu

Most manufacturers have moved to the UEFI type of BIOS for the following reasons:

> It is a graphical environment that provides mouse support.
> It enables you to use a virus-scanning utility that is not operating system dependent.

- It offers software that is not just configuration screens.
- It offers optional internet access for troubleshooting or download capabilities.
- It offers better system support for cooling, voltage levels, performance, and security.
- It supports increased hard drive capacities and the ability to divide the hard drive into sections that are not subject to the limitations of the traditional BIOS.
- It commonly has data related to temperature, voltage, CPU speed, bus speed, and fan speed.
- It can have a boot manager instead of relying on a boot sector. See Chapter 7, "Storage Devices," for more information on the GUID partition table (GPT) and boot sector.

From the BIOS/UEFI main menu, there might be icons you can use to access utilities or more advanced configurations, as shown in Figure 4.4.

FIGURE 4.4 Sample UEFI advanced menu

BIOS/UEFI Configuration Settings

BIOS/UEFI options vary by manufacturer, but many options are similar. You must save your changes whenever you make configuration changes. Some manufacturers allow saving screen captures to a USB flash drive. Exiting without saving changes is a common mistake. Table 4.1 shows some common settings and briefly explains each one. Note that the key terms shown in the table are on the CompTIA A+ certification exam.

TECH TIP

Using Setup to disable ports and connectors

Motherboards include connectors for hard drives as well as ports for USB or video connectors. If one of these connectors fails, you can disable it through Setup and obtain a replacement adapter. Setup can also be used to disable integrated motherboard ports.

TABLE 4.1 Common BIOS/UEFI Setup options

Setup option	Description
System information	Displays general information, such as the processor, processor speed, amount of RAM, type and number of hard drives and optical drives installed, BIOS/UEFI manufacturer, and BIOS/UEFI date.
General optimization	Allows faster booting through the disabling of features such as memory checking, booting to the network, and booting from removable drives.
Boot options, Boot sequence, Boot drive order, or Boot menu	Prioritizes devices in the order in which the computer looks for an operating system. Change the boot drive order when a system attempts to boot to an incorrect device.

Setup option	Description
CPU configuration or Advanced CPU settings	Contains settings such as CPU TM function, which affects CPU throttle management (slowing the CPU when overheated); clock speed, which may not be changeable; PECI (Platform Environment Control Interface), which affects how the thermal sensors report the core temperature of the CPU; Max CPUID, which is used for compatibility with older operating systems; CPU Ratio Control, which sets the CPU multipliers; and Vanderpool Technology, which is used with Intel virtualization.
Fan control/Fan considerations	Enables the configuration of case and/or CPU fans, including the ability to place the fans in silent mode or control fan speed.
Video options	Enables configuration to control video memory, aperture size, and which video controller is primary or secondary.
Onboard device configuration	Allows modification of devices built into the motherboard, such as audio, Bluetooth wireless, network, USB, or video ports.
* **Passwords**, **boot password**, **BIOS password**, power on password, password options, supervisor password, **administrator password**, or user password	Allows protection of the BIOS/UEFI menu options—specifically configuration of a password to enter the Setup program—to allow the computer to boot or to distinguish between someone who can make minor changes such as alterations to **boot options** or date and time (user password) and someone who can view and change all Setup options (supervisor or administrator password). Other vendors might have the following levels: full access (all screens except supervisor password), limited access, view-only access, or no access.
Temperature monitoring/ Hardware monitor	Shows CPU temperature and might include motherboard temperature, voltages, clock speeds, and fan speeds. Check fans/cooling solution if the temperature stays above 90°C.
* Virus protection	Runs a small virus-scanning application located in BIOS/UEFI. Some operating systems and software updates require this option to be disabled for the upgrade to proceed.
Numlock on/off	Allows default setting (enabled or disabled) of the Num Lock key function after booting.
USB permissions	Allows modification of USB speed and the number of ports to enable.
Integrated peripherals (enabling/disabling devices and ports)	Allows enabling/disabling and configuration of motherboard-controlled devices such as SATA ports and integrated ports, including USB, audio, and network. Sets the amount of RAM dedicated for video use.
Advanced BIOS options	Allows configuration of options such as CPU and memory frequencies, CPU, front side bus, north bridge, south bridge, chipset, and memory voltage levels.
SATA configuration	Allows viewing of Serial ATA values assigned by BIOS/UEFI and changing of some of the related options, as well as RAID configuration.
Devices	Allows configuration of USB, SATA, video, onboard devices, and PCI, where the M.2 slot might need to be enabled so the SSD will be recognized.

Setup option	Description
Virtualization support, Virtualization technology, or Secure virtual machine mode	Enables/disables virtualization so the virtualization software can access additional hardware capabilities.
ACPI (Advanced Configuration and Power Interface)	Determines what happens if power is lost, power options if a call comes into a modem, and power options when directed by a PCI or PCIe device or mouse/keyboard action.
* **Drive encryption**	Specifies the key used to encrypt the data on the hard drive. The computer will not boot without the correct password. The drive cannot be moved to another computer unless the correct password is entered.
* **LoJack**	Allows security settings to perform tasks such as locating the device, locking the device remotely, displaying an "if lost" message, or deleting data if stolen.
* Intrusion detection/ notification or Chassis intrusion	Allows notification if the computer case has been removed.
* **Secure Boot**	Checks every driver before launching the drivers and the operating system. Prevents an unauthorized operating system or software from loading during the boot process.
iGPU	Allows configuration of how much memory is allocated for the integrated GPU.
Built-in diagnostics	Provides access to hardware components, the hard drive, memory, the battery, and other diagnostic tests.
* Trusted Platform Module (**TPM**)	Allows enabling the TPM motherboard chip that generates and stores cryptographic keys and passwords. You can also clear the saved data using the TPM Clear option. Note that you might also see a fTPM (firmware TPM) option if the TPM function uses the CPU and not a separate chip to provide this function. You might also see a PTT option.

* Security options

TECH TIP

System boots from the wrong device

If the computer tries to boot from the wrong device, change the Boot Sequence setting in BIOS/UEFI. It is also possible that an optical disc is in the drive or a non-bootable USB drive is attached, and that is the first boot option currently selected.

Figure 4.5 shows a sample BIOS/UEFI screen where you can set the administrator or user password. Note that this is not a Windows or corporate network password.

FIGURE 4.5 Password security menu

TPM Considerations

TPM comes in two main versions, 1.2 and 2.0. Version 2.0 is a worldwide standard, but each computer manufacturer's UEFI options list differently. When you enable TPM through the UEFI, you select and enable the TPM, through a physical module or through the firmware. You can also clear the TPM.

TECH TIP

Clearing TPM invalidates security keys and causes data loss

If you clear the TPM, TPM is turned off and all existing security keys are invalidated, and this can lead to loss of access to encrypted data. Ensure that all data is backed up before clearing the TPM. You can keep all security keys and data if you just disable (turn off) the TPM instead of clearing it.

During the boot process, each component is checked for boot drivers, rootkits, and malware, and the TPM stores this information. The UEFI Secure Boot option, BitLocker Drive Encryption, and Windows Defender make use of the TPM. Once enabled, you can start the TPM initialization wizard by typing `tpm.msc` in the Windows *Search* textbox. You will be prompted to create a TPM owner password. This password can be saved to removable media and/or printed. Note that this is very important information and cannot be recovered.

CMOS Memory

Settings changed in system BIOS/UEFI are recorded and stored in a complementary metal-oxide semiconductor (**CMOS**) found in the motherboard chipset. CMOS is memory that requires a small amount of power provided by a coin-sized lithium battery (**CMOS battery**) when the system is powered off. The memory holds the settings configured through BIOS/UEFI. When the battery dies, all configuration information in CMOS is lost and must be reentered or relearned after the battery is replaced.

TECH TIP

Incorrect Setup information causes POST errors

If you incorrectly input configuration information, POST error codes or error messages that would normally indicate a hardware problem appear.

Motherboard Battery

The most common CMOS battery used today is a CR2032 lithium battery, which is about the size of a nickel. Figure 4.6 shows a lithium battery installed on a motherboard.

FIGURE 4.6 Motherboard battery

TECH TIP

Date, time, or settings reset

A first indication that a battery is failing is **inaccurate system date/time** on the computer. Another indication is if the computer asks you to press some key to continue.

No battery lasts forever. High temperatures shorten a battery's life span, which is typically 3 to 10 years.

TECH TIP

Using a battery recycling program

Many states have environmental regulations regarding battery disposal. Many companies also have battery recycling programs. The earth911.com website provides information regarding recycling and disposing of batteries and computer components by zip code or city/state.

Flashing/Clearing the BIOS/UEFI

Firmware updates are needed to obtain new BIOS/UEFI features and address security flaws that arise. The terms used for this process are "flashing the BIOS" and "updating or upgrading the firmware." A BIOS/UEFI upgrade may be necessary for a variety of reasons, including the following:

- To provide support for new or upgraded hardware, such as a processor or a faster USB port
- To provide support for a higher-capacity hard drive
- For increased virus protection
- For optional password protection
- To solve problems with the current version
- To provide a security patch

Viruses can infect the BIOS/UEFI, so you should keep the BIOS write-protected until you need to update it. The following procedure is one example of how to flash the BIOS/UEFI:

Step 1. After the system BIOS/UEFI upgrade is downloaded from the internet, execute the update by double-clicking on the filename.

Step 2. Follow the directions on the screen or from the manufacturer.

Step 3. Reboot the computer.

At times, you might need to reset the BIOS. There are four common ways to do this: Use the CMOS jumper, use the CMOS reset button, remove the CMOS battery, or use the BIOS/UEFI setting to reset to factory defaults. A **jumper** is a small piece of plastic that fits over pins. A jumper can be used to enable or disable a particular feature. Figure 4.7 shows an enlarged jumper and a CMOS password jumper. Figure 4.8 shows a CMOS reset button.

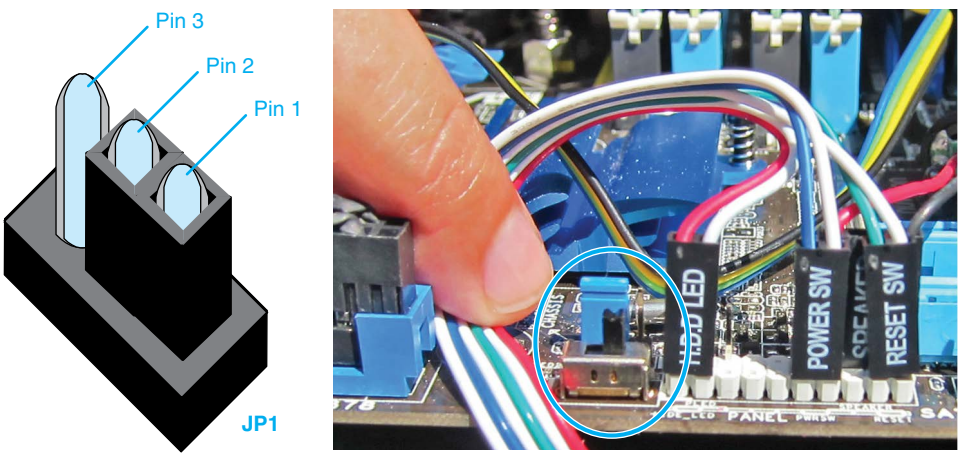


FIGURE 4.7 JP1 jumper block with pins 1 and 2 jumpered together and a CMOS password jumper

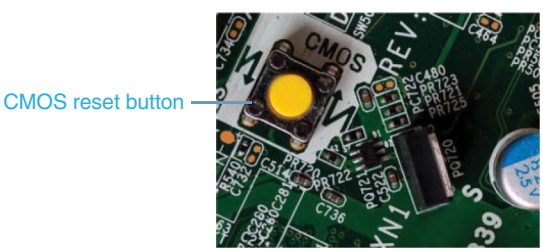


FIGURE 4.8 A CMOS reset button

TECH TIP

Don't clear CMOS after a BIOS/UEFI update

Do not clear the CMOS immediately after upgrading the BIOS/UEFI. Power down the system and then power it back on before clearing CMOS data.

If flashing a laptop's BIOS/UEFI, ensure that the laptop battery is fully charged or, better yet, connect the laptop to AC power. If the BIOS is downloaded (and not saved locally), connect the laptop to a wired network to do the download to ensure connectivity during the download process.

Keep in mind that not all vendors provide a method of recovering a BIOS/UEFI if a flash update does not go well. A computer without an operational BIOS/UEFI cannot boot, and a new motherboard must be purchased. You should therefore have a good reason for flashing the BIOS/UEFI and research the backup method the motherboard uses before flashing the BIOS/UEFI.

Configuration problems can also be associated with specific BIOS/UEFI settings. Table 4.2 lists some problems and how you might be able to solve them.

TABLE 4.2 Troubleshooting BIOS/UEFI-related issues

Issue	Things to try
Message appears stating that the date and time are not set, the clock is not set, press a specific key to continue, or all saved BIOS/UEFI settings are lost.	Replace the motherboard CMOS battery.
Bootable device not found message appears.	Check the BIOS/UEFI boot order setting and check the cabling and the drive/SSD.
Cannot configure a system for virtualization.	Enable virtualization in BIOS/UEFI.
Attached device does not work.	If the device connects to a motherboard port, ensure that the port is not disabled in BIOS/UEFI and the device connects to the correct port. If the device connects to a port on an adapter, disable the integrated port in BIOS.
System locks up sporadically.	If overclocking, put the system back to its original settings.
System is slow to boot or there are boot issues.	Check the BIOS/UEFI boot order setting.

Other Configuration Parameters

Other possible parameters contained in and set via the Setup program or operating system are interrupt requests (IRQs), input/output (I/O) addresses, direct memory access (DMA) channels, and memory addresses. These parameters are assigned to adapters and ports. No matter how the parameters are assigned, collectively they are known as **system resources**. Let's take a look at IRQs, I/O addresses, and memory addresses. Table 4.3 briefly describes these resources.

TABLE 4.3 System resources

Type	Description
IRQ	A number assigned to an adapter, a port, or a device so that orderly communication can occur between it and the processor. For example, when a key is pressed at the same time the mouse is moved, the keyboard has the highest priority because of its IRQ number.
I/O address	A unique address (think mailbox number), in hexadecimal, that allows the CPU to exchange data with another part. An example of an I/O address is 390h. Hexadecimal includes the numbers 0, 1, 2, 3, 4, 5, 6, 7, 8, and 9, as well as the letters A, B, C, D, E, and F.
Memory address	A unique address assigned to a memory chip installed anywhere in the system. The CPU uses memory addresses when it accesses information inside the memory chip.

Using Device Manager to See Resources

Adapter and device interrupts are viewed and set by using Device Manager in Windows or using various Control Panels. Technicians need to know how to use **Device Manager**, which shows the status of installed hardware. Here are the various ways to access Device Manager:

- Type `devmgmt.msc` at a command prompt or in a search textbox.
- Type `device manager` in the search textbox on the taskbar.
- Select *Settings* > type `device manager` in the *Find a setting* search textbox.
- Select the *Devices and Printers* Control Panel > *Device Manager* link.
- Select the *System and Security* Control Panel > *Administrative Tools* (Windows 10)/*Windows Tools* (Windows 11) > *Computer Management* > *Device Manager*.
- Right-click the *Start* button > *Device Manager*.

Within Device Manager, select *View* > *Resources by Type* and expand the *Interrupt request (IRQ)* section. Some interrupts have multiple entries. Multiple entries do not always indicate a resource conflict; they are allowed because devices may share IRQs.

In order to access specifics in Device Manager, use the *View* > *Devices by Type* option. Then expand any specific section, such as *Network Adapters*, right-click on a particular device or adapter, and select *Properties*. Figure 4.9 shows an integrated network card's properties, with the Change Setting button grayed out, which means these settings cannot be changed through Device Manager. (However, it might be possible to modify properties through the system BIOS/UEFI Setup program.) See Figure 4.10 for an example of memory addresses in Device Manager.

TECH TIP

How IRQs are assigned to multiple-device ports

Ports such as USB that support multiple devices require only one interrupt per port. For example, a single USB port can support up to 127 devices but needs only one IRQ for however many devices connect to a USB hub.

TECH TIP

What to do when a conflict occurs

If you suspect a resource conflict with a card, reboot the computer. The BIOS/UEFI and operating system will try to work things out. This may take multiple reboots. In addition, if an adapter is installed, moving it to another slot can resolve the situation.

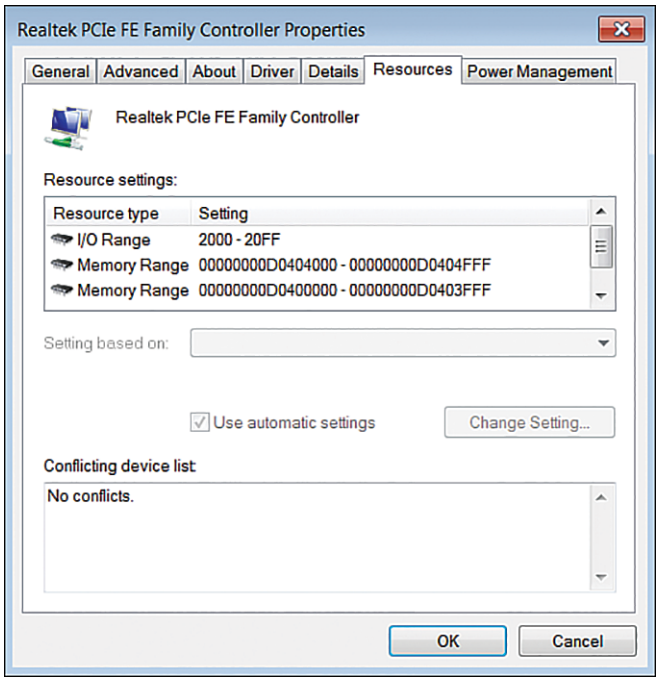


FIGURE 4.9 Resources tab in Device Manager

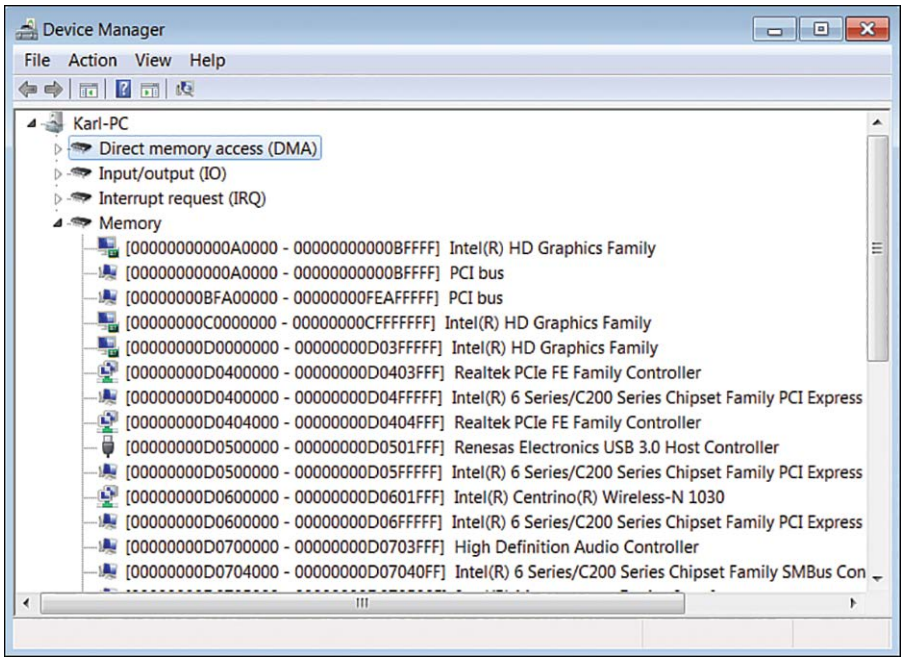


FIGURE 4.10 Memory addresses in Device Manager

Hardware Configuration Overview

Configuration of adapters and other hardware is easy if you follow the documentation and know how to obtain device drivers. Documentation for installation is frequently available on the internet, as are many device drivers. Some device drivers are provided as part of the Windows update process.

The system BIOS/UEFI plays an important role in the startup routine. Not only does it check hardware for errors as part of POST, it also detects installed adapters and devices. The BIOS/UEFI, along with the operating system, determines what resources to assign to a device or an adapter.

This information is stored in a part of CMOS known as the Extended System Configuration Data (**ESCD**) area. After the information is configured in the ESCD area, the information stays there and does not have to be recomputed unless another device is added.

After resources are allocated, the BIOS looks in the saved settings of CMOS to determine which device it should look to first for an operating system. If the BIOS/UEFI cannot locate an operating system in the first location specified in the saved settings, it tries the second device and continues on, looking to each device specified in the saved settings for an operating system. When an operating system is found, the operating system loads.

Installing Drivers

When installing hardware or an adapter in the Windows environment, a driver is required. Remember that a driver is software that allows the operating system to control hardware. The operating system detects the adapter or hardware installation and adds the device's configuration information to the registry. The **registry** is a central database in Windows that holds hardware information and other data. All software applications access the registry for configuration information instead of going to the adapter.

Windows comes with many drivers for common devices such as keyboards, mice, printers, and displays. Here are some processes used to install a driver:

- You might be prompted to install or search for a driver as part of the device installation process. You may have to designate where the driver is located, such as on media that comes with the hardware. You might also be required to download it and designate where the downloaded file is located.
- Use Device Manager to install a driver. Open *Device Manager* > expand the relevant particular hardware category > right-click the device > *Update Driver Software*, as shown in Figure 4.11.
- Use File Explorer to locate an executable file that comes with the hardware. Double-click on the Setup file provided to install software and/or a driver.
- Use the *Add Devices* link.
- Use the Add Hardware Wizard by typing `hdwwiz` in the Windows search textbox.

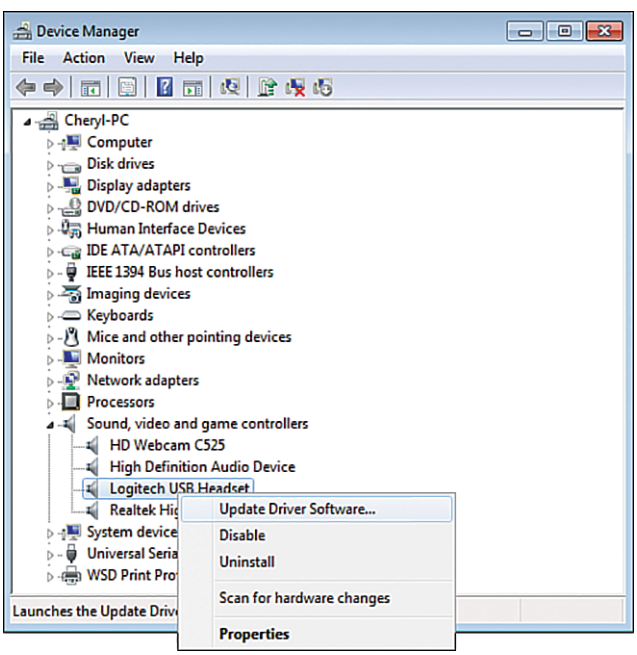


FIGURE 4.11 Update Driver Software option in Device Manager

Installing a USB Device

To install a USB device, perform the following steps:

Step 1. Power on the computer.

Step 2. Optionally, install the USB device's software. Note that some manufacturers require that software and/or device drivers be installed before the USB device is attached.

Step 3. Optionally, power on the device. Not all USB devices have external power adapters or a power button because they receive power from the USB bus.

Step 4. Locate a USB port on the rear or front of the computer or on a USB hub. Plug the USB device into a free port. The operating system normally detects the USB device and loads the device driver. You may have to browse to the driver.

Step 5. Verify installation in Device Manager.

TECH TIP

Ignoring a manufacturer's advice gets you in trouble

If a manufacturer recommends installing the device driver before attaching the USB device, follow the instructions! Failure to do so may require uninstallation of the driver and then reinstallation using recommended procedures in order for the device to work properly.

Installing/Configuring USB Cards

Additional USB ports can be added by using a USB hub or connecting a **USB expansion card**, which is a metal plate that has additional USB ports that connect to motherboard pins called a **USB header**. The plate inserts where an expansion card goes, but it does not have connectors that fit into an expansion slot. The metal plate simply slides into the spot where a card would normally go. Figure 4.12 shows one of these plates; this one has two USB ports and an eSATA port. Figure 4.13 shows the motherboard USB headers where the cables from the USB bracket would attach. You can also review Figure 2.12 to see how to attach the cables to the motherboard.

FIGURE 4.12 USB and eSATA bracket/ports that connect to motherboard pins

Keep in mind that if a motherboard does not have any pins, you can add more USB ports by purchasing a PCI or PCIe USB adapter with multiple ports. An adapter might not have the capability of providing power; you know it does if a power cable from the power supply can be attached to the card.

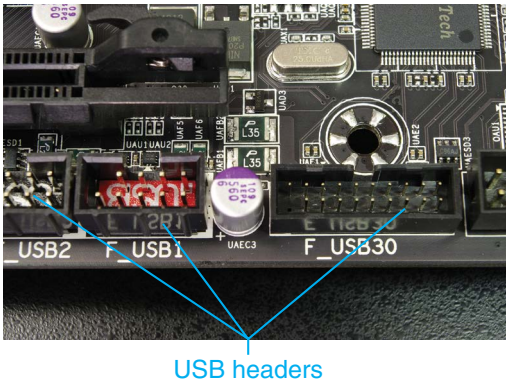


FIGURE 4.13 USB motherboard header pins

It is possible to install a USB card to add additional USB ports to a computer. USB ports are powered; therefore, a USB card normally has a place to connect power. If the power supply does not have the appropriate power connector, a power adapter may have to be purchased. Generic instructions for installing a USB card follow:

Step 1. Power down the computer and remove the power cord.

Step 2. Remove the computer cover. Locate an empty expansion slot. You may have to remove a screw or raise a retaining bar to be able to use the expansion slot (see Figure 4.14).

Step 3. Using proper antistatic procedures (see Chapter 5, "Disassembly and Power"), ground yourself or use antistatic gloves.

Step 4. Add a cable to the motherboard if using a USB bracket. Optionally, attach a power connector to the adapter.

Step 5. Ensure that the proper expansion slot is being used and insert the card firmly into the slot (see Figure 4.15). Ensure that the card is fully inserted by firmly pressing down on the adapter and visually inspecting it afterward. The card should be at a 90-degree angle from the PC. It should not tilt at either end. Ensure that the card fits snuggly in the expansion slot.

Step 6. Lower the expansion bar or attach a screw, if needed.

Step 7. Reinstall the computer cover, reattach the power cord, and power on the computer. Install drivers as necessary.

Step 8. Test by attaching a USB device to each port.

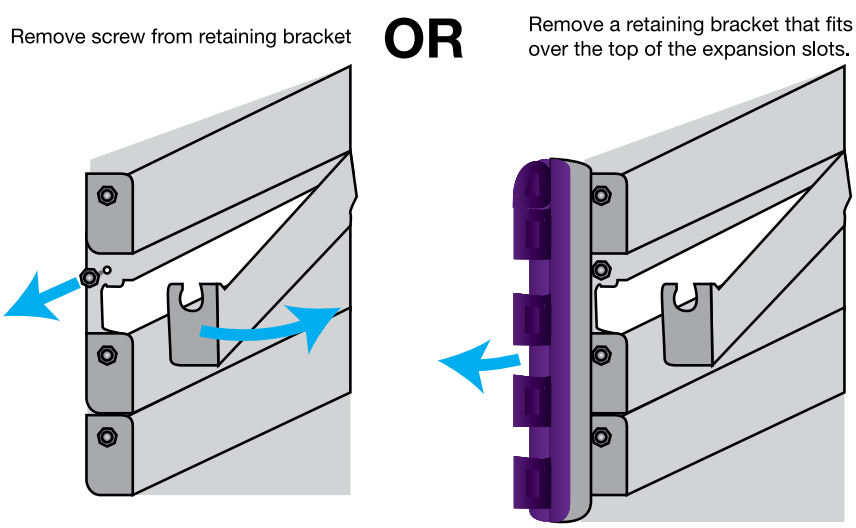


FIGURE 4.14 Adapter screw or retainer bar

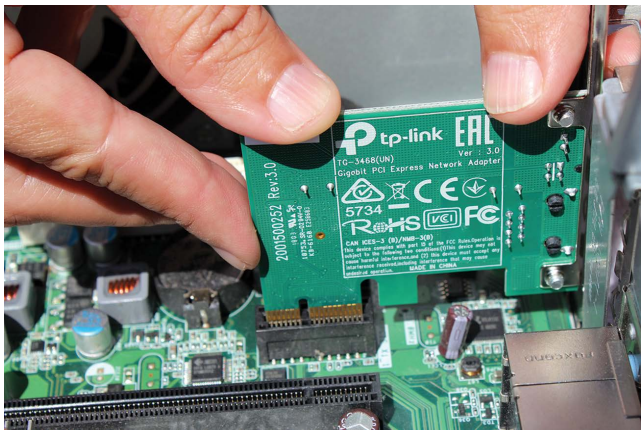


FIGURE 4.15 Inserting an adapter directly into an expansion slot

Troubleshooting USB

To troubleshoot USB device problems, check the obvious first: the cabling and power. Verify whether any USB device that plugs into a USB hub works. If no devices work, swap the hub or attach it to a different USB port. If some hub ports work and some do not, attach an external power source to the hub, change its configuration if necessary, and retest the devices. Restart the computer and retest the USB device.

USB ports can provide power at different levels, such as 2A at 5V (10W), 5A at 12V (60W), and 5A at 20V (100W). Not all USB-C cables can provide 100W power. Ensure that you are using a 5A-rated USB-C to USB-C cable.

You can verify how much power a USB device is consuming by using external software like USBDeview. You can view the power state with Device Manager by using these steps.

Step 1. Expand the *Universal Serial Bus Hub Controllers* section.

Step 2. Right-click on each *Generic USB Hub* option and select *Properties*.

Step 3. Access the *Details* tab and use the *Property* drop-down arrow to select *Power data*.

Step 4. In the *Current power state* section, notice the D0 through D3 states. A D0 state is a fully on state, and D3 is the lowest power state (sleep mode even, if it has devices attached).

A USB device could be drawing more power than is allowed. If this is the case, the computer can disable the port. The only way to re-enable the port is to restart the computer. If a device is using less than 50mA of power, the USB port never becomes active. Try plugging the USB device into a different USB port or verifying that the device works on another computer.

Windows has the ability to allow (the default setting) or disallow the computer to shut off the USB port/hub to save power. See the *Properties* > *Power Management* tab for the USB hub.

A USB device requires a driver that may be loaded automatically. An incorrect or outdated driver could cause problems. The following list can help when troubleshooting USB devices:

- Use Device Manager to ensure that a hub is functioning properly.
- Ensure that the BIOS/UEFI firmware is up-to-date.
- Use Device Manager to ensure that no USB device has an IRQ assigned and shared with a non-USB device.
- USB devices sometimes do not work in Safe Mode and require hardware support configured through the BIOS/UEFI.
- Sometimes a USB device stops working on a hub that has an external power source. In such a case, remove the hub's external power source and retest.

- If a self-powered USB hub gets its power disconnected, the hub becomes a bus-powered hub and outputs only lower power on each port. Reattach the power cord or remove the hub and then reattach it.
- If a newly attached USB device reports that it is attached but does not work properly, upgrade the driver.
- Do not connect USB devices to a computer that is in standby mode or sleep mode. Doing so may prevent the computer from coming out of standby mode.
- For intermittent USB device problems, disable power management to see if doing so solves the problem.
- Test a device connected to a USB hub by connecting it directly to a USB port that has nothing else attached. The problem may be caused by other USB devices or a USB hub.
- Remove the USB device's driver and reinstall it. Sometimes you must reboot the computer to give the new drivers priority over the general-purpose drivers.
- If a USB device is running slowly, try attaching it to a different port that has fewer devices connected to the same port.
- Verify that the USB port is enabled in BIOS/UEFI if it is integrated into the motherboard or attached to the motherboard through an adapter cable.
- Refer to the USB device manufacturer's website for specific troubleshooting details.

Installing an eSATA Card

A Serial ATA (SATA) port allows connection of a SATA storage device such as an internal hard drive or an optical drive. External SATA (eSATA) ports allow connectivity of storage devices outside the computer or laptop. If a computer has no eSATA ports or does not have enough of them, you have two options. The first option is to install an **eSATA bracket**, as shown in Figure 4.16. Notice that SATA cables are simply attached to the backs of the ports. Each SATA cable attaches to a port on the motherboard. For the bracket shown in the figure, the motherboard needs to have two available SATA ports in order to have two external ports.

FIGURE 4.16 eSATA bracket with cables

The second option is to install a PCIe **eSATA card**, as shown in Figure 4.17. This card allows you to connect both internal and external SATA drives. It commonly has at least two ports: one for connecting internal drives using standard SATA cables and another for connecting external eSATA devices. You could attach a SATA cable from the top of this card to an internal device or attach an eSATA cable from one of the external ports to an external eSATA device.

To install an eSATA card or bracket, perform the following steps:

Step 1. Power off the computer and unplug it.

Step 2. Remove the computer cover and locate an unused expansion slot. You may have to remove a screw or raise a retaining bar to be able to use the expansion slot.

Step 3. Remove the slot cover.

Step 4. Using proper antistatic procedures (see Chapter 5), ground yourself or use antistatic gloves.

Step 5. Ensure that the proper expansion slot is being used. Insert the card firmly into the expansion slot. If only a bracket is being used, insert the bracket between the motherboard and the back of the case where there is an empty expansion slot.

Step 6. Lower the expansion bar or attach a screw to keep the card or bracket firmly in place.

Step 7. If a bracket is being used, attach each SATA cable to an available SATA motherboard port. Make note of which SATA port is being used as each one may need to be enabled within BIOS/UEFI.

Step 8. Reinstall the computer cover, reattach the power cord, and power on the computer. Go into BIOS/UEFI and enable the appropriate SATA ports as necessary. Install any software that came with the card.

Step 9. Test by attaching an eSATA device to each port.

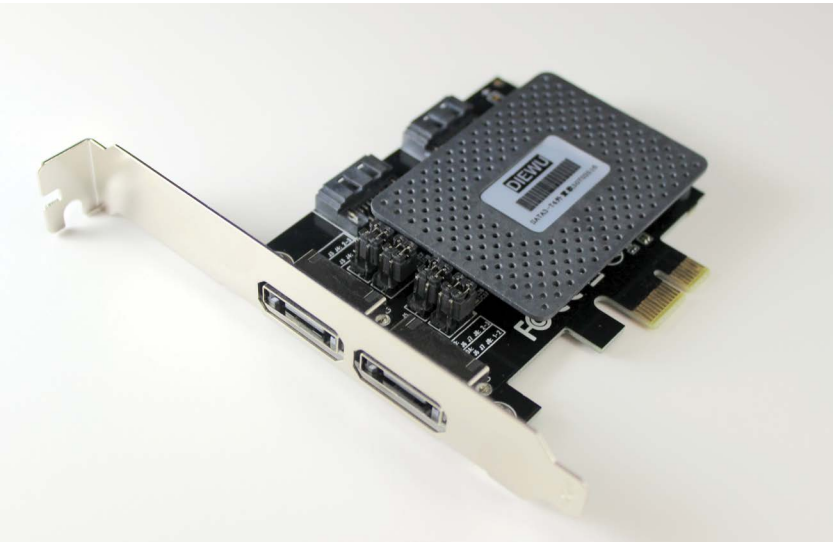


FIGURE 4.17 eSATA PCIe card

Installing a Network Interface Card

Almost every device that connects to a wired or wireless network does so by using a network interface card (**NIC**). Many devices have wired and wireless NICs built in, but if such a NIC fails, a new NIC must be installed, such as the Ethernet NIC shown in Figure 4.18.

You must take several steps as part of the installation process before connecting to the network:

Step 1. Power off the computer and unplug it.

Step 2. Remove the computer cover and locate an unused expansion slot. Remove the slot cover.

Step 3. Ground yourself and ensure that the proper expansion slot is being used. Insert the card firmly into the expansion slot. Secure the card.

Step 4. Reinstall the computer cover, reattach power, and power on the computer. Download and install the latest driver.

Step 5. Give the computer a unique name and optionally join a workgroup or domain.

Step 6. Configure TCP/IP addressing information, as described in Chapter 13, “Networking.”

FIGURE 4.18 Ethernet network interface card

Troubleshooting Configurations

The following are possible indications that a device is not working:

- A new device is installed and the new device or a previously installed device does not work.
- The computer locks up or restarts when performing a specific function, such as when playing or recording audio.
- The computer hangs during startup or shutdown.
- A device does not work properly or fails to work at all.

TECH TIP

Verifying hardware with Device Manager

A small down arrow by a device's icon in Device Manager means the device is disabled, and an exclamation point (!) on a yellow field usually indicates a resource conflict or driver problem. An "i" indicates that the Use Automatic Settings feature is not being used for the device, and resources were manually configured.

In Device Manager, if an exclamation point (!) appears, the hardware device is not working properly, and you should check for cabling issues, resource conflicts, and configuration issues. With any Device Manager issue, you can right-click the device and select *Properties*. Look at the *General* tab to see if there are error codes. If a yellow question mark appears, Windows does not recognize the device, and you can try one of the following:

- Perform a Windows update to ensure that you have the latest drivers, security updates, and fixes.
- Manually update the driver by right-clicking the device in *Device Manager* and selecting *Properties* > *Driver* tab > *Update Driver*. You can download the driver from the device manufacturer's website or let Windows try to find the driver.

TECH TIP

Using the General tab for troubleshooting

On the *General* tab of the Properties dialog for any adapter or port, check the *Device Status* section for any error codes, including those for resource conflicts.

SOFT SKILLS: A GOOD TECHNICIAN PRACTICE: CHANGE ONLY ONE THING AT A TIME AND DOCUMENT

The least effective type of computer technician is a "gun slinger." The term *gun slinger* brings to mind images of Wild West ruffians who had shooting matches with other gangsters in the town's main street. Gun slingers drew their guns frequently and with little provocation. They did not put much thought into their method or consider other possible resolutions. You must strive *not* to be this type of technician.

A gun slinger technician changes multiple things simultaneously. For example, if there is no display on the output, the technician might swap out the monitor, disable the onboard video port, add a new video adapter, power on the computer, and, when output appears, call the problem "solved." If a computer problem is repaired using such a technique, the technician never knows exactly what solved the problem. A gun slinger technician might get frustrated easily because it is easy to forget what has been tried when multiple things have been tried simultaneously—and it is almost impossible to know which one worked (see Figure 4.19).

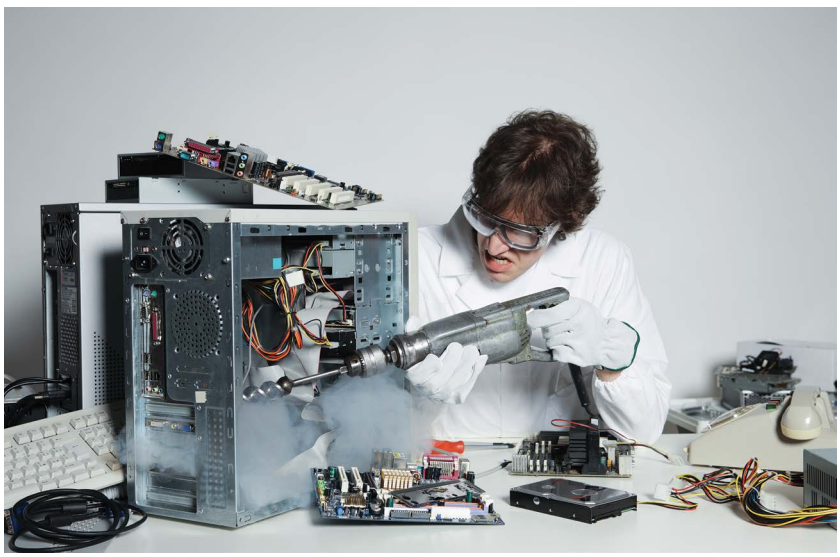


FIGURE 4.19 A gun slinger technician in action

A good technician, on the other hand, makes a list of symptoms (even if it is simply a mental list) followed by a list of things to try. Then the technician tries the possible solutions, starting with the simplest one (the one that costs the least amount of time for the computer user). The technician documents each step. After each approach that does not fix the problem, the technician puts the system back to the original configuration before attempting the next possible solution. This method keeps the technician focused on what has been tested, and if another technician takes over, the steps do not have to be repeated. Best of all, when one of the possible solutions fixes the problem, the exact solution is known.

Gun slinger technicians do not learn as quickly as other technicians because they do not determine the real causes of problems. Each time they are presented with a problem similar to one they have seen in the past, gun slinger technicians use the same haphazard troubleshooting method. These technicians are actually dangerous to an organization because they are not good at documenting what they have done and determining exactly what fixes a particular problem. A good computer technician should methodically troubleshoot a problem by making only one change at a time and reverting the change if the change does not solve the problem. Furthermore, the technician needs to document the issue and its resolution for future problems.

Chapter Summary

- The BIOS/UEFI is used to enable/disable, configure, and troubleshoot motherboard components, expansion slots, and ports, and it sets power-on and BIOS/UEFI passwords.
- An updated type of BIOS is BIOS/UEFI, which allows the use of a mouse and a graphical environment. Security options, support for larger hard drives, antivirus software, remote management, and utilities may also be included.
- When a computer is off, a motherboard battery holds saved settings in CMOS. If the computer does not keep the date and time, replace the battery.
- The TPM chip can be enabled or cleared through UEFI. Note that if you clear the TPM chip, all digital security certificates, passwords, and encrypted data are loss. Consider disabling it instead.
- Each port and card uses system resources such as interrupts, I/O addresses, and memory addresses.
- You can use Device Manager to view and change system resources. You can also use Device Manager to see whether a device is working properly.
- A USB, eSATA card or bracket, or NIC can be added to a computer to provide additional ports.

A+ CERTIFICATION EXAM TIPS

- ✓ A lot of questions from both exams can come from this chapter, especially in the troubleshooting areas. Review the troubleshooting bullets and tech tips. Research issues on the internet and read people's postings. Their stories and frustrations (and successes) will stick in your mind and help you with the exam.
- ✓ Using at least one computer, go through the BIOS/UEFI menus. Review what types of things can be configured through BIOS/UEFI. Important settings include the following: boot options, USB settings (including permissions and the ability to disable the ports), fan options/considerations, security settings (such as Secure Boot and boot and BIOS passwords), temperature monitoring, and TPM.
- ✓ Be able to install and configure a network interface card (NIC) and other adapters, such as sound, video, and capture cards.
- ✓ Know what to do if a system tries to boot to an incorrect device or if the system date/time is off.

Key Terms

administrator password, BIOS, BIOS password, boot password, boot options, bootable device not found, CMOS, CMOS battery, Device Manager, drive encryption, eSATA bracket, eSATA card, ESCD, fan considerations, fan control, flash BIOS, I/O address, inaccurate system date/time, IRQ, jumper, LoJack, memory address, NIC, Passwords, POST, registry, Secure Boot, Setup, system resources, temperature monitoring, TPM, UEFI, USB expansion card, USB header, USB permissions, Virtualization Support

Review Questions

1. When would a technician flash a BIOS/UEFI?
   - **a.** When the date and time start to be incorrect
   - **b.** When a port or motherboard component does not perform at its maximum potential
   - **c.** When the driver for a motherboard port is out of date
   - **d.** When the motherboard battery fails
2. What is the effect of setting an administrator password in BIOS/UEFI?
   - **a.** It prevents the computer from having multiple devices that can boot the system.
   - **b.** It prevents the BIOS/UEFI from being infected with a virus.
   - **c.** It prevents a user from accessing the computer operating system.
   - **d.** It prevents a user from changing system Setup settings.
3. Which program is used to determine the driver version being used for a card installed in a computer?

   [BIOS | CMOS | Task Manager | Device Manager | system Setup]
4. Which program is commonly used to verify that a new piece of hardware is recognized by the operating system, functions, and the system resources assigned?

   [BIOS/UEFI | CMOS | manufacturer-provided application | Device Manager]
5. Where would a CR2032 lithium battery most likely be used in a tower PC?
   - **a.** As a laptop battery
   - **b.** Inside the processor
   - **c.** On the motherboard
   - **d.** In the CMOS
6. Which BIOS/UEFI option might need to be modified in order to boot a Windows computer from a flash drive that contains Ubuntu, a Linux-based operating system?

   [LoJack | Secure Boot | Virus Protection | USB Configuration | Hyper-Threading]
7. What is a TPM?
   - **a.** A method of sharing resources between adapters
   - **b.** A physical module that stores passwords and digital certificates
   - **c.** The technique used by a USB hub when multiple devices are attached to it
   - **d.** A type of lithium battery used to keep current Setup configuration data
8. A technician is looking at a used computer that was recently purchased by someone. The computer is requesting a password before the operating system loads. What can the technician do to remove the password?
   - **a.** Press the key to enter BIOS.
   - **b.** Press the F8 key as the computer boots.
   - **c.** Remove the CMOS battery for a minute and then reinstall it.
   - **d.** Hold down the power button for 10 seconds as the computer is booting.
9. Which tab of a device's Properties dialog has a *Device Status* section that might contain helpful troubleshooting information or the status of the device?

   [General | Advanced | Driver | Details | Management]

10. A technician receives a complaint about a computer being slow to respond to typed keystrokes. The technician installs more memory and a new keyboard. The customer is happy. What, if anything, could have been done better?

_____

_____

_____

11. What is the maximum wattage that can be provided by a USB port?

[100 | 5 | 2.5 | 4.5]

Consider the following BIOS/UEFI configuration menu options when answering Questions 12–15.

Main menu	Onboard Devices menu	Boot Device Priority menu
BIOS information	PCIe	1st boot device
BIOS version	LAN1 controller	2nd boot device
Build date	USB 2.0 controller	3rd boot device
EC F/W version	USB 3.0 controller	4th boot device
CPU information	Audio	
Memory information	OnChip SATA controller	
System information	SATA	
System language	HDMI/DVI	
System date		
System time		

12. Which menu would you use to determine whether the system should be flashed?

a. Main menu

b. Onboard Devices menu

c. Boot Device Priority menu

13. A computer is mounted inside a cabinet, and you want to know if the USB 3.0 port has been disabled. Which menu would you use?

a. Main menu

b. Onboard Devices menu

c. Boot Device Priority menu

14. Which menu would you use to determine whether the particular SATA port you used to connect to an eSATA bracket is enabled?

a. Main menu

b. Onboard Devices menu

c. Boot Device Priority menu

15. A technician wants to boot from an eSATA external hard drive. Which submenu item should she use?

[OnChip SATA controller | SATA | CPU information | 1st boot device]

16. A technician keeps having to configure the date and time. What component is suspect?

[CPU | BIOS/UEFI | CMOS battery | chipset]

17. What are three ways to get more USB ports? (Choose three.)
    a. Connect a USB hub to an existing USB port.
    b. Connect a network hub to an existing USB port.
    c. Install a PCIe adapter that has USB ports.
    d. Install an AGP adapter that has USB ports.
    e. Install a USB bracket that has USB ports and attaches to motherboard pins.
    f. Use a USB port multiplexer.
18. When would a technician use UEFI?
    a. When managing configuration through Device Manager
    b. When the date and/or time continues to be wrong
    c. When an adapter has just been installed
    d. When replacing a motherboard
19. A computer is being used in a medical office. For security reasons, the technician has been asked to reasonably ensure that no one attaches any external media. What would the technician probably do?
    a. Password protect the BIOS/UEFI and disable unused ports.
    b. Swap out the motherboard for one that doesn't have extra ports.
    c. Assign user rights through user passwords on the computer.
    d. Encrypt the hard drive.
    e. Flash the chipset.
20. A technician for a small company set a BIOS/UEFI password on every computer. The technician leaves the company, and the replacement technician needs to access the BIOS/UEFI. What should the new technician do?

    _____

    _____

    _____

Exercises

Exercise 4.1 System Expansion

Objective: To be able to explore different ways to expand a system

Parts: None

Procedure: Use the documentation in Table 4.4 to answer the questions.

TABLE 4.4 Motherboard specifications

Component	Description
CPU	Support for Intel Celeron, Core i3, and Core i5
Chipset	Intel B150 Express
Memory	2 DDR4 DIMM sockets supporting up to 32 GB Dual-channel support Support for DDR4 2133 MHz
Onboard graphics	Integrated graphics processor 2 HDMI ports Maximum 512 MB shared memory

Component	Description
Audio	Realtek ALC887 codec 2/4/5.1/7.1 channel Support for S/PDIF out
LAN	2 Intel GbE LAN chips that support 10/100/1000 Mb/s
Expansion slots	1 PCIe 3.0 x16 slot 1 M.2 Socket 1 connector for wireless module
USB	Chipset: > 4 USB 2.0/1.1 ports (2 on back and 2 through the internal USB header) > 6 USB 3.0/2.0 ports (4 on back and 2 ports through the internal USB header)
Internal connectors	1 24-pin ATX main power connector 1 4-pin ATX 12V power connector 6 SATA 6 Gb/s connectors 1 M.2 Socket 3 connector 1 CPU fan header 1 system fan headers 1 front panel header 1 front panel audio header 1 USB 3.0/2.0 header 1 USB 2.0/1.1 header 4 serial port headers 1 S/PDIF out header 1 speaker header 1 clear CMOS jumper
Back panel connectors	2 USB 2.0/1.1 ports 1 PS/2 keyboard/mouse port 2 Wi-Fi antenna connectors 2 HDMI ports 4 USB 3.0/2.0 ports 2 RJ45 ports 6 audio jacks

1. The computer that uses this motherboard has one SATA hard drive attached. The person who owns this computer wants to use an eSATA drive.

   Based on the documentation given, can the user attach an eSATA drive to the computer as it is configured now?

   [Yes | No]

2. The technician wants to use an eSATA bracket that has two eSATA ports/cables in addition to one internal SATA device.

   Does the motherboard support this? Explain how you know.

   _____

   _____

3. The user who owns the computer does not like to use USB hubs.

   What is the maximum number of devices the user can connect to the back of the computer without using USB hubs? What advice might you give the user regarding these ports?

   _____

   _____

   _____

   _____

   _____

4. The user wants additional USB ports on the back of the computer. The technician would like to use a USB bracket to provide two additional ports.

   Based on the documentation, can a USB bracket be used with this motherboard? How can you tell? Be specific.

   _____

   _____

Exercise 4.2 BIOS/UEFI Options

Objective: Use information found on the BIOS/UEFI screen to determine which option to use

Parts: None

Procedure: Use Figures 4.20 and 4.21 to answer the questions.

Use Figure 4.20 to answer Questions 1–5.

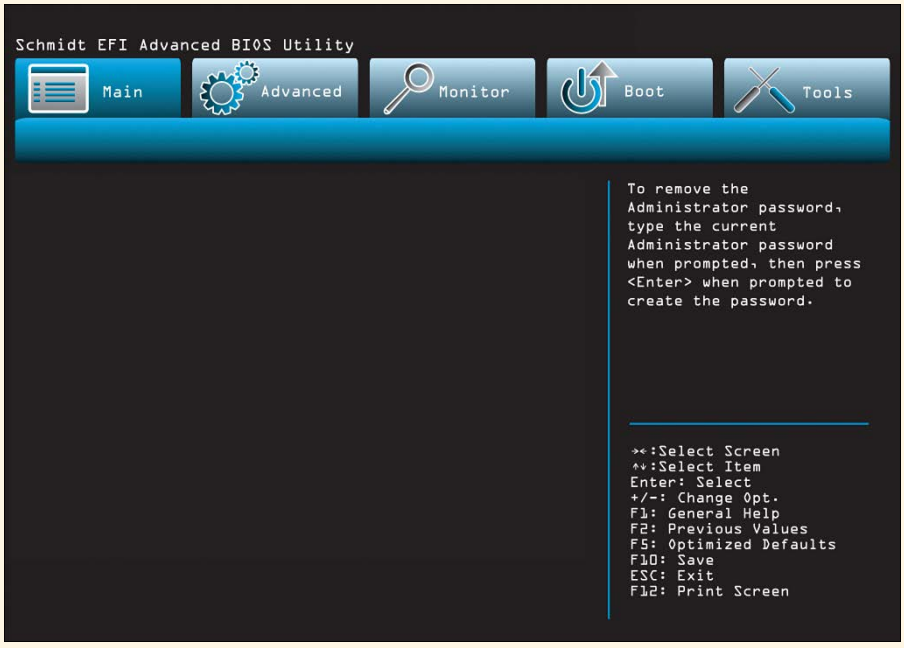


FIGURE 4.20 Sample BIOS/UEFI window 1

1. The user has modified BIOS/UEFI options to the point where half the ports don't work and the computer is running slowly.

   Which menu option or keystroke should the technician use in order to solve this problem?

   _____

2. The technician has modified some settings but now wants to research some alternatives and doesn't want to keep the settings he just changed.

   Which menu option or keystroke should the technician use in this situation?

   _____

3. The computers in the research lab have to have extra security. A technician configuring a new computer for that lab is using the BIOS/UEFI to disable all USB ports on the front and rear panels.

   Which menu option is used to complete this task?

   [Main | Advanced | Monitor | Boot | Tools]

4. The technician wants to see the last time anyone opened the case.

   Which menu option is used to complete this task?

   [Main | Advanced | Monitor | Boot | Tools]

5. The user has complained that the system takes too long to boot. One thing a prior technician did was to always have the system try to boot from an external drive used to reimage the computer. If the external drive wasn't found, then it used the internal hard drive to load the operating system.

   Which menu option should the new technician use to change the system to use the internal hard drive to load the operating system as the computer's first choice?

   [Main | Advanced | Monitor | Boot | Tools]

Use Figure 4.21 to answer Questions 6–10.

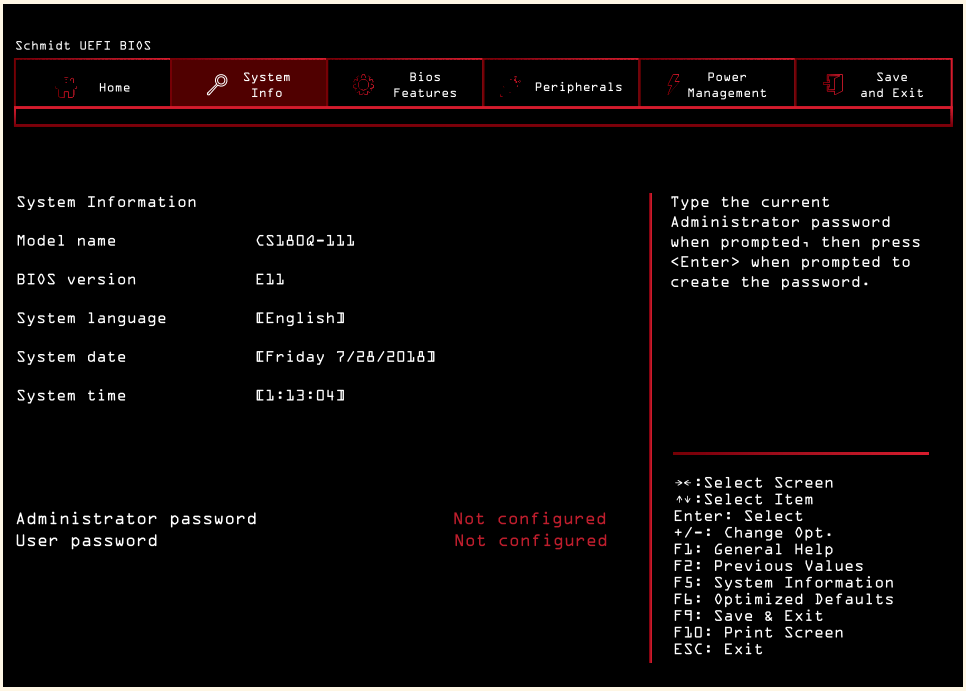


FIGURE 4.21 Sample BIOS/UEFI window 2

6. The technician wants to stop the user from changing BIOS/UEFI settings.

   Which menu option or keystroke should the technician use in order to set a BIOS/UEFI administrator password?

   [Home | System Info | Peripherals | Power Management]

7. A week ago, a user complained about the computer time being wrong. The technician changed the time and date. Now the user has complained again that the date and time are incorrect.

   If the technician changes the time again and checks the computer the next day and finds it off again, what should the technician do?

   a. Flash the BIOS/UEFI.

   b. Replace the motherboard.

   c. Replace the motherboard battery.

   d. Reset the time a third time.

8. A gamer has been adjusting timing features on this motherboard to make the system go faster.

   Which keystroke could the user use in order to take a screenshot of the current settings?

   _____

9. The technician has been modifying BIOS/UEFI settings.

   What keystroke should the technician use when exiting the Setup screen?

   _____

10. The technician wants to enable two SATA ports so a two-port eSATA bracket can be cabled to the motherboard.

    Which menu option should the technician use to ensure that the two SATA ports are enabled?

    [Home | System Info | Peripherals | Power Management]

Activities

Flip the CLASSROOM

Internet Discovery

Objective: To obtain specific information on the internet regarding a computer or its associated parts

Parts: Computer with internet access

Procedure: Use the internet to answer the following questions.

Questions:

1. A customer owns an ASUS M241 all-in-one computer. Determine the procedure for accessing the computer's Setup program. Write the key(s) to press and the URL where you found this information.

   _____

2. What is the latest BIOS/UEFI version for the ASUS M241 all-in-one computer? Write the URL where you found this information.

   _____

   _____

3. A Windows 10 ASUS M241 computer owner wants to know if this model has a TPM. Provide the URL where you found this information.

   _____

4. A customer owns a TYAN S7025 motherboard. How many and which type of PCIe slots does this motherboard have? Write the answer and the URL where you found the answer.

   _____

   _____

5. On the same TYAN S7025 motherboard as in Question 4, which motherboard jumper is used to clear CMOS? Write the answer and the URL where you found the information.

_____

6. On the same TYAN S7025 motherboard as in Question 4, which BIOS/UEFI menu option is used to configure the order in which the system looks for devices to boot the computer? Write the answer and the URL where you found the answer.

_____

_____

Soft Skills

Objective: To enhance and fine-tune a future technician's ability to listen, communicate in both written and oral forms, and support people who use computers in a professional manner

Activities:

1. In teams, come up with a troubleshooting scenario that involves a computer technician who uses gun slinging techniques and the same scenario involving a technician who is methodical. Explain what each technician type does and how each one solves the problem. Also detail how these two types of technicians treat the customer differently. Determine ways that a gun slinging technician might be harmful to a computer repair business. Either demonstrate or report on your findings.
2. After exploring the BIOS/UEFI options, turn to a fellow student, pretend they are a customer you're talking to on the phone, and walk them through accessing Setup. Explain the purposes of at least five of the options. Reverse roles and cover five other options. Be sure to act like a typical computer user when playing the customer role.
3. Brainstorm a troubleshooting scenario in which you fix a problem that involves accessing the Setup program and/or an adapter. Document the problem using a word processing application. Create an invoice using either a word processing or spreadsheet application. Share your documents with others in the class.

Critical Thinking Skills

Objective: To analyze and evaluate information as well as apply learned information to new or different situations

Activities:

1. Describe a situation where you think adding an eSATA card makes sense.

_____

_____

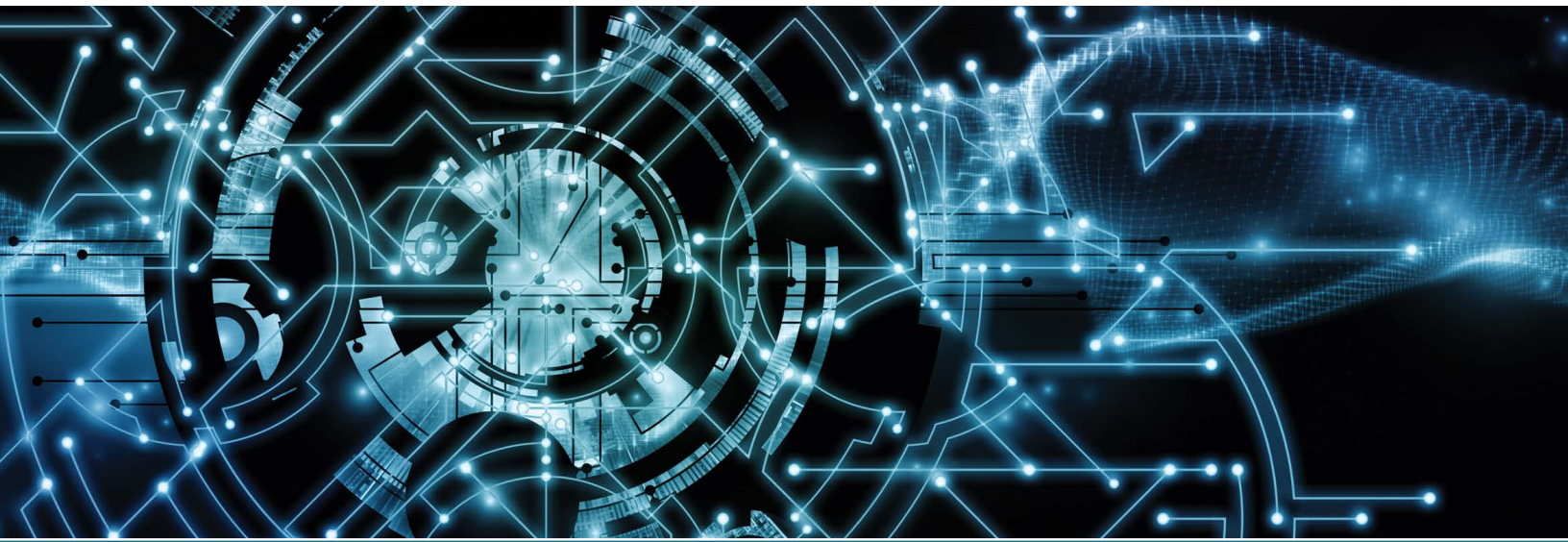
_____

2. Compare and contrast a post office with IRQs, I/O addresses, and memory addresses shown in Device Manager. For example, how might something that happens in a post office relate to an IRQ in a PC (or I/O address or memory address)?

3. Your parents have a new computer, and they see a message to press F2 to enter Setup. They do this, and they want you to explain what they are looking at.

This page intentionally left blank

5 Disassembly and Power



In this chapter you will learn:

- How to prevent static electricity, RFI, and EMI from harming or interfering with a computer
- The tools needed to work on computers
- How to take apart a computer and put it back together
- How to perform basic voltage and continuity checks
- How to install, upgrade, or replace a power supply
- Tips for good written communication

CompTIA Exam Objectives:

- ✓ 1201-3.2 Summarize basic cable types and their connectors, features, and purposes.
- ✓ 1201-3.5 Given a scenario, install and configure motherboards, central processing units (CPUs), and add-on cards.
- ✓ 1201-3.6 Given a scenario, install the appropriate power supply.
- ✓ 1201-5.1 Given a scenario, troubleshoot motherboards, RAM, CPUs, and power.
- ✓ 1202-4.4 Given a scenario, use common safety procedures.
- ✓ 1202-4.5 Summarize environmental impacts and local environment controls.
- ✓ 1202-4.7 Given a scenario, use proper communication techniques and professionalism.

Disassembly Overview

It is seldom necessary to completely disassemble a computer. However, when a technician is first learning about PCs, disassembly can be both informative and fun. A technician might disassemble a computer when it has a problem of undetermined cause or a grounding problem. An **equipment grounding** problem occurs when the motherboard or adapter is not properly installed and a trace (a metal line on the motherboard or adapter) touches the computer frame, causing the adapter and possibly other components to stop working.

Electrostatic Discharge (ESD)

You must take precautions when disassembling a computer. The electronic circuits located on the motherboard and adapters are subject to ESD. Electrostatic discharge (**ESD**) is a difference of potential between two items that causes static electricity. Static electricity can damage electronic equipment. The average person requires a static discharge of 3,000 volts before they feel it. An electronic component can be damaged with as little as 30 volts. Some electronic components might not be damaged the first time static electricity occurs. However, the effects of static electricity can be cumulative, weakening or eventually destroying a component. An ESD event is not recoverable: Nothing can be done about the damage it induces. Electronic chips and memory modules are most susceptible to ESD strikes.

TECH TIP

Atmospheric conditions affect static electricity

When humidity is low, the potential for ESD is greater than at any other time; however, too much humidity is bad for electronics. Keep humidity between 45% and 55% to reduce the threat of ESD.

A technician can prevent ESD by using a variety of methods. The most common tactic is to use an **antistatic wrist strap**, also called an **ESD strap**. An antistatic wrist strap puts the technician and the computer at the same voltage potential. As long as the technician and the computer or electronic part are at the same potential, static electricity does not occur. See Figure 5.1.

FIGURE 5.1 Antistatic wrist strap

One end of the strap encircles the technician's wrist, and the other end attaches to the computer. The clip attaches to a grounding post or a metal part of the computer case, as shown in Figure 5.2, or the power supply. The electronic symbol for ground is ⏚, and you might see this near a ground post.

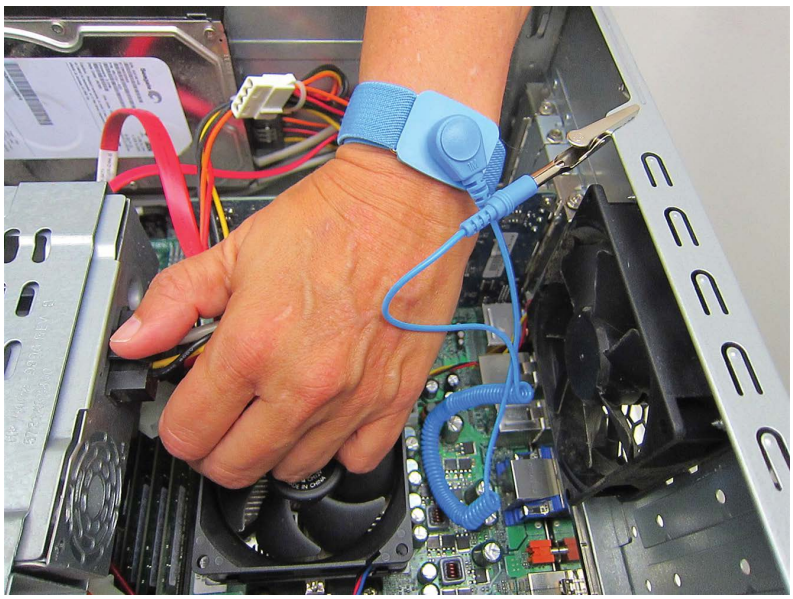


FIGURE 5.2 Where to attach an antistatic wrist strap

TECH TIP

When *not* to wear an antistatic wrist strap

A technician should not wear an ESD wrist strap when working inside a cathode ray tube (CRT) monitor or power supply because of the high voltages there. Of course, a technician should not be inside these devices unless properly trained in electronics.

Antistatic gloves (see Figure 5.3) can be used instead of an antistatic wrist strap. Laptops and other mobile devices frequently do not have good places to attach a wrist strap, and in such a case, antistatic gloves work better.

FIGURE 5.3 Antistatic gloves

Antistatic bags are good for storing spare adapters and motherboards when the parts are not in use. However, antistatic bags lose their effectiveness after a few years. Figure 5.4 shows an antistatic bag with an adapter inside it. **ESD mats** are available to place underneath a computer being repaired, and such a mat might have a snap for connecting the antistatic wrist strap.

FIGURE 5.4 Antistatic bag

If an antistatic wrist strap is not available, you can still reduce the chance of ESD damage. After removing the computer case, stay attached to an unpainted metal computer part. One such part is the power supply. If you are right-handed, place your bare left arm on the power supply. Remove the computer parts one by one, always keeping your left elbow (or some other bare part of your arm) touching the power supply. If you are left-handed, place your right arm on the power supply. By placing your elbow on the power supply, you leave both hands free to remove computer parts. This **self-grounding** method is an effective way of keeping the technician and the computer at the same voltage potential, thus reducing the chance of ESD damage. However, it is not as safe as using an antistatic wrist strap. Also, removing the power cable from the back of the computer is a good idea. A power supply provides a small amount of power to the motherboard even when the computer is powered off. Always unplug the computer and use an antistatic wrist strap when removing or replacing parts inside a computer!

TECH TIP

Good news about ESD

Electronics manufacturers are designing components that are less susceptible to ESD. However, you should still ground yourself using any means possible. Each zap weakens a component!

Electromagnetic Interference (EMI)

Electromagnetic interference (**EMI**) is noise caused by electrical devices, such as a computer, a pencil sharpener, a motor, a vacuum cleaner, an air conditioner, and fluorescent lighting. The electrical devices outside the computer case, including speakers, cause more EMI problems than the computer.

A specific type of EMI that negatively affects computers is radio frequency interference (**RFI**). RFI is simply noise that occurs in the radio frequency range. If a computer has an intermittent problem, check the surrounding devices for the source of the problem. EMI problems are very hard to track to the source. Any electronic device—even a computer or printer—can be a source of EMI or RFI. EMI can also come through power lines. Move the computer to a different wall outlet or to a totally different circuit to determine whether the power outlet is the problem source. EMI can also affect files on a hard drive.

TECH TIP

Replacing empty slot covers

To help with EMI and RFI problems, replace slot covers for expansion slots that are no longer being used. Slot covers are shown in Figure 4.14 (refer to Chapter 4, "Introduction to Configuration"). Slot covers also keep out dust and improve the airflow within the case.

Tools

No chapter on disassembly and reassembly would be complete without mentioning tools. Tools are used in removing/replacing field replaceable units (FRUs), which are parts of the computer or other electronic devices such as the power supply or motherboard.

Many technicians do not go on a repair call with a full tool case. The vast majority of all repairs are completed with the following basic tools that are shown in Figure 5.5:

- Small and medium flat-tipped screwdrivers
- #0, #1, and #2 Phillips screwdrivers
- 1/4- and 3/16-inch hex nut drivers
- Small diagonal cutters
- Needle-nose pliers

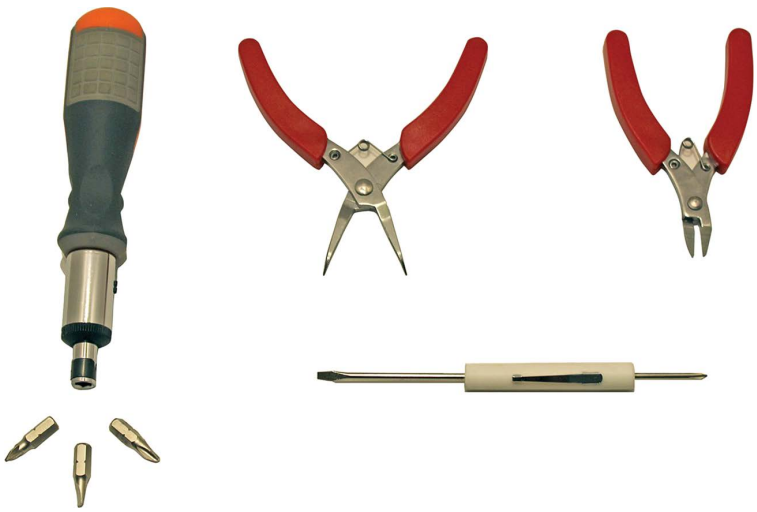


FIGURE 5.5 Basic PC technician tools

Screwdrivers take care of most disassemblies and reassemblies. Sometimes manufacturers place tie wraps on new parts, new cables, or the cables inside the computer case. Diagonal cutters are great for removing these tie wraps without cutting cables or damaging parts. Needle-nose pliers are good for straightening bent pins on cables or connectors, and they are useful for doing a million other things. Small tweaker screwdrivers and needle-nose pliers are indispensable.

TECH TIP

Getting those wayward screws

Although magnetic screwdrivers are handy for picking up dropped screws, they can affect memory, so avoid using them, if possible. If a screw rolls under the motherboard and cannot be reached, tilt the computer so that the screw rolls out. Sometimes the case must be tilted in different directions until the screw becomes dislodged.

Disassembly

Before a technician disassembles a computer, the following disassembly suggestions should be considered:

- Do not remove the motherboard battery; if you do, the configuration information in CMOS will be lost.
- Use proper grounding procedures to prevent ESD damage.
- Keep paper, a pen, a phone, or a digital camera nearby for note taking, diagramming, and photo taking. Even if you have taken apart computers for years, you might find something unique or different inside this one.
- Have ample flat and clean workspace.
- When removing adapters, do not stack the adapters on top of one another.
- If possible, place removed adapters inside a special ESD protective bag.
- Handle each adapter, motherboard, or processor on the side edges. Avoid touching the gold contacts on the bottom of an adapter. Sweat, oil, and dirt cause problems.
- Remember that hard drives require careful handling. A very small jolt can cause damage to stored data.
- You can remove a power supply but do not disassemble a power supply without proper training and tools.
- Document screw and cable locations. Label them if possible.

The following section describes the steps in disassembling a computer.

Step 1. Remove Power and External Cables

The first step in disassembling the computer is to remove the power cord. A small amount of power is sent to the motherboard even when the computer is powered off so that the computer can be "woken up" (especially in a corporate environment) and updates can be applied. The next step is removing external cables. Make notes about which cable attaches to each specific port. Figure 5.6 shows the back of the computer, where this is done.

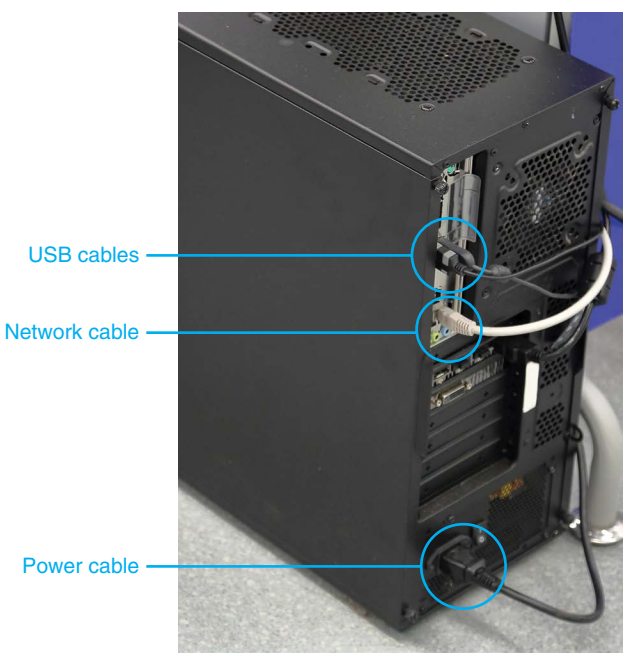


FIGURE 5.6 Removing power and external cables

Step 2. Open the Case

Opening or removing the case is sometimes the hardest part of disassembly. When possible, refer to the manufacturer's directions when opening a case. Some manufacturers have tabs or covers over the retaining screws, and others have retention levers or tabs that have to be pressed before the cover slides open or away. For some computers, you must press downward on a tab on top of the computer while simultaneously pressing upward on a tab on the bottom of the computer.

For all screws, take notes/photos. Use an egg carton to hold removed screws and label the carton cup where the screws go. Most of the time, you can access inside the computer case by simply removing the screws that hold down the side panel, as shown in Figure 5.7.

FIGURE 5.7 Removing case screws

Step 3. Remove Internal Cables and Connectors

Internal cables can be tricky. Inserting a cable backward into a device or an adapter can damage the device, motherboard, or adapter. Most cables are keyed so the cable inserts into the connector only one way.

A cable may have a pull tab or plastic piece that is used to remove the cable from the connector and/or device. Use this if possible or firmly grip the connector, not the cable. If a connector has a locking tab, release the tab *before* disconnecting the cable to prevent damage to the cable and/or connector.

Be careful with drive cables. Some of the narrow drive cables, such as Serial Advanced Technology Attachment (SATA) cables, are not very sturdy and do not connect as firmly as some of the other computer cables. Also, with this particular cable type, it does not matter which cable end attaches to the device. A 90°-angled version of this cable (see Figure 5.8) might attach to devices in a case that has a limited-space design and might have a release latch. Figure 5.9 shows the **SATA connectors** used for the cables in Figure 5.8 that connect to hard drives and/or optical drives.

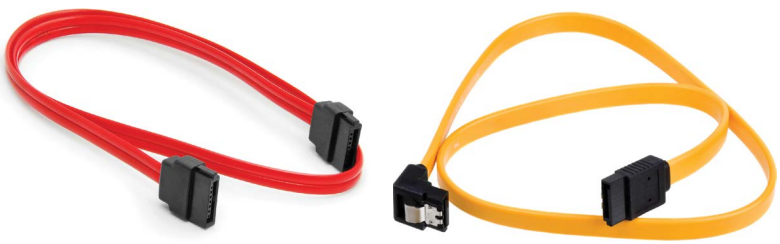


FIGURE 5.8 SATA cables including 90°-angled cable with a latch

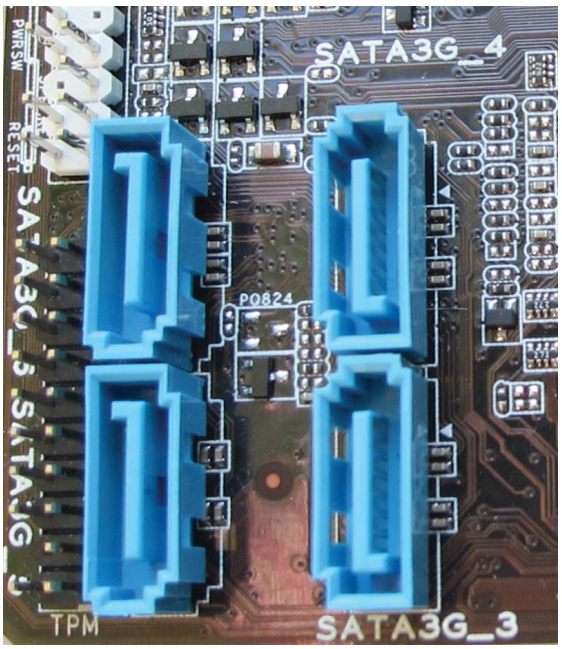


FIGURE 5.9 Motherboard SATA drive connectors

TECH TIP

Snug connections

When connecting cables to a motherboard or internal components, ensure that each cable is connected tightly, evenly, and securely.

Motherboard connectors are usually notched so that the cable inserts only one way; however, not all cables are notched. Some motherboards have pin 1 (or the opposite pin) labeled. Ensure that pin 1 of a cable matches pin 1 of the connector.

Figure 5.10 shows a motherboard power connector that comes in two parts, a 20-pin part and a 4-pin part; it is known as a **20 + 4 connector** and can be inserted into a **24-pin motherboard power connector**. Notice the clip on the larger 20-pin connector. Press this clip to release the cable before pulling the cable out of the connector. If the connection is tight, keep your hands on the sides of the connector and wiggle back and forth to inch it upward.

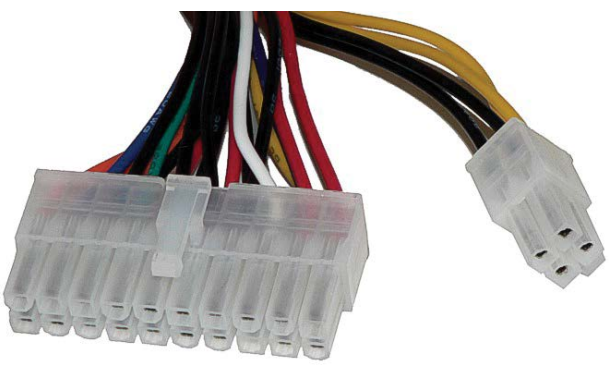


FIGURE 5.10 Motherboard power connector

Specific cables connect from the motherboard **front panel connectors** to lights, ports, or buttons on the front panel. These include the power button, a reset button, USB ports, a microphone

port, a headphone port, speakers, fans, the drive activity light, and the power light, to name a few. Be very careful when removing and reinstalling these cables. Usually, each one of them has a connector that must attach to the appropriate motherboard pins. Be sure to check all ports and buttons after you have reconnected these cables. Refer to the motherboard documentation if your diagramming, photos, or notes are incomplete. Figure 5.11 shows the motherboard pins and the cables.

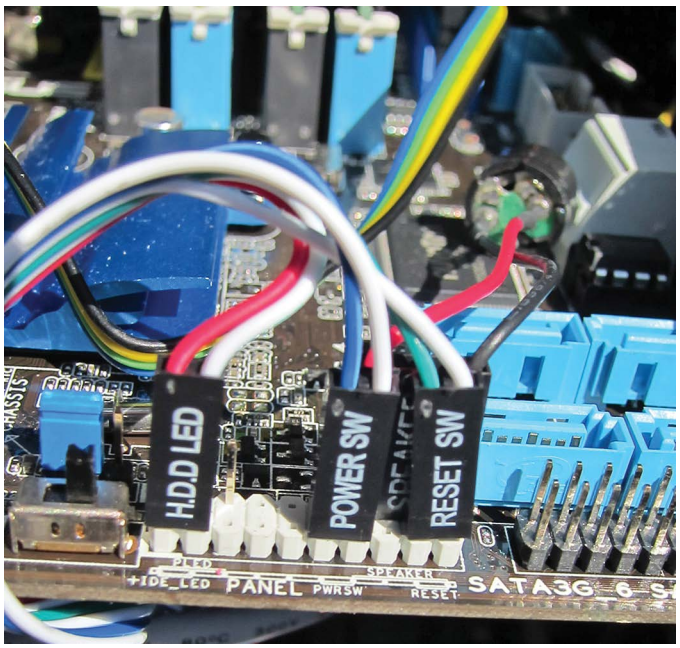


FIGURE 5.11 Motherboard front panel cables

TECH TIP

Carefully connecting front panel cables

Ensure that you connect the front panel cables to the appropriate pins and in the correct direction. Some manufacturers label their cables, as shown in Figure 5.11. Once you have one cable oriented correctly, the others are commonly oriented in the same direction. For example, Figure 5.11 shows all the white wires oriented in the same direction.

The motherboard also contains pins that are used to connect cables such as those that go to the CPU or case fans. Look back at Figure 3.20 (refer to Chapter 3, "On the Motherboard") to see how fans connect to pins on the motherboard.

Step 4. Remove Adapters

Adapters commonly have retaining screws or a bar that keeps the adapters firmly in the case (refer to Figure 4.14 in Chapter 4). Use the edges of the adapter to pull it upward and out of the expansion slot. Do not touch the contacts on the bottom of the adapter. Never pile adapters on top of one another. If you have an empty expansion slot, insert an expansion slot bracket to cover the hole so proper airflow will be maintained within the case. Figure 5.12 shows an adapter being removed.

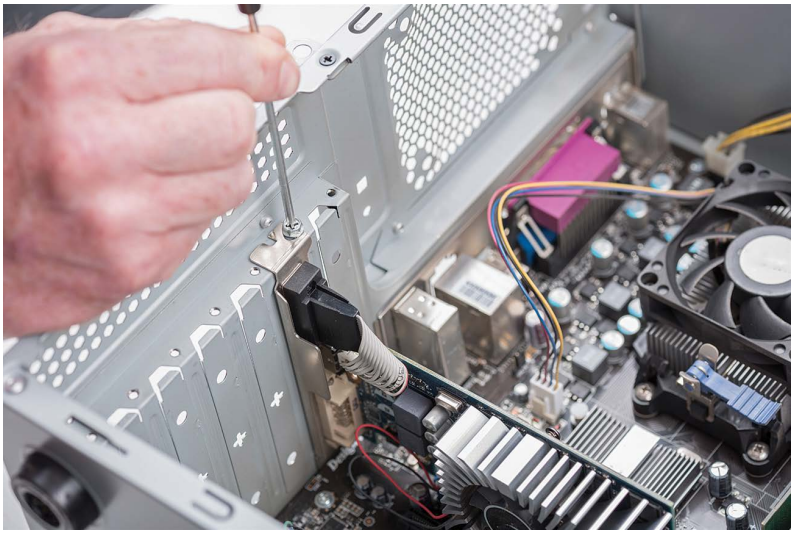


FIGURE 5.12 Adapter removal

Step 5. Remove Storage Devices

Hard drives must be handled with care when disassembling a computer. Inside traditional mechanical hard drives are hard platters with read/write heads located just millimeters above the platters. If dropped, the read/write heads might touch the platter, causing damage to the platter and/or the heads. Today's mechanical hard drives have self-parking heads, but even with this feature, improper handling can cause damage to the hard drive.

A solid-state drive (SSD) does not contain fragile heads. However, these drives are susceptible to ESD. Use proper antistatic handling procedures when removing/installing them. Store a solid-state drive in an antistatic bag when not in use.

A hard drive or an optical drive slides into a drive bay. Some cases require the hard drive to have drive rails that attach to the side of the drive. Other cases require that the drive be screwed directly into the hard drive bay. Figure 5.13 shows a hard drive being removed. You can see that this particular case requires screws to secure drives inserted into the drive bays.

FIGURE 5.13 Removing a hard drive

Figure 5.14 shows a hard drive that has a guide rail attached and a different set of guide rails below the drive. When replacing a drive, the drive rails would have to be removed from the old drive and attached to the replacement drive. When installing a new drive, drive rails might have to be purchased.

FIGURE 5.14 Hard drive rails

Step 6. Remove the Motherboard

Chapter 3 covers motherboard replacement extensively, and here we discuss issues related to building a computer from scratch or disassembling a computer. Some cases include a standard I/O panel shield that might need to be removed to install the I/O shield that may come with a motherboard. The **I/O shield** is a part that allows for optimum airflow and grounding for the motherboard ports. The I/O shield helps ensure that the motherboard is installed correctly and properly aligned with the case. Figure 5.15 shows a motherboard I/O shield.

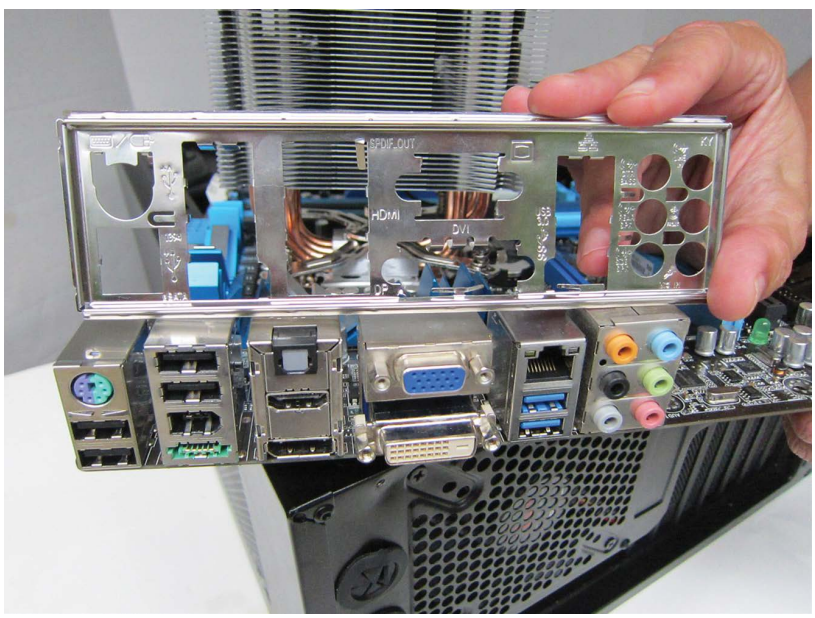


FIGURE 5.15 Motherboard I/O shield

Some computer cases have plastic or metal (commonly brass) **standoffs** that allow the motherboard to be screwed into the case without the motherboard solder joints touching and grounding to the computer case, causing the motherboard not to work. Some standoffs are plastic, and they slide into slots on the computer case. Do not remove these types of standoffs; just leave them attached and slide the motherboard out of the slots. The most common type of standoff is a metal standoff that screws into the case (see Figure 5.16); this standoff has a threaded side that the motherboard sits on and a screw that attaches the motherboard to the standoff.

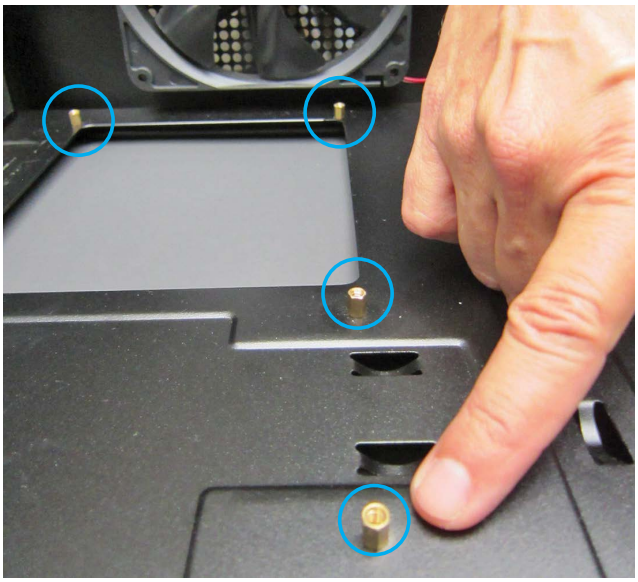


FIGURE 5.16 Motherboard standoff

Some motherboards have not only screws that attach them to the metal standoffs but also one or more retaining clips. A retaining clip might need to be pressed down, lifted up, or bent upward in order to allow the motherboard to be slid out of the case. The case might contain one or more notches, and the motherboard might have to be slid in a particular direction (usually in the direction going away from the back I/O ports) before being lifted from the case.

All-in-One Computers

The same disassembly concepts apply to all-in-one computers as to desktop computers including cabling, storage device removal, RAM removal, motherboard removal, and power. The difference is the space in which the devices are installed: An all-in-one computer has everything installed on the back of the display, as shown in Figure 5.17.

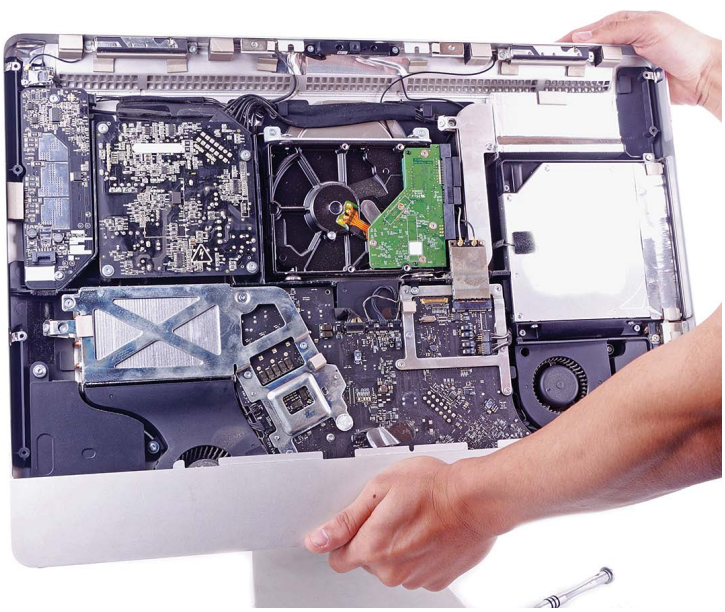


FIGURE 5.17 All-in-one computer parts

Reassembly

Reassembling a computer is easy if the technician is careful and properly documents the disassembly. Simple tasks may become confusing after many parts have been removed. Writing reminders or taking photos takes less time than having to troubleshoot the computer because of poor reassembly. A technician should reinsert all components into their proper places, being careful to replace all screws and parts and to install missing slot covers, if possible.

When reinstalling a motherboard, reverse the procedure used during disassembly. Ensure that the motherboard is securely seated into the case and that all retaining clips and/or screws are replaced. Visual inspection can also help. Ensure that the ports extend fully from the case through the I/O shield. As a final step, ensure that the drives and cover are aligned properly when the case is reinstalled.

Cables and connectors are the most common sources of reassembly problems. Ensure that cables are fully attached to devices and the same motherboard connector. Ensure that power cables are securely attached.

Preventive Maintenance

In the course of daily usage, computers get dirty (see Figure 5.18), especially inside. Dust accumulates, creating insulation and increasing the amount of heat generated. Additional heat can cause electronic components to overheat and fail. It can also cause the processor to consistently run at a lower speed.

FIGURE 5.18 Dust inside a computer

Preventive maintenance includes procedures performed to prolong the life of a computer. A computer in a normal working environment should be cleaned at least once a year. Typical preventive measures include vacuuming the computer and keyboard keys and spraying compressed air inside the power supply and in hard-to-reach areas such as around connectors. Before accessing internal parts, be sure to power down a computer and remove the power cord, remove the battery and AC adapter for a laptop or other mobile device, and allow a laser printer to cool. Preventive measures for many individual devices are described in their respective chapters.

TECH TIP

Carefully cleaning displays

To clean displays, use either wipes specifically designed for displays or a soft lint-free cloth dampened with either water or a mixture of isopropyl alcohol and water. Never put liquid directly on the display and ensure that the display is dry before closing a laptop.

When performing preventive maintenance, power on the computer to be certain it operates. Perform an audio and visual inspection of the computer as it boots. Electronic equipment such as PCs and mobile devices is designed to operate at room temperature (around 73°F [23°C]). For an environment above 80°F (27°C), a device should have additional cooling methods.

Manufacturers sometimes have a preventive **maintenance kit** for service calls. Common components list and are described in Table 5.1.

TABLE 5.1 Preventive maintenance items

Item	Description
Portable vacuum	Used to suck dirt from inside the computer. Be sure to use nonmetallic attachments. With a vacuum cleaner that has the ability to blow air, vacuum first and then set the vacuum cleaner to blow to get dust out of hard-to-reach places. Hold fan blades in place while you do this.
Toner vacuum	Used to clean computers and laser printers. Special vacuum bags are used to prevent the toner from melting and potentially damaging vacuum cleaner parts.
Special vacuum bags	Used for laser printers so that the toner does not melt on the vacuum motor.
Compressed air	Used to remove dust in hard-to-reach places (preferably after vacuuming).
Urethane swabs	Used to clean between keys on a keyboard. If a key is sticking, disconnect the keyboard before spraying or using contact cleaner on it.
Monitor wipes	Used on the front of the display. Wipes with an antistatic solution work best.
Lint-free cloths	Used to clean laptop touchpads and other components. Dampen a cloth to remove residual finger oil.
General-purpose cloths	Used to clean the outside of the case and to clean the desktop areas under and around the computer.
General-purpose cleanser	Used with soft lint-free cloths or lint-free swabs. Never spray or pour liquid on any computer part.
Denatured alcohol	Used on rubber rollers, such as those inside printers.
Antistatic brush	Used to brush dirt from hard-to-reach places.
Optical drive cleaning kit	Can include a lens cleaner that removes dust and debris from an optical lens; a disc cleaner that removes dust, dirt, fingerprints, and oils from the disc; and a scratch repair kit to resurface, clean, and polish CDs, DVDs, and BDs.
Gold contact cleaner	Used to clean adapter contacts as well as contacts on laptop batteries and the contacts where the battery inserts.

Item	Description
Safety goggles	Used in dusty environments or when dealing with chemicals in a poorly ventilated area. Indirect vent goggles prevent a splash from coming into contact with eyes. Nonvented goggles protect from dust, splash, and chemical vapors.
Air filter mask	Used for protection from airborne fumes, dust, and smoke. There are two types of filters: those for vapors and those for particles. Filtering for vapors helps when using chemical cleaners and solvents. Filtering for particles helps with things that make you sneeze, such as dust, pollen, and mold. Insert an additional layer into a mask for additional protection.

A cleaning solution company may provide a material safety data sheet (**MSDS**) or safety data sheet (**SDS**) that contains information about a product, including its toxicity, storage, disposal, and health/safety concerns. Computer components have the potential to contain toxic substances. Larger companies have very specific rules about how electronic waste is handled. Each state commonly has specific disposal procedures for chemical solvents and toxic waste. Use the MSDS/SDS, research handling/disposal guidelines according to local government regulations, and use appropriate safety equipment when performing preventive maintenance.

TECH TIP

Knowing your state aerosol can disposal laws

Some states have special requirements for disposal of aerosol cans, especially those that are clogged and still contain some product.

To perform the preventive maintenance, power off the computer, remove the power cord, and vacuum the computer with a nonmetallic attachment. Do not start with compressed air or by blowing dust out of the computer because the dirt and dust will simply go into the air and eventually fall back into the computer and surrounding equipment. Figure 5.19 shows vacuuming inside a computer. Remember to hold your finger or a brush on the fan blade so it does not spin out of control and damage the fan.

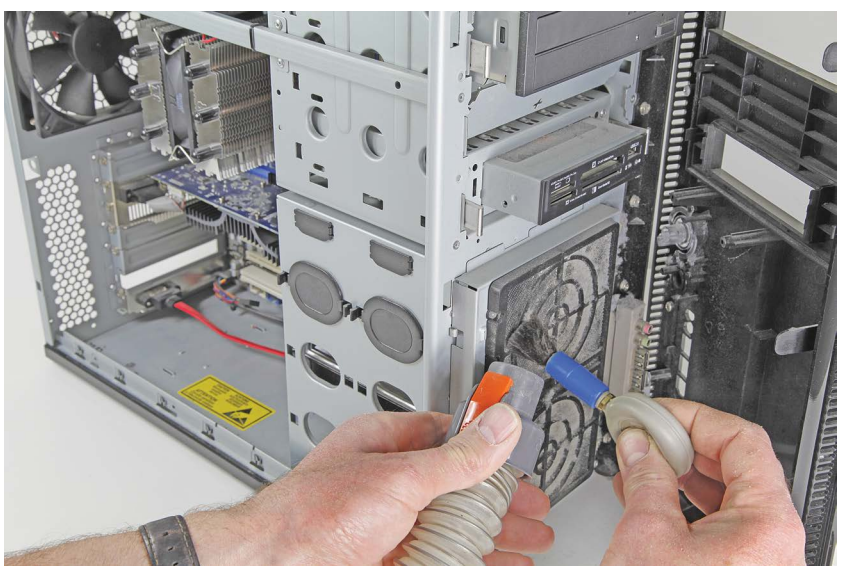


FIGURE 5.19 Preventive maintenance vacuuming

After vacuuming as much as possible, use compressed air to blow the dust out of hard-to-reach places, such as inside the power supply and under the motherboard (see Figure 5.20). If you are performing maintenance on a laptop computer, remove as many modules as possible before vacuuming or using compressed air. Use appropriate safety equipment, including safety goggles and a mask, when performing preventive maintenance.

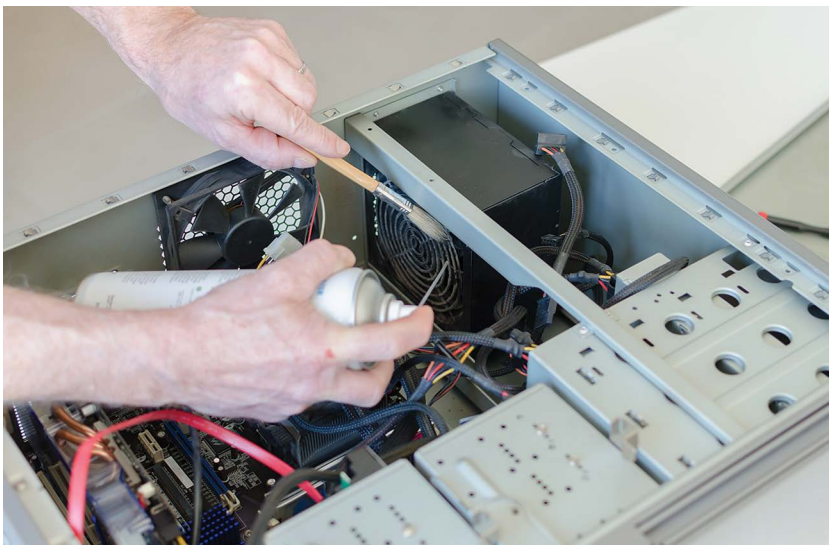


FIGURE 5.20 Preventive maintenance using compressed air

Basic Electronics Overview

A technician needs to know a few basic terms and concepts related to electronics when testing components. The best place to start is with electricity. There are two types of electricity: AC and DC. The electricity provided by a wall outlet is alternating current (**AC**), and the type of electricity used by computer components is direct current (**DC**). Devices such as radios, TVs, and toasters use AC power. Low-voltage DC power is used for a computer's internal components. A computer's power supply converts AC electricity from the wall outlet to DC for the internal components. Electricity involves electrons flowing through a conductor, much like the way water runs through a pipe. With AC, electrons flow alternately in both directions. With DC, electrons flow in one direction only.

TECH TIP

Always unplug a computer before working inside it

The power supply provides power to the motherboard even if the computer is powered off. Leaving the power cord attached can cause damage when replacing components such as the processor or RAM.

Electronics: Terminology

Voltage, current, power, and resistance are terms commonly used in the computer industry. **Voltage**, which is a measure of the pressure pushing electrons through a circuit, is measured in **volts** and shown with a value followed by a capital V. A power supply's output is measured in volts. Power supplies typically put out +3.3 volts, +5 volts, +12 volts, and –12 volts. Another designation is +5VSB. This is for the computer's standby power, which is always provided, even when the computer is powered off. This supplied voltage is why you have to unplug a computer when working inside it.

TECH TIP

Polarity is important only when measuring DC voltage

When a technician measures the voltage coming out of a power supply, the black meter lead (which is negative) connects to the black wire from the power supply (which is ground). The red meter lead connects to either the +5 or +12 volt wires from the power supply.

The term *volts* is also used to describe voltage from a wall outlet. Wall outlet voltage is normally 120VAC (120 volts AC). A multimeter is a tool used to take voltage readings. Figure 5.21 shows a multimeter being used to take a DC voltage reading on a battery.

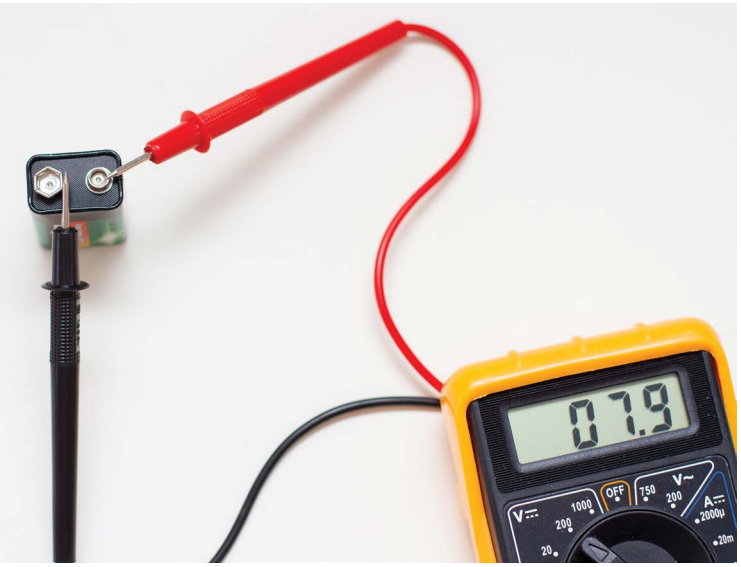
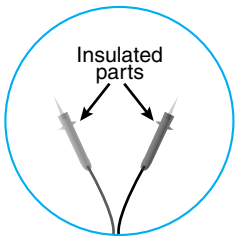


FIGURE 5.21 DC voltage reading

It is important to have the black meter lead on the negative and the red lead on the positive when measuring DC voltage. If the meter's leads are reversed, the reading on the meter could be the opposite of what it should be. Figure 5.22 shows rules to observe when working with meters.



1. Select AC or DC on the meter (some meters automatically select AC or DC).

   VAC or ACV or ~ or Ṽ

   VDC or DCV or — or ⎓ or V̄

2. Select the appropriate voltage range (0-10V, 0-100V, etc). The meter can be damaged if you measure a high voltage in a low range (but not the reverse). Use the highest range for unknown voltages.

3. Touch only the insulated parts of the meter probes.

FIGURE 5.22 Meter rules

Power supplies, flat panel displays, and mobile device displays also contain high voltage levels. 120 volts AC is present inside the power supply of a desktop computer. Power supplies and monitors have capacitors inside them that hold a charge even after the computer is turned off. Be extremely careful when working with these devices.

Current is measured in **amps** (amperes), which is the number of electrons going through a circuit every second. In the water pipe analogy, voltage is the amount of pressure applied to force the water through the pipe, and current is the amount of water flowing. Every device needs a certain

amount of current to operate. A power supply is rated for the amount of total current (in amps) it can supply at each voltage level. For example, a power supply could be rated at 20 amps for the 5-volt level and 8 amps for the 12-volt level.

TECH TIP

Current is what kills people when an electrical shock is received

Voltage determines how much current flows through the body. A high-current and low-voltage situation is the most dangerous.

Power is measured in **watts**, which is a measurement of how much work is being done. It is determined by multiplying volts by amps. Power supplies are described as providing a maximum number of watts or having a specific wattage rating. It is the sum of all outputs (for example, [5 volts × 20 amps] + [12V × 8 amps] = 100 watts + 96 watts = 196 watts).

Resistance is measured in **ohms**, which is the amount of opposition to current in an electronic circuit. The resistance range on a meter can be used to check continuity. A **continuity** check is used to determine whether a wire has a break in it. A conductor (wire) in a cable or a good fuse will have very low resistance to electricity (close to zero ohms). A broken wire or a bad fuse will have a very high resistance (millions of ohms, sometimes shown as infinite ohms, or OL). For example, a cable is normally made up of several wires that go from one connector to another. If you measure the continuity from one end of a wire to the other, it should show no resistance. If the wire has a break in it, the meter shows infinite resistance. Figure 5.23 shows examples of readings for a good wire and for a broken wire.

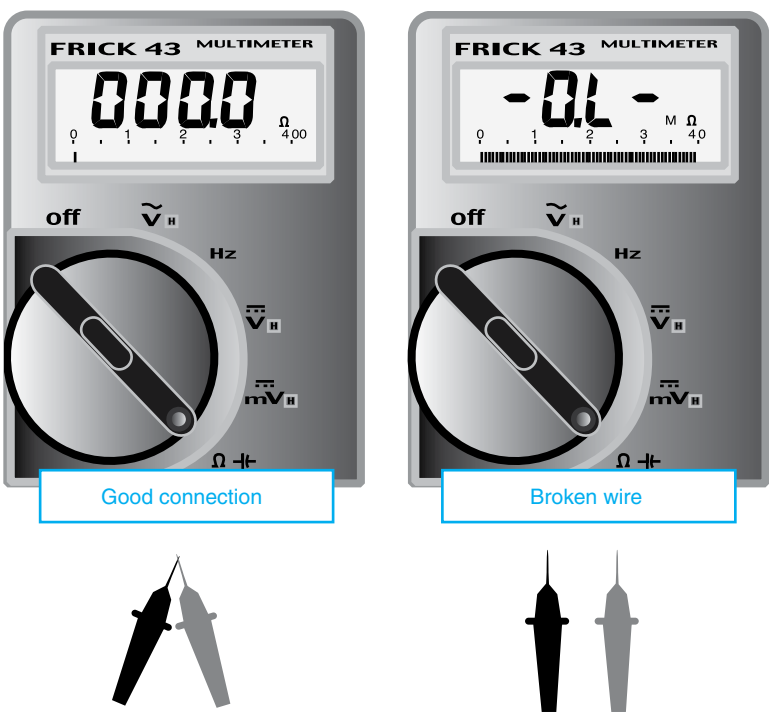


FIGURE 5.23 Sample resistance meter readings

Digital meters have different ways of displaying infinity. Always refer to the meter manual. When checking continuity, the meter is placed on the ohms setting, sometimes shown as an omega symbol (Ω).

Polarity is not important when performing a continuity check. Either meter lead (red or black) can be placed at either end of the wire. However, you do need a pin-out diagram (wiring list) for the cable in order to check continuity because pin 1 at one end could connect to a different pin number at the other end.

A technician needs to be familiar with basic electronics terms and checks. Table 5.2 consolidates this information.

TABLE 5.2 Basic electronics terms

Term	Value	Usage
Voltage	Volts	Voltage is relevant when checking AC voltage from a wall outlet (typically 120VAC) and when checking the DC output voltage from a power supply (typically ±12VDC, +3.3VDC, and ±5VDC).
Current	Amps (amperes)	Each device needs a certain amount of current to operate. A power supply is rated for total current in amps for each voltage level (such as 24 amps for 5-volt power and 50 amps for 12-volt power).
Resistance	Ohms	Resistance is the amount of opposition to electric current. Resistance measurements are used to check continuity on cables and fuses. A cable that shows little or no resistance has no breaks in it. If a cable has a break in it, the resistance is infinite.
Wattage (power)	Watts	Watts is a measure of power and is derived by multiplying amps by volts. Power supply output is measured in watts.

Power Supply Overview

A power supply is an essential component within a computer; no internal computer device works without it. A power supply converts AC to DC, distributes lower-voltage DC power (**3.3V**, **5V**, and **12V** output voltage) to components throughout the computer, and provides cooling through the use of a fan located inside the power supply.

The AC voltage a power supply accepts is normally either 100 to 120 volts or 200 to 240 volts. (Note that the A+ certification exam objectives list this as **110V vs. 220V input voltage**.) Some dual-voltage power supplies can accept either. This type of power supply might have a selector switch on the back. Select power supplies can monitor the incoming voltage from the wall outlet and automatically switch from 100VAC to 240VAC at 50 to 60 Hz. These power supplies are popular with mobile devices and are great for international travel.

TECH TIP

Powering on a power supply without anything attached could damage the power supply

Do not power on a power supply without connecting to the motherboard and possibly a device such as an optical drive or hard drive. An ATX power supply usually requires a motherboard connection at a minimum.

Power Supply Form Factors

Just as motherboards come in different shapes and sizes, so do power supplies. Today's power supply form factors are ATX, ATX12V, and micro-ATX. The ATX power supply form factor was

the first type to allow a small amount of voltage to be provided to the motherboard so that both hardware and software could be used to "wake up" the device and/or to conserve power.

The micro-ATX power supply form factor is a smaller version than a full-sized ATX power supply to fit in smaller cases. Other form factors include LFX12V (low profile), SFX12V (small form factor), EPS12V (used with server motherboards), CFX12V (compact form factor), SFX12V (small form factor), TFX12V (thin form factor), WTX12V (workstation form factor for high-end workstations and select servers), and FlexATX (smaller systems).

Intel, AMD, and video card manufacturers certify specific power supplies that work with their processors and video cards. A computer manufacturer can also have a proprietary power supply form factor that is not compatible with different computer models or other vendors' machines. Laptop power supplies are commonly proprietary.

Power Supply Connectors

Table 5.3 lists the possible ATX power supply connectors, and Figure 5.24 shows them.

TABLE 5.3 ATX power supply connectors

Connector	Notes	Voltage(s)
24-pin main power or 20 + 4 pin main power	Main ATX power connector to the motherboard	+3.3, +5, +12, –12
15-pin SATA power	Internal SATA power connector	+3.3, +5, +12
8-pin 12V	12 V for CPU used with an ATX12V v1 power supply	+12
8-pin PCIe	PCIe video; connects to a PCIe video adapter (Note that some connectors are 6 + 2-pin, meaning they accept either the 6- or 8-pin cable.)	+12
6-pin PCIe	PCIe video; connects to a PCIe video adapter	+12
6-pin	Sometimes labeled AUX; connects to the motherboard if it has a connector	+3.3, +5
4-pin **Molex**	Connects to a peripheral device such as a hard drive or a CD/DVD drive	+5, +12
4-pin Berg	Connects to a peripheral device such as a floppy drive	+5, +12
4-pin 12V	Sometimes labeled AUX or 12V; connects to the motherboard for the CPU	+12
3-pin	Used to monitor fan speed	N/A

TECH TIP

The motherboard, case, and power supply must be size compatible

The motherboard and case form factor and the power supply form factor must fit in the case and must work together. For optimum performance, research what connectors and form factors are supported by both components.

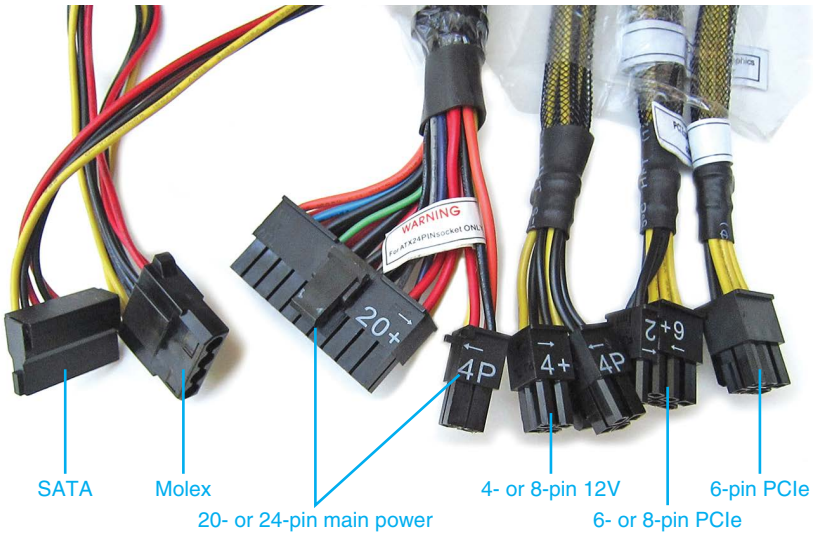


FIGURE 5.24 ATX power supply connectors

Figure 5.25 illustrates the ATX 24-pin motherboard connector standards. Older power supplies had a 20-pin motherboard connector that you could plug straight into the 24-pin motherboard socket (leaving pins 11, 12, 23, and 24 empty), or you could buy a **20-pin to 24-pin motherboard adapter**. Notice in Figure 5.25 that the power cable is only one connector, and the cable inserts into the connector one way only. Also notice that a power good signal (labeled PWR_OK in Figure 5.25) goes to the motherboard. When the computer is turned on, POST allows the power supply to run a test on each of the voltage levels. The voltage levels must be correct before any other devices are tested and allowed to initialize. If the power is okay, a power good signal is sent to the motherboard. If the power good signal is not sent from the power supply, a timer chip on the motherboard resets the CPU. Once a power good signal is sent, the CPU begins executing software from the BIOS/UEFI. Figure 5.25 also shows the +5VSB connection to provide standby power for features such as Wake on LAN or Wake on Ring (covered later in this chapter).

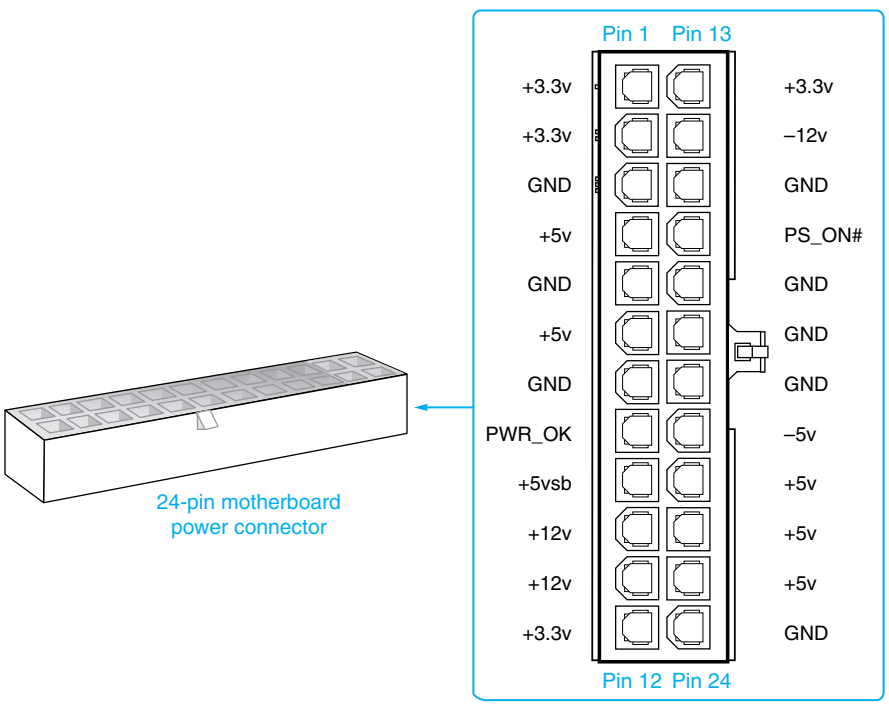


FIGURE 5.25 ATX 24-pin motherboard pinout drawing

The quantity and type of connectors available on a power supply depend on the power supply manufacturer. If a video card needs a PCIe connector and two Molex power connectors are free, a dual Molex-to-PCIe converter can be purchased. If a SATA device needs a power connection and only a Molex cable is free, a Molex-to-SATA converter may be used. Figure 5.26 shows a dual Molex-to-PCIe converter on the left and a Molex-to-SATA converter on the right.

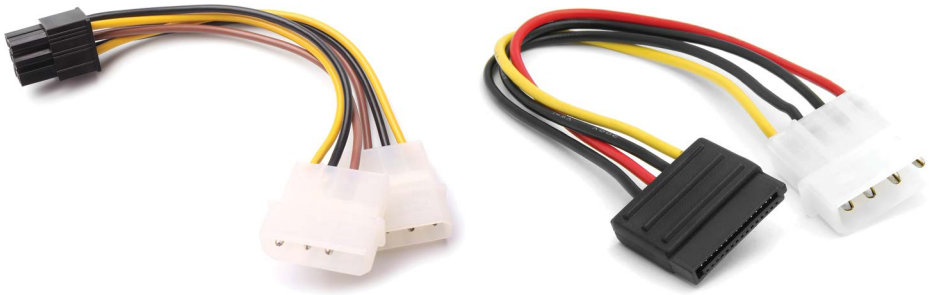


FIGURE 5.26 Dual Molex-to-PCIe and Molex-to-SATA converters

Power supply connectors can connect to any device; there is not a specific connector for a hard drive, an optical drive, and so on. If there are not enough connectors from a power supply for the number of devices installed in a computer, a Y power connector can be purchased at a computer or electronics store.

Purposes of a Power Supply

The power from a wall outlet is high-voltage AC. The type of power computers need is low-voltage DC. All computer parts (the electronic chips on the motherboard and adapters, the electronics on the drives, and the motors in the hard drive and optical drive) need DC power to operate. Power supplies in general come in two types: linear and switching. Computers use switching power supplies. The main functions of a power supply include the following:

- Convert AC to DC
- Provide DC voltage to the motherboard, adapters, and peripheral devices
- Provide cooling and facilitate airflow through the case

TECH TIP

Powering on an ATX power supply

On an ATX power supply that has an on/off switch, ensure that it is set to the *on* position. If an ATX power supply switch is present and in the off position, the motherboard and operating system cannot turn on the power supply. Some ATX power supplies do not have external on/off switches, and the computer can be powered down only via the operating system.

TECH TIP

Checking the input voltage selector

Some power supplies and laptops have input voltage selectors; others have the ability to accept input from 100 to 240 volts for use in various countries (dual-voltage). Ensure that the power supply accepts or is set to the proper input voltage.

Another purpose of a power supply is to distribute proper DC voltage to each component. Several cables with connectors come out of the power supply. With ATX motherboards, there is only a 24-pin connector used to connect power to the motherboard. The power connector inserts only one way into the motherboard connector. Figure 5.27 shows an ATX connector being inserted into a motherboard.

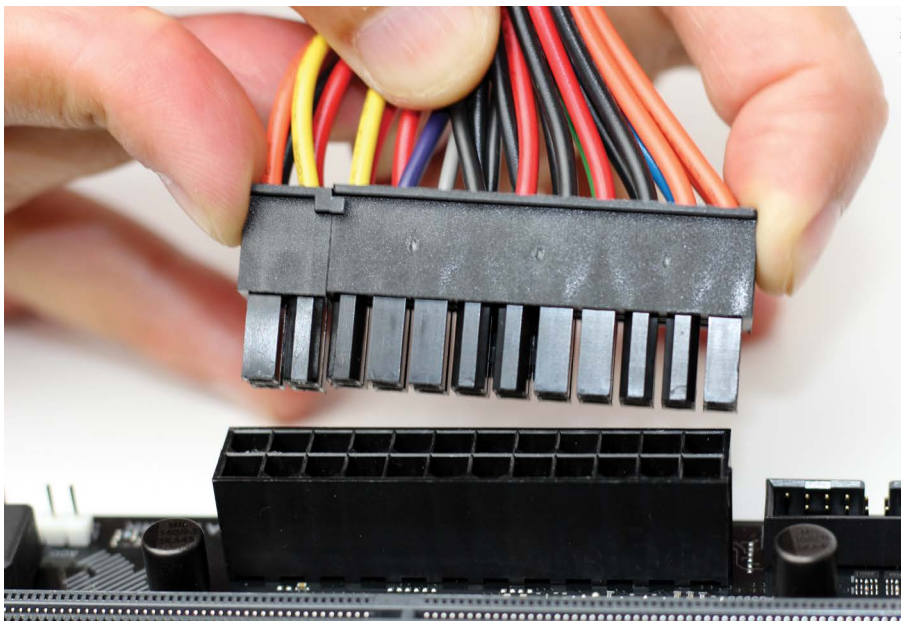


FIGURE 5.27 Installing an ATX power connector on a motherboard

Most modern computer cases are designed for bottom-mounted PSUs. In this scenario, it is best to install the PSU with its fan facing downward. This allows the PSU to pull cool air in directly from outside the case, improving efficiency. This air is then exhausted through the back of the PSU, outside the computer case. Thus, the PSU's airflow is usually separate from the primary case airflow, creating a more efficient cooling system. When using a case without bottom ventilation, it is common to mount the PSU with the fan facing upward, drawing air from inside the case and exhausting it out of the case.

TECH TIP

Don't block air vents

Whether a computer is a desktop model, a tower model, or a desktop model mounted in a stand on the floor, ensure that nothing blocks the air vents in the computer case.

Because heat sinks generate a lot of heat, it is important to have the proper amount of airflow and in the right direction. Additional fans can be installed to provide additional cooling for a PC. Figure 5.28 shows extra cooling fans installed, power supply connections, and LED lights, which are popular in cases today.

TECH TIP

Airflow and ventilation

Airflow should be through the computer and over the motherboard to provide cooling for the motherboard components.

Cases have different numbers of and locations of mounting spots for the case fan(s). Figure 5.29 shows potential installation sites for additional case fans.

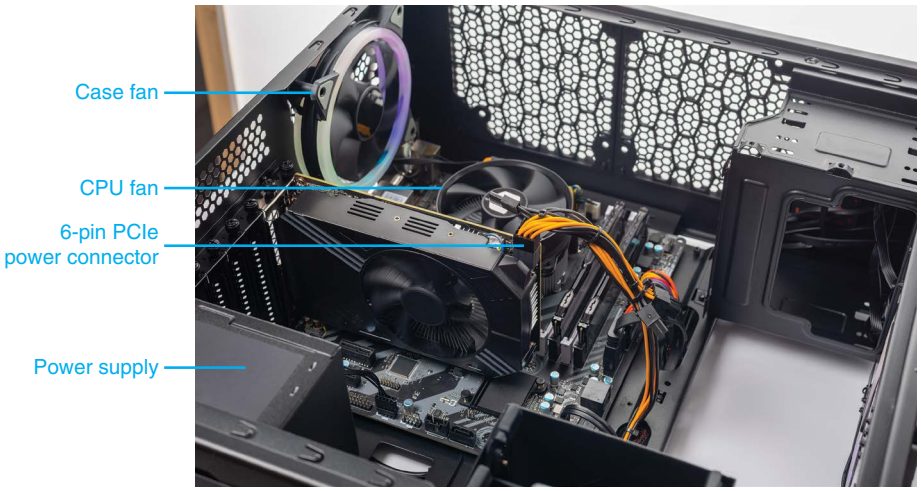


FIGURE 5.28 Computer case auxiliary fan with LED lighting

TECH TIP

Being careful when installing an auxiliary fan

Place a fan so the outflow of air moves in the same direction as the flow of air generated by the power supply. If an auxiliary fan is installed inside a case in the wrong location, the auxiliary airflow could work against the power supply airflow, reducing the cooling effect.

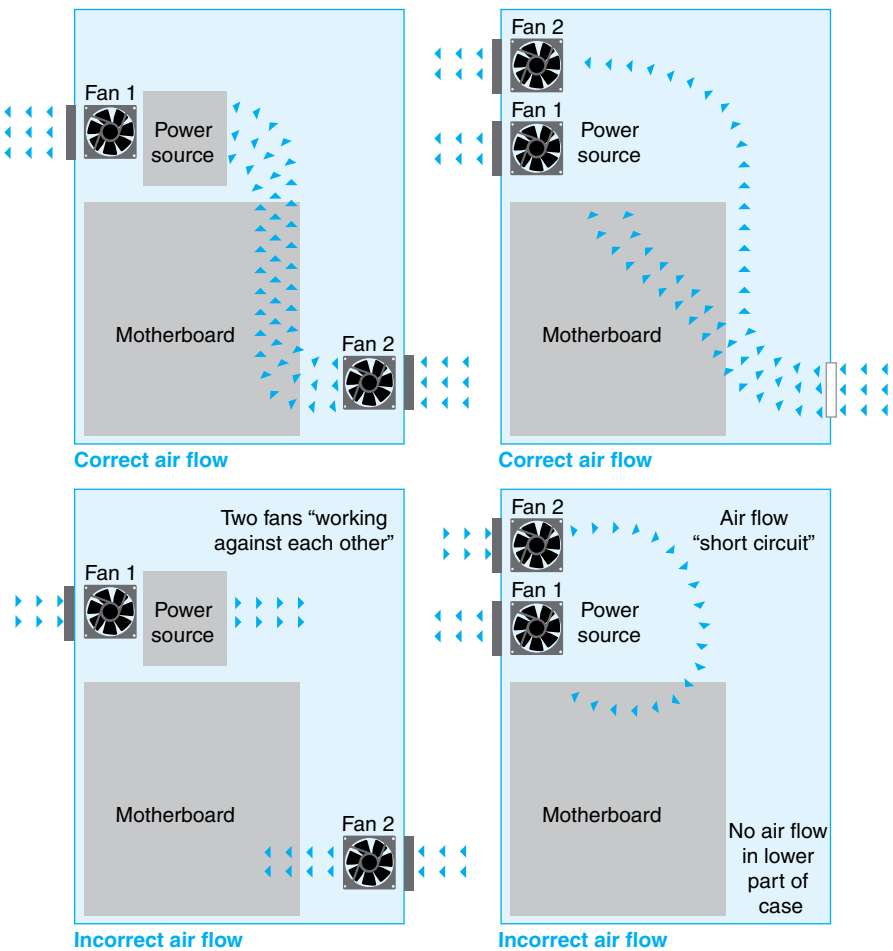


FIGURE 5.29 Placement of auxiliary fans

Advanced Configuration and Power Interface (ACPI)

Advanced Configuration and Power Interface (**ACPI**) gives the BIOS/UEFI and operating system control over various devices' power and modes of operation. ACPI has various operating states, as shown in Table 5.4.

TABLE 5.4 ACPI operating states

Global system state	Sleep state	Description
G0 Working	S0	The PC is running.
G1 Sleeping		Requires less power than the G0 state and has multiple sleep states: S1, S2, S3, and S4.
	S1	CPU is still powered, and unused devices are powered down. RAM is still being refreshed.
	S2	CPU is not powered. RAM is still being refreshed. System is restored instantly upon user intervention.
	S3	Power supply output is reduced. RAM is being refreshed. Some information in RAM is restored to the CPU and the cache.
	S4	Lowest-power sleep mode, which takes the longest to come up. Information in RAM is saved to a hard drive or flash media.
G2 Soft off	S5	Power consumption is almost zero. Requires the operating system to reboot. No information is saved anywhere.
G3 Mechanical off		This is the only state in which the computer can be disassembled. Power on the computer to use it again.

ACPI allows apps to work with the operating system to manage power, such as when an application is set to automatically save a document, but might not do so until the hard drive is being used for something else in order to conserve power in a laptop. In the Windows environment, the sleep mode (also known as suspend mode) uses one of the G1 sleeping ACPI states to allow the device to be awakened to continue working. The hibernate mode uses the G1 S4 mode and takes the longest to bring a device back to a working state.

TECH TIP

Which power option to select: standby or hibernate?

Most people who want to quickly re-access the device would select the standby option. However, the hibernate mode saves more energy.

Two common BIOS/UEFI and adapter features that take advantage of ACPI are Wake on LAN and Wake on Ring. The **Wake on LAN** feature allows a network administrator to control the power to a workstation remotely and directs the computer to come out of sleep mode. Software applications can also use the Wake on LAN feature to perform updates, upgrades, and maintenance tasks. The feature can also be used to bring up computers immediately before the business day starts. Wake on LAN can be used with web or network cameras to start recording when motion is detected or to bring up a network printer so that it can be used when needed.

Wake on Ring allows a computer to come out of sleep mode when the phone line has an incoming call. It lets the computer receive phone calls, faxes, and emails when the user is not present.

TECH TIP

Why leave computers on at the office?

In Windows, when a computer is shut down, it is put in soft off, or S5, state. Wake on LAN is not officially supported from this state, and for this reason, corporate environments request that users leave their computers turned on but logged off on specific days or every day.

Replacing or Upgrading a Power Supply

Power supplies are rated in watts. Today's typical computers have power supplies with **wattage ratings** ranging from 250 to 500 watts, although powerful computers, such as network servers or higher-end gaming systems, can have power supplies rated 600 watts or higher. Internal and external devices powered by a particular type of port, such as USB, are affected by the number of amps available from the +5VDC and +12VDC power supply output and the total amount of wattage available.

Each device inside a computer uses a certain amount of power, and the power supply must provide enough power to run all the devices. The power each device or adapter requires is usually defined in the documentation for the device or adapter or on the manufacturer's website. The computer uses the wattage needed, not the total capacity of a power supply.

TECH TIP

Watching the wattage

Many manufacturers overstate the wattage. The wattage advertised is *not* the wattage available at higher temperatures, such as when mounted inside a computer. Research a model before purchasing.

Some power supplies are listed as being dual or triple (or tri) rail. A **dual-rail power supply** has two +12V output lines that are monitored for an over-current condition. A triple-rail power supply simply has three +12V output lines monitored. Keep in mind that most manufacturers do not have two or more independent 12V sources; they all derive from the same 12V source but have independent output lines. Figure 5.30 shows how the +12V rails might be used.

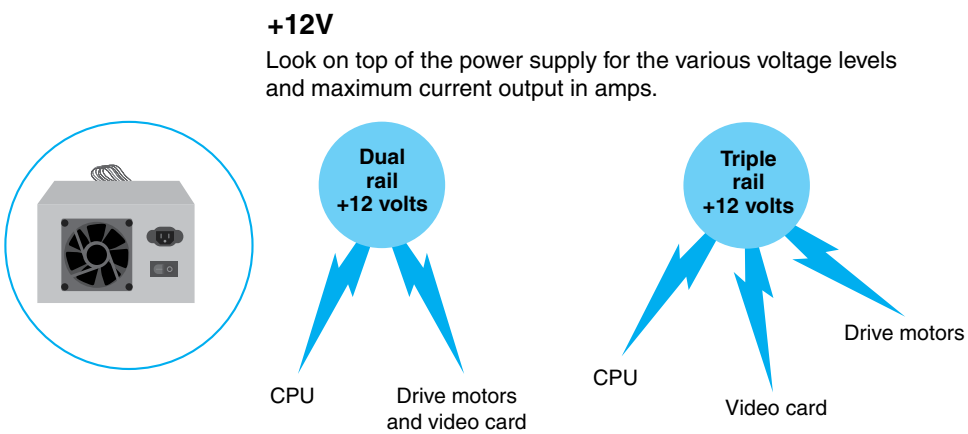


FIGURE 5.30 12V rails

Some people are interested in exactly how much power their system is consuming. Every device in a computer consumes power, and each device may use one or more different voltage levels (for

example, +5V, –5V, +12V, –12V, and +3.3V). A power supply has a maximum amperage for each voltage level (for example, 30 amps at +5 volts and 41 amps at +12V). To determine the maximum power being used, in watts, multiply the amps by the volts. If you add all the maximum power levels, the amount will be greater than the power supply's rating. This means that you cannot use the maximum power at every single voltage level; however, because –5V and –12V are not used very often, normally this is not a problem.

Number of Devices/Types of Devices to Be Powered

To determine the power being consumed, you must research every device to determine how much current it uses at a specific voltage level. Internet power calculators are available to help with this task. It is important to have a power supply powerful enough for the number of devices and types of devices installed in the computer. Table 5.5 lists sample computer component power requirements.

TABLE 5.5 Sample computer component power requirements

Component	Power consumption
Motherboard (without processor)	5W to 150W
Processor	10W to 140W
PATA IDE hard drive	3W to 30W
SATA hard drive	2W to 15W
Optical drive	10W to 30W
Nonvideo adapter	4W to 25W
PCIe video card with one power connector	50W to 150W
PCIe video card with two power connectors	100W to 300W
Extra fan	3W
RAM module	15W

Choosing a Power Supply

When choosing a power supply, the first things to consider are size and form factor because the power supply has to fit in the case. A computer (especially a server or network equipment) may have a **redundant power supply** that can be used if one power supply fails. The second thing to consider is wattage: You should buy a power supply that has the same wattage as or more wattage than the original power supply.

TECH TIP

All power supplies are not created equal

A technician needs to replace a power supply with one that provides an equal or greater amount of power. Search the internet for power supply reviews. A general rule of thumb is that if two power supplies are equal in wattage, the heavier one is better because it uses a bigger transformer, bigger heat sinks, and higher-quality components.

The 80 PLUS is a power supply **energy efficiency rating** system that has been incorporated into ENERGY STAR specifications. Efficiency involves converting more AC to DC. The rating system consists of six levels of efficiency, with 80 PLUS Titanium being the highest. Each level must provide a particular level of efficiency at a specific amount of load. (Load is the number of components being used simultaneously that require power.)

Just because a power supply is not certified as 80 PLUS does not mean that it is not an energy-efficient power supply, but the level can give you an idea of the difference between power supplies. When choosing a power supply, the most important things to consider are as follows:

- Size and form factor
- Wattage
- Number and type of connectors
- Energy efficiency
- Number of 12V rails monitored for an over-current condition

Some people like extra features such as colored lights inside the power supply, an internal fan, and/or ports for detachable cables. A **modular power supply** comes with detachable cables (see Figure 5.31) so that cables that are not used are simply not attached to the power supply to aid in cable management.

FIGURE 5.31 Modular power supply with detachable cable ports

TECH TIP

Power values for energy-efficient monitors

Always keep the screen saver timeout value shorter than the power saver timeout value, especially with green (energy-efficient) monitors!

Power Protection

Power supplies have built-in protection against adverse power conditions. However, the best protection for a computer is to unplug it during a power outage or thunderstorm. Surge protectors and uninterruptible power supplies (UPSs) are commonly used to protect against adverse power conditions. A line conditioner can also be used. Each device has a specific purpose and guards against certain conditions. A technician must be familiar with each device in order to make recommendations for customers. Figure 5.32 shows a surge protector, and Chapter 19, "Operational Procedures," covers these devices in more detail.

FIGURE 5.32 Tripp Lite surge protector

Symptoms of Power Supply Problems

A power supply is sometimes a source of unusual problems, causing issues ranging from those not noticed by a user to those that shut down a system. The following is a list of symptoms of power supply problems:

- The power light is off and/or the device won't turn on (**no power** or **blank screen**).
- The power supply fan does not turn when the computer is powered on.
- The computer sounds a continuous **POST beep**. (This could also be a bad motherboard or a stuck key on the keyboard.)
- When the computer powers on, it does not beep at all. (This could also be a bad motherboard.)
- When the computer powers on, it sounds repeating short beeps. (This could also be a bad motherboard.)
- During POST, one of the POST checks is a power good signal from the power supply, and an error message indicates that the power supply did not pass the POST test.
- The **computer reboots**, powers down without warning, has **random shutdowns**, or reboots continuously.
- The power supply fan is noisy (emits a loud or **unusual noise**).
- The power supply is too hot to touch.
- The computer emits a **burning smell**, emits smoke, or is **overheating**.
- The power supply fan spins, but no power goes to other devices.
- The monitor has a power light, but nothing appears on the monitor, and no PC power light illuminates.

Checking Power Supply Voltages

Refer to Figure 5.25 and notice how +3.3V, +5V, –5V, +12V, and –12V are output and supplied to the motherboard (with +5V and +12V being the most common voltages supplied to devices). The motherboard and adapters use +3.3V and +5V, but –5V is seldom used. Hard drives and optical

drives commonly use +5V and +12V. The +12 voltage is used to operate the device motors found in drives, the CPU, internal cooling fans, and the graphics card. Drives are now being made that use +5V motors. Chips use +5V and +3.3V, and +3.3V is also used for memory, PCI/PCIe adapters, and some laptop fans. The negative voltages are seldom used.

A technician must occasionally check voltages in a system. There are four basic checks for power supply situations: wall outlet AC voltage, DC voltages going to the motherboard, DC voltages going to a device, and ground or lack of voltage with an outlet tester. A **power supply tester** can be used to check DC power levels on the different power supply connectors. Figure 5.33 shows a PC power supply tester. The type of connectors varies from vendor to vendor, so make sure you get a tester that can handle Molex, SATA, and main system power at a minimum.

FIGURE 5.33 PC power supply tester

Solving Power Supply Problems

When you suspect that a problem is caused by a power supply, swap out the power supply, make the customer happy, and be on your way! Power problems are not usually difficult to detect or troubleshoot.

TECH TIP

Do not disassemble a power supply

Power supplies are not normally disassembled. Manufacturers often rivet them shut. Even when a power supply can be disassembled, you should not take it apart unless you have a background in electronics.

Do not overlook the most obvious power supply symptoms. Start by checking the computer power light. If it is off, check the power supply's fan by placing your palm at the back of the computer. If the fan is turning, it means the wall outlet is providing power to the computer, and you can assume that the wall outlet is functioning. Check the motherboard for LEDs and refer to the manual for their meaning. Test the power outlet with another device. Ensure that the power cord is inserted fully into the wall outlet and the computer. If you suspect that the wall outlet is faulty, use an **AC circuit tester** to verify that the wall outlet is wired properly.

The following troubleshooting questions can help you determine the location of a power problem:

> Did the power supply work before? If not, check the input voltage selector switch on the power supply and verify that it is on the proper setting.

- Is the power supply's fan turning? If yes, check voltages going to the motherboard. If they are good, maybe just the power supply fan is bad. If the power supply's fan is not turning, check the wall outlet for proper AC voltages. Be advised, though, that some modern PSUs have a fan control that only activates the fan under load or when a specific temperature is reached, so a non-spinning fan doesn't necessarily indicate a problem
- Is a surge strip used? If so, check to see whether the surge strip is powered on and then try a different outlet in the surge strip or replace the surge strip.
- Is the computer's power cord okay? Verify that the power cord plugs snugly into the outlet and into the back of the computer. Swap the power cord to verify that it is functioning.
- Is the front panel power button stuck?
- Are the voltages going to the motherboard at the proper levels? If they are low, something might be overloading the power supply. Disconnect the power cable to one device and re-check the voltages. Replace the power cable to the device. Remove the power cable from another device and recheck the motherboard voltages. Continue doing this until the power cord for each device has been disconnected and the motherboard voltages have been checked. A single device can short out the power supply and cause the system to malfunction. Replace any device that draws down the power supply's output voltage and draws too much current. If none of the devices is the cause of the problem, replace the power supply. If replacing the power supply does not solve the problem, replace the motherboard.

If a computer does not boot normally but does boot when you press Ctrl+Alt+Del, the power good signal is likely the problem. Some motherboards are more sensitive to the power good signal than others. For example, say that a motherboard has been replaced, and the system does not boot. At first glance, the problem might appear to be a bad replacement board, but it could be caused by a power supply failing to output a consistent power good signal, so try replacing the power supply.

TECH TIP

Checking the power good signal

Check the power supply documentation to see whether the power supply outputs a power good signal, sometimes called a power OK signal, rather than the normal +5V. Turn on the computer. Check the power good signal on the main motherboard power connector (attached to the power supply). Do this before replacing the motherboard. A power supply with a power good signal below +3V needs to be replaced.

Sometimes when a computer comes out of sleep mode, not all devices respond, and the PC's power or reset button has to be pressed to reboot the computer. The following situations can cause this to happen:

- A screen saver conflicts with ACPI. Set the screen saver to *None* to see if it is causing the problem.
- One or more adapters/devices are not ACPI compliant.
- An adapter/device has an outdated driver.
- The system BIOS/UEFI or an installed adapter BIOS needs to be updated.

To see whether the screen saver causes a problem, use the Windows *Personalization* Settings > *Screen saver settings* link and set the screen saver option to *None*. Identifying a problematic adapter, device, or driver requires internet research. Check each adapter, device, and driver individually. Use the *Power Options* Control Panel to change the power scheme. For each device, check for a *Power Management* tab on the *Properties* dialog box and make changes if needed.

SOFT SKILLS: WRITTEN COMMUNICATION SKILLS

When technicians are in school, they seldom think that the skills they should be learning involve writing. However, in the workplace, technicians use **written communication** skills when they document problems and use email (see Figure 5.34). Advisory committees across the country say that in addition to having technical knowledge, it is important that technicians be able to communicate effectively both in writing and orally, and they should be comfortable working in a team environment.

FIGURE 5.34 Technicians must frequently provide written communication

Regardless of the size of a company, documentation is normally required. The documentation might be only the number of hours spent on a job and a basic description of what was done, but most companies require a bit more. Documentation should be written so others can read and understand it. Keep in mind that if another technician must handle another problem from the same customer, good documentation saves time and money. The following is a list of complaints from managers of technicians:

> Avoids doing documentation in a timely manner
> Does not provide adequate or accurate information on what was performed or tried
> Has poor spelling, grammar, capitalization, and punctuation skills
> Writes in short, choppy sentences, using technical jargon
> Does not provide updates on the status of a problem

You can use this list to determine where to improve your skills and avoid making the same mistakes.

Email is a common means of communication for technicians. The following is a list of guidelines for effective email communication:

> Do not use email when a meeting or a phone call is more appropriate.
> Include a short description of the email topic in the subject line.
> Do not write or respond to an email when you are angry.
> Send email only to the appropriate people; do not copy others unnecessarily.
> Stick to the point; do not digress.
> Use a spelling and grammar checker; if one is not included in the email client, write the email in a word processing application or online sentence checker and then paste the document into the body of the email.

- Use proper grammar, punctuation, and capitalization; do not write in all uppercase or all lowercase letters.
- Smile when you are typing. Your good attitude will come across in your writing.
- Focus on the task at hand. Read your note out loud if it is a critical one.
- Write each email as if you were putting the message on a billboard (see Figure 5.35); you never know how the content might be used or who might see it.

The number-one complaint about technical support staff is not their lack of technical skills but their lack of communication skills. Spend as much of your education practicing your communication skills as you do your technical skills.

FIGURE 5.35 Consider what you write; it could be publicized

Chapter Summary

- Wearing a wrist strap or staying in contact with unpainted metal keeps you and the computing device at the same electrical potential so you won't induce current into any part and weaken/damage it.
- EMI and RFI cause issues. Move the computer or the offending device and replace all slot covers/openings.
- When removing parts, have the right tools, lighting, and antistatic items, as well as ample workspace. Take notes. Don't use magnetized tools. Avoid jarring hard drives.
- Be careful when installing an I/O shield and be aware of standoffs when dealing with the motherboard.
- Preventive maintenance procedures prolong the life of a computer. Vacuum before spraying compressed air.
- An MSDS/SDS describes disposal and storage procedures and contains information about toxicity and health concerns. Cities/states have specific disposal rules for chemicals, batteries, electronics, and so on. Know the disposal rules in the area where you work.
- AC power goes into the power supply or mobile device power brick. DC power is provided to all internal parts of the computing device. Power is measured in watts.
- Continuity checks are done on cabling, and a good wire shows close to 0 ohms.
- A power supply converts AC to DC, distributes DC throughout a unit, and provides cooling. The power supply must be the correct form factor and able to supply the current amount of wattage for a particular voltage level, such as +5V or +12V. Multiple rails are commonly

available for +12V because the CPU commonly needs its own connection. The numbers and types of connectors vary, but converters can be purchased.

> Use ACPI to control power options through the BIOS/UEFI and the operating system. Wake on LAN and Wake on Ring are power features that allow a device to be powered up from a lowered power condition for a specific purpose.

> AC circuit testers, multimeters, and power supply testers are tools used with power problems.

> In all communications and written documentation, be professional and effective. Use proper capitalization, grammar, punctuation, and spelling.

A+ CERTIFICATION EXAM TIPS

- ✓ Review the chapter summary. Don't forget that other chapters have preventive maintenance tips, too, including the chapters on storage devices, multimedia devices, printers, and other peripherals.
- ✓ Always remember to power down a computer, remove the power cord/power brick/battery, and allow a laser printer to cool before performing maintenance. Preventive maintenance often involves using a vacuum and compressed air.
- ✓ Be familiar with proper component handling and storage, including the use of antistatic bags, ESD straps, and ESD mats.
- ✓ Know the purpose of a MSDS.
- ✓ Know that IT personnel must strictly adhere to local government regulations when handling electronic components, hazardous materials, and potentially environmentally sensitive equipment to ensure workplace safety and protect the environment.
- ✓ Wear safety goggles and an air filter mask for protection from airborne particles.
- ✓ Be aware of temperature risks, effects of humidity on electronic equipment, and when ventilation is needed.
- ✓ Be able to identify power connectors, including the Molex connector.
- ✓ Know that a 24-pin or a 20 + 4-pin cable can be used to connect to the 24-pin motherboard connector.
- ✓ Know that a power supply outputs 3.3V, 5V, and 12V. If a computer is to be used internationally, ensure that it supports an auto-switching power supply that accepts either 110V (North America) or 220VAC (Europe/Asia) as input voltage.
- ✓ Know where redundant power supplies are used, what a modular power supply is, how to select the appropriate wattage rating, and how to select an energy-efficient unit.
- ✓ Be familiar with common power problem symptoms, including lack of power (blank screen), unusual noise from the power supply or fan, POST beeps, burning smell, and the computer rebooting or powering down without warning.
- ✓ The following communication and professionalism skills are part of the 220-1202 exam: Use proper language and avoid jargon, acronyms, and slang when applicable; and provide proper documentation on the services provided.

Key Terms

3.3V, 4-pin 12V, 5V, 6-pin PCIe, 8-pin PCIe, 12V, 20 + 4 connector, 20-pin to 24-pin motherboard adapter, 24-pin motherboard connector, AC, AC circuit tester, ACPI, air filter mask, amp, antistatic bag, antistatic wrist strap, blank screen, burning smell, compressed air, computer reboot, continuity, DC, dual-rail power supply, EMI, energy efficiency rating, equipment grounding, ESD, ESD mat, ESD strap, front panel connector, I/O shield, maintenance kit, modular power supply, Molex, MSDS, no power, ohm, overheating, POST beep, power, power supply tester, preventive maintenance, random shutdown, redundant power supply, resistance, RFI, safety goggles, SATA connector, self-grounding, SDS, standoff, toner vacuum, unusual noise, volt, voltage, Wake on LAN, Wake on Ring, watt, wattage rating, written communication

Review Questions

1. What would happen if you removed the battery from a motherboard by accident?

_____

2. List three tasks commonly performed during preventive maintenance.

_____

_____

_____

3. Computers used in a grocery store warehouse for inventory control have a higher part failure rate than do the other company computers. Which of the following is most likely to help in this situation?
   - **a.** an antistatic wrist strap
   - **b.** a preventive maintenance plan
   - **c.** antistatic pads
   - **d.** high-wattage power supplies
4. Which of the following can prolong the life of a computer and conserve energy? (Choose all that apply.)
   - **a.** a preventive maintenance plan
   - **b.** antistatic mats and pads
   - **c.** upgraded power supply
   - **d.** a power plan
   - **e.** Li-ion replacement batteries
   - **f.** extra case fans
5. Which power component has a 24-pin connector?
   - **a.** main motherboard connector
   - **b.** power supply fan
   - **c.** case fan
   - **d.** AUX power for the CPU
6. A mechanical hard drive randomly becomes unavailable, and after replacing the drive, the technician suspects that the drive may not be getting 5 volts consistently. What could help in this situation?
   - **a.** a UPS
   - **b.** a surge protector
   - **c.** antistatic wipes
   - **d.** a preventive maintenance plan
   - **e.** a power supply tester
7. When disassembling a computer, which tool will help you remove the memory module?
   - **a.** magnetic screwdriver
   - **b.** needle-nose pliers
   - **c.** #1 or #2 Phillips screwdriver
   - **d.** antistatic wrist strap
8. A user had a motherboard problem last week, and a technician fixed it. Now the same computer has a different problem. The user reports that the USB ports on the front do not work anymore. What is the first thing you should check?
   - **a.** power supply
   - **b.** power connection to the front panel
   - **c.** motherboard connections to the front panel
   - **d.** voltage output from the power supply to the USB connectors

9. Which of the following items would be specialized for use with a laser printer?

[surge strip | vacuum | power supply tester | antistatic wrist strap]

10. Which two of the following would most likely cause an unusual noise on a desktop computer? (Choose two.)

[motherboard | USB drive | power supply | case fan | memory | PCIe adapter]

11. A computer will not power on. Which of the following would be used to check the wall outlet?

[power supply tester | UPS | multimeter | POST]

12. A computer will not power on. After checking the wall outlet and swapping the power cord, what would the technician use next?

a. resistance

b. power supply tester

c. antistatic wrist strap

d. magnetic screwdriver

e. nonmagnetic screwdriver

13. Which of the following is affected by the power supply wattage rating?

a. number of adapters and internal storage devices

b. number of power supply connectors

c. speed of the processor

d. type of power supply connectors

14. Which of the following would help with computer heat?

a. increasing the power supply wattage

b. upgrading to a larger power supply form factor

c. unplugging unused power connectors

d. installing case fans

15. [T | F] Power supply disassembly is a common requirement of a PC technician.

16. Consider the following email.

From: Cheryl a. Schmidt
To: Network Engineering Technology Faculty
Subj: [None]
We have little time to get the PMS done on the PCs and N/W gear. What software do you want?

Reword this email to illustrate good written communication skills.

_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

17. List three recommendations for good technical written communication.

_____

_____

_____

_____

_____

18. A computer is doing weird things, such as shutting down unexpectedly and hanging. You suspect a power problem. You check the power good (power OK) signal on the power supply's main motherboard connector. The voltage reading shows that you have power (+2.5 volts). What are you going to do next?

    a. Check the voltage coming out of a Molex or SATA connector.

    b. Check the wall outlet voltage.

    c. Replace the power supply.

    d. Check the power supply cable for resistance.

19. What is the purpose of the I/O shield?

    a. It prevents dust and dirt from coming in through the front computer ports.

    b. It provides grounding for motherboard ports.

    c. It prevents dust and dirt from coming into the power supply.

    d. It protects the technician from shocks.

20. Which two items would help a technician maintain personal safety while working on PCs and printers in an extremely dusty warehouse? (Choose two.)

    [vacuum | toner vacuum | safety goggles | antistatic wrist strap | air filter mask]

Exercises

Exercise 5.1 Identifying Power Supply Connectors

Objective: To be able to identify the purposes of common power supply connectors

Procedure: Identify the power supply connectors in Figure 5.36.

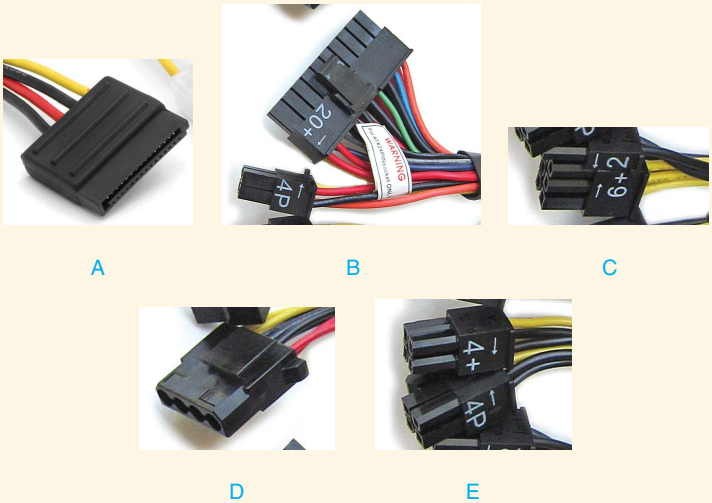


FIGURE 5.36 Identifying power connectors

____ 1. Molex for older optical drive

____ 2. SATA for hard drive

____ 3. PCIe video

____ 4. Main motherboard

____ 5. CPU

Exercise 5.2 Recognizing Computer Replacement Parts

Objective: To be able to recognize parts from a computer

Procedure: Use the following information to answer the questions.

The following parts were ordered by someone building their own computer:

a. Intel Core i7 4.4 GHz

b. ASUS Rampage V Extreme X99 (does not include USB 3.1 headers)

c. Triage 8 GB

d. Micro-ATX with two 3.5-inch" internal and two 5.25-inch" external drive bays

e. EVA 450 W

1. What part is designated by the letter a?

[memory | hard drive | optical drive | CPU]

2. What part is designated by the letter b?

[motherboard | processor | memory | hard drive]

3. What part is designated by the letter c?

[motherboard | optical drive | RAM | SATA hard drive | SSD]

4. What part is designated by the letter d?

   [RAM | case | all storage devices | power supply]

5. What part is designated by the letter e?

   [case | SSD | optical drive | power supply]

Exercise 5.3 Describing Computer Parts

Objective: To be able to recognize computer parts based on a description

Procedure: Match the description to the computer part affected during disassembly.

____ 1. 24-pin connector	a. power supply to motherboard cable
____ 2. I/O shield	b. front panel to motherboard cable
____ 3. antistatic bag	c. hard drive to motherboard cable
____ 4. ESD strap	d. goes around integrated ports
____ 5. grounding	e. attaches to wrist and computer
____ 6. hard drive	f. holds an adapter when not in use
____ 7. HDD LED	g. helps with EMI
____ 8. SATA 3	h. keeping in contact with the computer
____ 9. slot cover	i. attaches motherboard to case
____ 10. standoffs	j. might need guide rails

Activities

Flip the CLASSROOM

Internet Discovery

Objective: To obtain specific information on the internet regarding a computer or its associated parts

Parts: Computer with internet access

Procedure: Complete the following procedure and answer the following questions.

1. Locate an internet site that provides tips for doing computer preventive maintenance.

   Write two of the best tips and the URL where you found the information.

   _____

   _____

2. Locate an internet site where you can buy a computer toolkit that includes an antistatic wrist strap.

   List the URL where you found the toolkit and at least three sizes of screwdrivers or bits provided.

   _____

   _____

   _____

3. Locate a power supply tester that includes a SATA connector.

   List the manufacturer and model.

   _____

   _____

4. Find a website on good netiquette.

   Give three recommendations for good netiquette and the name of the website (not the URL) where you found them.

   _____

   _____

   _____

   _____

   _____

5. You have just started working at a place that uses the HP Elite 800 G2 23-inch nontouch all-in-one computer.

   You have been sent to do power checks on the power supply of one of these units. How do you get the cover off? Explain in detail, using complete sentences.

   _____

   _____

   _____

   _____

   _____

   What recommendation does HP give for cleaning stubborn stains that might be found on computer cases in the maintenance shop?

   _____

   According to the documentation for the HP Elite 800 G2, how does the process of removing an AMD processor differ from the process of removing an Intel processor?

   _____

   _____

   _____

Soft Skills

Objective: To enhance and fine-tune a future technician's ability to listen, communicate in both written and oral forms, and support people who use computers in a professional manner

Activities:

1. Prepare a business proposal for a replacement power supply for a specific computer. State the computer and present your proposal to the class.
2. Write an informal report on the skills learned while taking apart a computer and reassembling it. Share your best practices with a small group.
3. Work in teams to decide the best way to inform a customer about the differences between an ATX power supply and an SFX power supply. Present your description to the class as if you were talking to the customer. You might consider showing motherboards and cases to help illustrate your point. Each team member must contribute. Each classmate votes for the best team explanation.

Critical Thinking Skills

Objective: To analyze and evaluate information as well as apply learned information to new or different situations

Activities:

1. Use the internet to find a description of a particular computer that lists each device that is installed and the type of motherboard, integrated ports, and so on. Then locate a power supply calculator. Find a replacement power supply, based on the calculations performed. Write the details of what you looked for in the replacement power supply, the power supply, vendor, number and type of connectors, and cost.

   _____

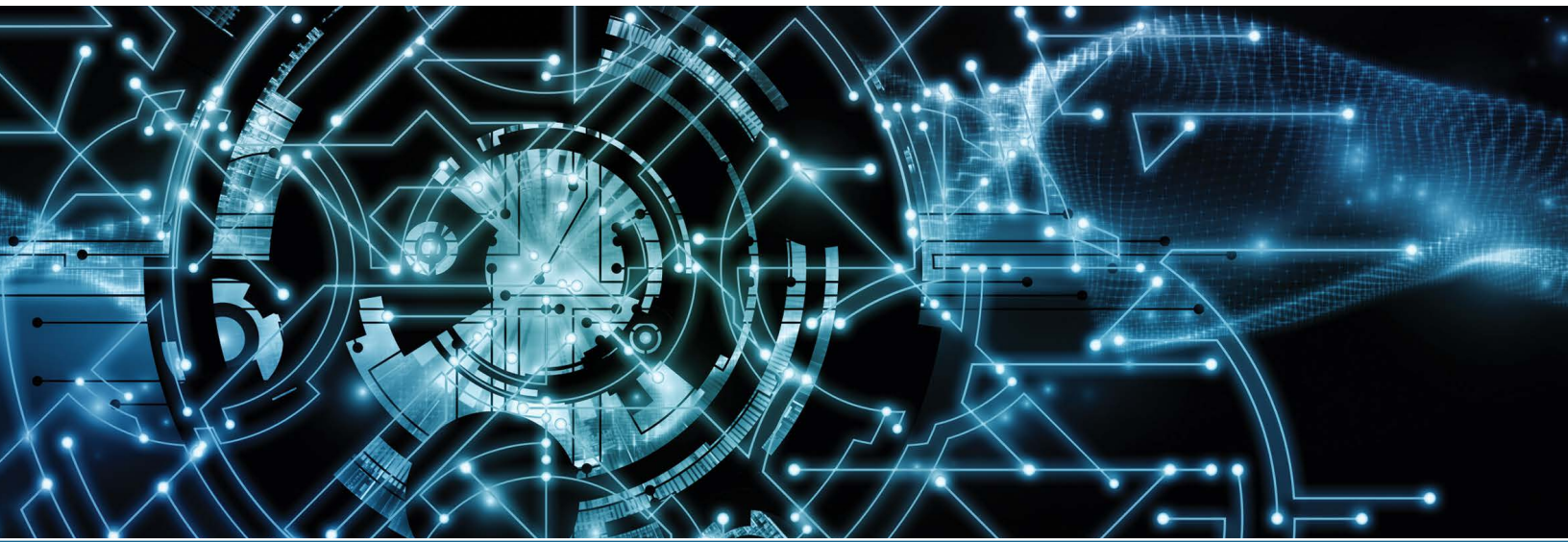
   _____

2. For one of the computers in the classroom, locate the documentation on how to disassemble it. Looking through the documentation, find at least three things that are good tips that you might not have thought of immediately if you were disassembling the computer. Then find at least three safety tips. Place all of this information in an outline. An alternative is to be creative and present the tips graphically on one page or presentation slide.

   _____

This page intentionally left blank

6 Memory



In this chapter you will learn:

- Different memory technologies
- How to plan for a memory installation or upgrade
- How to install and remove memory modules
- How to optimize memory for Windows platforms
- Best practices for troubleshooting memory problems
- The benefits of teamwork

CompTIA Exam Objectives:

- ✓ 1201-3.3 Compare and contrast RAM characteristics.
- ✓ 1201-3.4 Compare and contrast storage devices.
- ✓ 1201-5.1 Given a scenario, troubleshoot motherboards, RAM, CPUs, and power.
- ✓ 1202-1.3 Compare and contrast basic features of Microsoft Windows editions.
- ✓ 1202-1.4 Given a scenario, use Microsoft Windows operating system features and tools.
- ✓ 1202-4.7 Given a scenario, use proper communication techniques and professionalism.

Memory Overview

Computer systems need software to operate, and software resides in memory. A technician must understand memory terminology, determine the optimum amount of memory for a system, install the memory, fine-tune it for the best performance, and troubleshoot and solve any memory problems.

The main type of memory found on the motherboard is random-access memory (**RAM**), specifically dynamic RAM (**DRAM**). The other type of RAM is static RAM (**SRAM**). DRAM is less expensive but slower than SRAM. With DRAM, the 1s and 0s inside the chip must be refreshed. Over time, the charge, which represents information inside a DRAM chip, leaks out. The information, which is stored in 1s and 0s, is periodically rewritten to the memory chip through the refresh process. The refreshing is accomplished inside the DRAM while other processing occurs. Refreshing is one reason DRAM chips are slower than SRAM.

Most memory on a motherboard is DRAM, but a small amount of SRAM can be found inside the processor, just outside the processor inside the processor housing, and sometimes on the motherboard. SRAM is also known as **cache memory**. Cache memory holds the most frequently used data so the CPU does not return to the slower DRAM chips to obtain the data. For example, on a motherboard with a bus speed of 233 MHz, accessing DRAM could take as long as 90 nanoseconds. (A nanosecond, abbreviated ns, is one-billionth of a second.) Accessing the same information in cache could take as little as 23 nanoseconds. Figure 6.1 shows a motherboard with DRAM and a processor that contains SRAM.

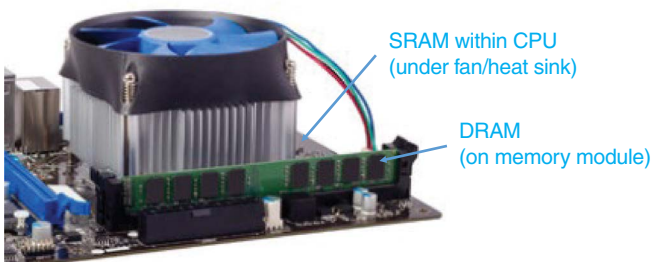


FIGURE 6.1 DRAM and SRAM

As noted in Chapter 3, "On the Motherboard," to determine memory requirements, you must consider the operating system, applications, and installed hardware. Memory is one of the most critical things on the motherboard that can easily be upgraded. Let's start with the physical memory module.

TECH TIP

Don't forget hard drive space and video memory

RAM is only one piece of the puzzle. All of a computer's parts—including RAM, hard drive space, and video memory—must work together to provide good (optimal) system performance.

Memory Physical Packaging

The memory used on motherboards today comes in packaging known as a dual in-line memory module (**DIMM**), which has 168, 184, 240, or 288 pins. Memory can also be called a memory stick, or a technician might call one memory module a stick of memory or simply RAM. Laptops

and printers use a smaller DIMM called a small outline DIMM (**SODIMM**). Figure 6.2 shows the progression of memory packaging. Figure 6.3 shows a SODIMM.

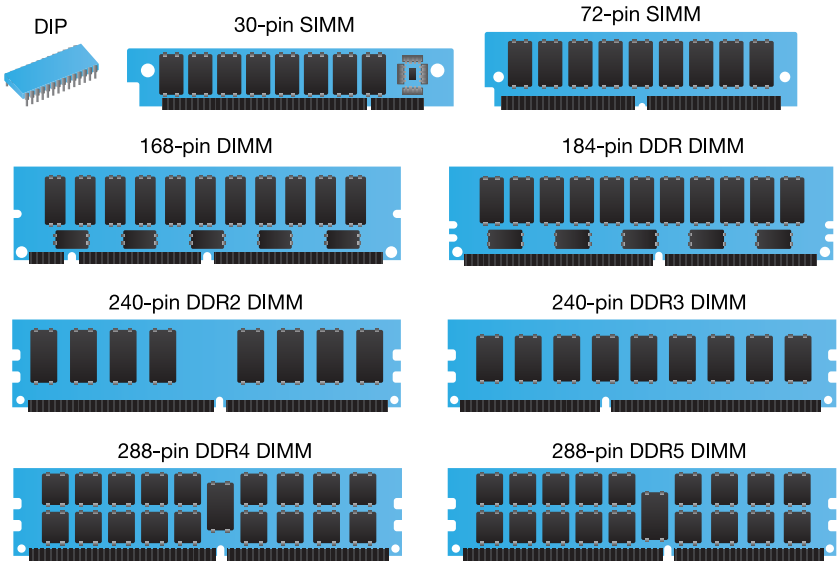


FIGURE 6.2 Memory chips/modules

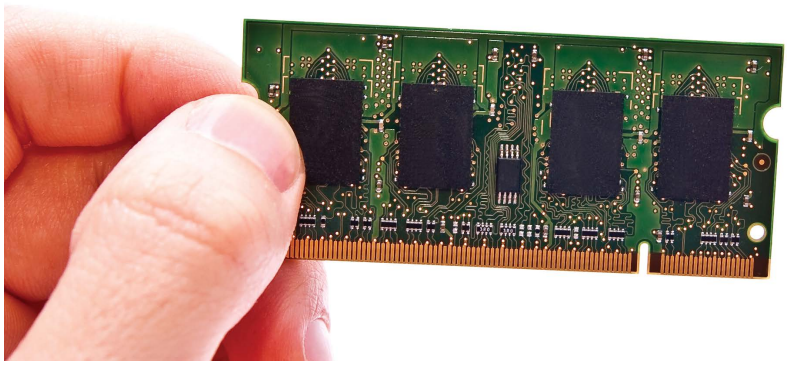


FIGURE 6.3 SODIMM

Planning a Memory Installation

Now that you know a little about memory types, let us look at how to go about planning a memory installation. Some key points follow:

> Refer to the system or motherboard documentation to see what type of memory is supported.
> Determine what features are supported.
> Determine how much memory is needed.
> Determine what memory module(s) you need and how many of them.
> Research prices and purchase the memory module(s) you needed.

Planning the Memory Installation: Memory Module Types

Technology has provided faster DRAM speeds without increasing the cost too greatly. Table 6.1 lists some of the memory technologies available today. Note that CompTIA calls these DDR types double data rate iterations (**DDR iterations**).

TABLE 6.1 Memory module types

Technology	Explanation
Synchronous DRAM (SDRAM)	Performs very fast burst memory access. New memory addresses are placed on the bus but before the prior memory address retrieval and execution is complete. SDRAM synchronizes its operation with the CPU clock signal to speed up memory access. Used with DIMMs.
Double data rate (DDR)	Sometimes called DDR SDRAM or DDR RAM. DDR memory can send twice as much data because data is transmitted on both sides of the clock signal (that is, on the rising and falling edges instead of just on the rising edge).
DDR2	Sometimes called DDR2 RAM. DDR2 uses 240-pin DIMMs and is not compatible with DDR.
DDR3	Uses 240-pin DIMMs and is not compatible with DDR2 or DDR. Supports multicore processor-based systems and more efficient power utilization (1.5V).
DDR4	Operates at a lower voltage (1.2V) and faster speeds than DDR3 modules. DDR4 uses 288-pin DIMMs and has a unique memory slot.
DDR5	Operates at a lower voltage (1.1V) with increased speeds compared to DDR4 modules. Uses 288 pins like DDR4 in a unique slot. It has twice the bank groups as DDR4 with higher bandwidth that works more efficiently with multicore processors.
DDR6	Expected to operate at a lower voltage, faster speeds, and increased channels compared to DDR5.

TECH TIP

Using a lower-voltage chip

DDR4 and DDR5 memory can be purchased as modules that use a lower voltage than standard modules. The motherboard must support this feature. These modules will have an L at the end (DDR4L, for example) and are commonly used in laptops and mobile devices.

Even though all the DDR modules have different numbers of pins, they are the same physical size. A DDR5 module does not fit in a DDR2, DDR3, or DDR4 slot. You have to make sure you have the right kind of module for the motherboard. Figure 6.4 shows DDR4 DIMM. Notice in Figure 6.4 the metal casing, called a heat spreader, on the outside of the memory module. Aluminum or copper is commonly used on heat spreaders in order to dissipate heat away from the memory.

FIGURE 6.4 DDR4 DIMM

TECH TIP

Using the right type of memory chips

The chipset and motherboard design are very specific about what type, speed, and features the memory chips can have. Refer to the motherboard documentation.

Table 6.2 lists some examples of DIMM models.

TABLE 6.2 DIMMs

Memory type	Data rate
DDR4-2400	2.4 GT/s
DDR4-2666	2.66 GT/s
DDR4-3200	3.2 GT/s
DDR5-4800	4.8 GT/s
DDR5-6000	6 GT/s
DDR5-7500	7.5 GT/s

Older DIMMs can be shown with either the PC*X*- or DDR*X*- designation, and which type to buy can be confusing. A brief explanation might help. DDR3-2000 is a type of DDR3 memory that could also be shown with the designation PC3-16000, where 16,000 MB/s is the theoretical bandwidth of the memory chip. The good news about DDR4 and DDR5 is that the module names now match the standard names.

Planning the Memory Installation: Memory Features

In addition to determining what type of memory chips are going to be used, you must determine what features the memory chips might have. The computer system or motherboard documentation delineates what features are supported. Table 6.3 helps characterize memory features.

TABLE 6.3 Memory features

Feature	Explanation
Error correction code RAM (**ECC RAM**)	An alternative to parity checking that uses a mathematical algorithm to verify data accuracy. ECC can detect up to 4-bit memory errors and correct 1-bit memory errors. ECC is used in higher-end computers and network servers. Non-ECC memory modules are simply modules that do not support ECC.
Non-ECC RAM	Memory that does not use ECC error checking (and typically doesn't do any type of error checking at all). If the advertisement does not say it is ECC, you can assume that the module doesn't do error checking.
Unbuffered memory	Memory in which data is sent immediately through the memory chip. Unbuffered memory is faster than registered or fully buffered memory.
Buffered memory (registered memory)	A memory module that has extra chips (registers) near the bottom of the module that delay all data transfers by one clock tick to ensure accuracy. Buffered memory is used in servers and high-end computers. If you install a registered memory module into a system that allows both registered and unbuffered memory, all memory must be registered modules. These modules are sometimes advertised as fully buffered DIMMs (FBDIMMs).

Feature	Explanation
Single rank	A memory module that has one set of DRAM chips. If an advertisement does not state the rank or says 1R, assume the module is single rank.
Dual rank	A memory module that has two single-rank sets. (The CPU usually accesses only one rank at a time.)
Serial presence detect (**SPD**)	A module that has an extra EEPROM that holds information about the DIMM (capacity, voltage, refresh rates, and so on). The BIOS/UEFI reads and uses this data for best performance. Some modules have thermal sensors (sometimes listed as TS in an advertisement) used to monitor and report memory heat conditions.
Dual-voltage memory	A module (which might be listed with an L) that can operate at a lower voltage level (thus with less heat) if the motherboard supports this feature. Note that all installed modules must also support the lower voltage for the system to operate in this mode.
Extreme memory profile (XMP)	A type of memory module that allows the BIOS/UEFI to configure voltage and timing settings in order to overclock the memory.

A memory module might use more than one of the categories listed in Tables 6.2 and 6.3. For example, a DIMM could be a DDR4 module, could be registered, and could support ECC for error detection and correction. Most registered memory also uses the ECC technology. Memory modules can support either ECC or non-ECC, and they can be registered or unbuffered memory. It is important that you research this *before* you purchase memory.

TECH TIP

Motherboard documentation is your best friend

Don't second-guess memory specifications. Use the motherboard documentation to determine which memory module(s) to buy.

Planning for Memory: How Much Memory to Install

When you want to improve the performance of a computer, adding memory is one of the easiest upgrades. The amount of memory needed depends on the operating system, applications, number of applications open at the same time, type of computer, and maximum amount allowed by the motherboard.

Memory modules come in specific capacities, such as the ones shown in Figure 6.5. Notice that the capacities double. If someone installed four 512 MB modules, for example, the total amount installed would be 2 GB (as two 512 MB modules equals 1 GB). If a motherboard has four memory expansion slots and the maximum the motherboard supports is 32 GB, then using two 16 GB sticks would be preferable to using a single 32 GB stick because this configuration allows for dual-channel operation (covered in the next section), which significantly improves memory bandwidth and overall system performance. Also, using multiple sticks of the same size can provide better stability and potentially higher speeds compared to using multiple sticks of different sizes.

The operating system you use determines, to a great extent, the amount of memory required. Generally, the older or less powerful the operating system, the smaller the amount of RAM you need. Table 6.4 provides a starting point for calculating memory requirements. Remember that you will need more memory as you begin to run more applications simultaneously and require more memory if the computer will be used to game or do photo/video/sound manipulation. Notice that Apple computers (macOS) have similar memory recommendations to PCs.

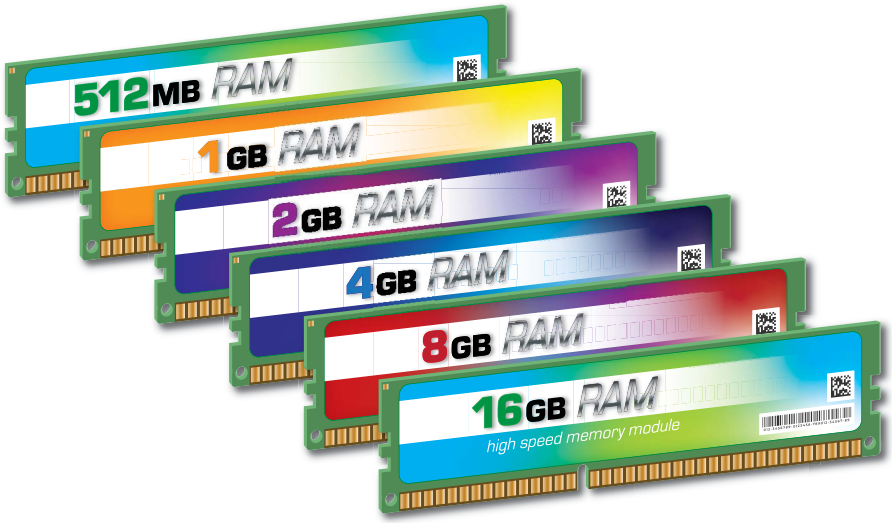


FIGURE 6.5 Memory module capacities

TABLE 6.4 Minimum operating system starting memory recommendations

Operating system	Minimum amount of RAM to start calculations
Windows 10	2 GB
Windows 11	4 GB
macOS Sierra/Catalina/Big Sur	4 GB
macOS Ventura/Sonoma/Sequoia	8 GB
Linux	Depending on the version, from 64 MB

NOTE The memory recommendations shown in Table 6.4 are not the minimum requirements listed by the operating system vendors.

When upgrading memory, you need to know a couple of key pieces of information:

> How much memory are you starting with?
> How many motherboard RAM slots are currently being used, and are there any slots free?
> What is the maximum amount of memory that your motherboard supports?

Table 6.5 shows the Windows memory limits.

TECH TIP

Windows might have memory limitations

Even if the motherboard allows more memory, your operating system has limitations. Upgrade the operating system if this is the case.

TABLE 6.5 Windows memory limits

Operating system	Memory limitation
Windows 10/11 Home	128 GB
Windows 10 Pro/Enterprise Windows 11 Pro/Education	2 TB
Windows 11 Pro for Workstations/Enterprise	6 TB

To see the amount of installed memory, access the *System Information* window from the command prompt by typing `msinfo32` and pressing [Enter]. Figure 6.6 shows the System Information window for a computer system that currently has 24 GB of RAM installed.

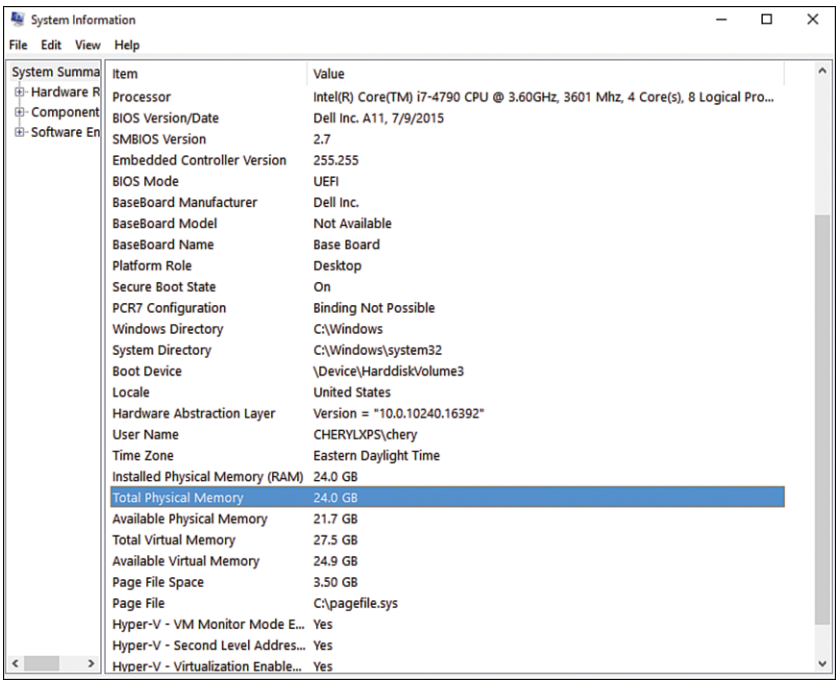


FIGURE 6.6 System Information window

TECH TIP

Every motherboard has a maximum

Each motherboard supports a maximum amount of memory. You must check the computer or motherboard documentation to see how much this is. There is not a workaround for this limitation. If you want more memory than the motherboard allows, you must upgrade to a different motherboard.

Figure 6.7 shows a sample advertisement for a micro-ATX motherboard. The *Specifications* tab commonly shows the type of memory supported (and may also show the exact speeds supported), the maximum amount of memory, and the number of memory slots.

Overview | Specifications | Warranty

Specifications

Motherboard Specifications	
Motherboard Type	Desktop
Processor Socket	Intel
Processor Interface	LGA 1700
Form Factor	Micro ATX
Processors Supported	12/13/14th Gen Intel Core
Chipset	
Northbridge	B760
Memory	
Memory Type	DDR5
Maximum Memory Supported	256 GB
Number of Slots	4

FIGURE 6.7 Sample motherboard memory specifications

TECH TIP

Beware of RAM over 4 GB

Do not install over 4 GB on a computer with a 32-bit operating system such as 32-bit Windows. The operating system will not be able to recognize anything over 4 GB.

To determine how many slots you are currently using and whether you have any free, you need to either (1) access the BIOS/UEFI to see this information; (2) use the *Task Manager* > *Performance* tab; or (3) remove the computer cover and look at the motherboard to see which memory slots have installed modules and whether there are any free slots. A memory sales website may have a tool that determines the type of memory you are using and makes recommendations. However, because you want to be a proficient technician, you can determine this for yourself.

Planning for Memory: Channel Configurations

A motherboard has a certain number of memory slots, determined by its manufacturer. The type of memory module that inserts into a slot and the features that the module has are determined by the motherboard manufacturer.

Most motherboards today support dual-channel memory. **Dual-channel** allows the motherboard memory controller chip to handle processing of memory requests more efficiently by using two memory paths simultaneously. For example, say that a motherboard has four memory slots. With dual-channeling, a motherboard with four memory slots is divided into two channels, and each channel has two slots. Figure 6.8 shows this concept.

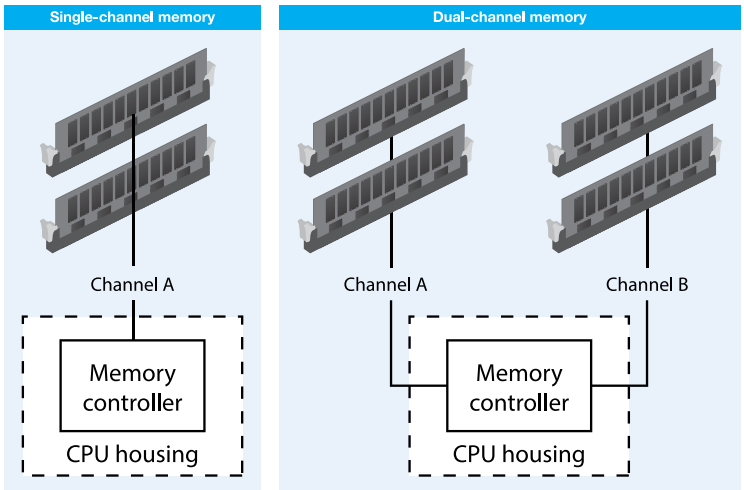


FIGURE 6.8 Dual-channel memory

Dual-channeling increases a system's performance. However, it speeds things up best if the memory modules match exactly—same memory type, same memory features, same speed, and same capacity. Figure 6.9 illustrates this concept.

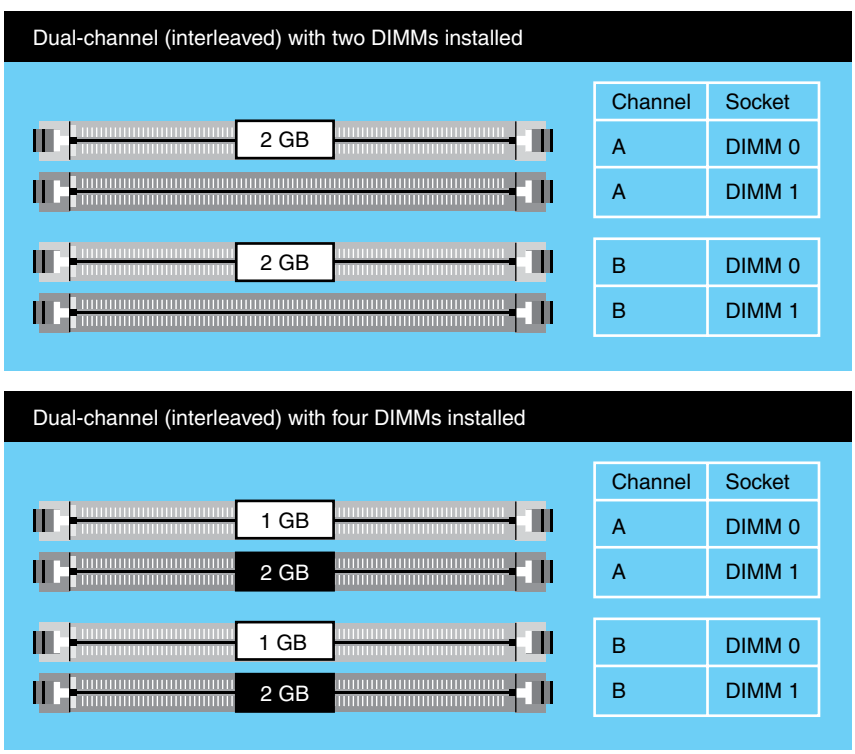


FIGURE 6.9 Dual-channeling

Notice in Figure 6.9 that in the first example, two identical memory modules are inserted: one memory module in Channel A and the other in Channel B. Some motherboard manufacturers require that the memory modules match in all respects—manufacturer, timing, and capacity—in order to support dual-channeling. If they support modules that don't match perfectly, the channel will operate at the lower specifications.

In the second example in Figure 6.9, four DIMMs are installed. Notice that the Channel A total capacity matches the Channel B total capacity (3 GB in both channels, for a total of 6 GB).

TECH TIP

Use exact memory module pairs with dual-channeling

Channel A and Channel B (sometimes labeled Channel 0 and Channel 1) should have matching memory modules. Buy a kit (a package of pre-tested memory modules that are guaranteed to work together) to ensure that the two modules are the same.

To see why it's so important to refer to the motherboard documentation when planning for the correct amount of memory, let's look at an example. Figure 6.10 shows a motherboard layout with four memory slots that have different labeling than shown in Figure 6.9. Motherboard manufacturers can label their motherboards any way they want. This is one of the reasons documentation is so important.

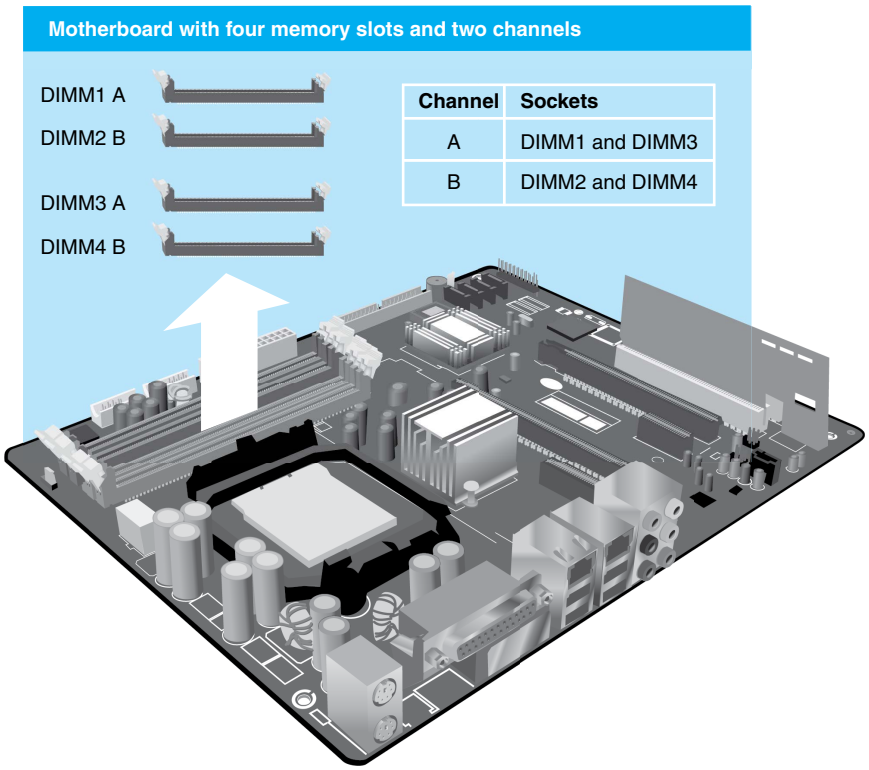


FIGURE 6.10 Motherboard with four memory slots and two channels

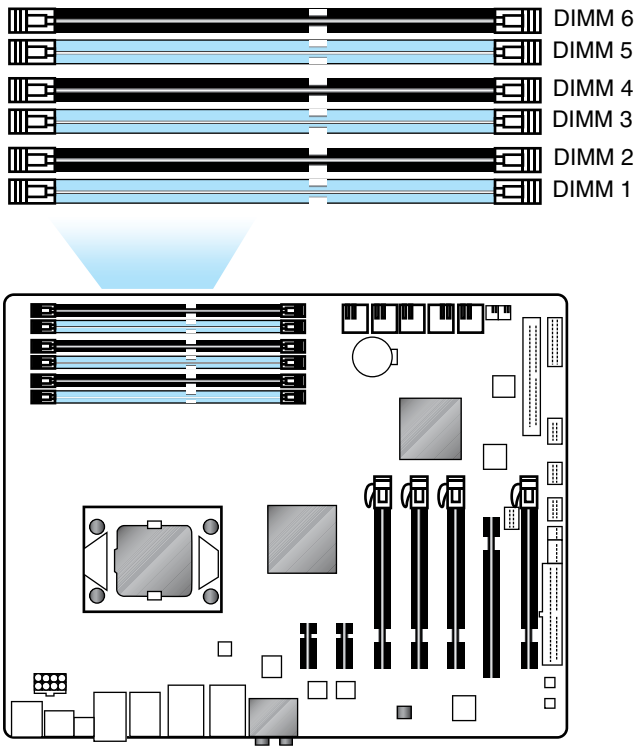
The motherboard in Figure 6.10 allows 512 MB, 1 GB, and 2 GB unbuffered non-ECC DDR3 DIMMs, for a maximum of 8 GB. Say that the customer wants 2 GB of RAM. What could you do? How many memory modules would you buy, and what capacities? Table 6.6 shows the possible solutions. The best solution is the second one because it has the largest-capacity chips and takes advantage of dual-channeling, with slots left over for more upgrading.

TABLE 6.6 Possible solutions

Solution	Number and size of memory module(s) needed
1	Four 512 MB DIMMs installed in DIMM1, DIMM2, DIMM3, and DIMM4 slots (dual-channeling)
2*	Two 1 GB DIMMs installed in DIMM1 and DIMM2 slots (dual-channeling)
3	Two 1 GB DIMMs installed in DIMM1 and DIMM3 slots (not dual-channeling)
4	One 2 GB DIMM installed in DIMM1 (not dual-channeling)

*Best solution

Many newer motherboards and server motherboards support **triple-channel** memory, where three memory modules work together, or **quad-channel** memory, where four memory modules are accessed simultaneously; this feature is most commonly found on server motherboards. Figure 6.11 shows a motherboard that has six memory expansion slots and supports triple-channeling.



Dual-channel Configuration	DIMM 1	DIMM 2	DIMM 3	DIMM 4	DIMM 5	DIMM 6
Two modules	X		X			
Four modules	X	X	X	X		

Triple-channel Configuration	DIMM 1	DIMM 2	DIMM 3	DIMM 4	DIMM 5	DIMM 6
Three modules	X		X		X	
Six modules	X	X	X	X	X	X

FIGURE 6.11 Motherboard with six memory slots and three channels

TECH TIP

Motherboard documentation with 1DPC/2DPC

If the motherboard documentation states 1DPC 1R max speed up to 4,800+ MHz or 2DPC 2R max speed up to 4,000+ MHz, the 1 or 2 DPC is how many memory slots are in each channel (1 or 2 DIMMs per channel). The 1R or 2R refers to single rank or dual-rank memory modules.

Planning for Memory: Researching and Buying Memory

The researching and buying step in the process of planning for a memory installation/upgrade is the step most likely to make your head spin. Different websites list memory differently. A few, such as Kingston Technology (kingston.com) and Crucial (crucial.com), specialize in memory and make it as painless as possible. They even provide tools that will scan your computer and recommend compatible memory or storage upgrades! Nevertheless, as a technician, you should be familiar with all aspects of memory and memory advertisements.

TECH TIP

Buying the fastest type of memory a motherboard allows

Buying memory that is faster than the motherboard allows is like taking a race car on a one-lane unpaved road: The car has the ability to go faster, but it is not feasible with the type of road being used.

A confusing aspect of buying memory is memory speed. Memory speed can be represented using MHz or the PC rating. The higher the number, the faster the speed of the module. Table 6.7 shows examples of how different amounts of memory might be advertised.

TABLE 6.7 Sample DIMM advertisements

Memory module	How it might be advertised
2 GB	DDR3 PC3-10600 > CL9 > UNBUFFERED > NON-ECC > DDR3-1333 > 1.35V > 256 Megx64
2 GB kit (1 GBx2)	DDR3 PC3-10600 > CL9 > REGISTERED > ECC > DDR3-1333 > 1.5V > 128 Megx72
4 GB	PC4-17000 2133MHz uDIMM single-rank
16 GB (2x8 GB)	DDR4 3200MHz Desktop Memory Kit CL16
16 GB	DDR5 PC5-38400 CL40 uDIMM 1.1V non-ECC unbuffered

Notice in Table 6.7 how the ads either list the memory module as a DDR4 or PC4 for DDR4 type. If an ad doesn't mention ECC, then you can assume that the memory does no error checking. Today's electronics are very accurate, and for most non-financial applications, **non-parity** (no error checking) memory is fine. uDIMM indicates unregistered or unbuffered memory.

The second and fourth rows in Table 6.7 list kits for a motherboard that has dual-channeling capabilities. The 16 GB kit includes two 8 GB memory modules, for a total of 16 GB. A couple of the advertisements list the **CL rating**. CL (column address strobe [CAS] latency) is the amount of time (based on clock cycles) that passes before the processor moves on to the next memory address.

TECH TIP

CL ratings and speed

The lower the CL rating, the faster the memory. Think of access time as a track meet: The person with the lowest time wins the race and is considered to be the fastest. Chips with a lower CL rating are faster than those with higher numbers.

Installing Memory Overview

Memory is an important part of computer performance. Installation involves planning, installing, and possibly removing some older modules. Lack of planning can lead to less-than-optimal performance. The following is the best process for determining which memory chips to install in each bank:

Step 1. Determine which chip capacities can be used for the system. Look in the documentation included with the motherboard or computer for this information.

Step 2. Determine how much memory is needed. Ask the users which operating system is installed and which applications they are using (or look yourself). Refer to documentation for each application to determine the amount of RAM recommended. Plan for growth.

Step 3. Determine the capacity of the chips that go in each bank by drawing a diagram of the system, planning the memory population on paper, and referring to the system or motherboard documentation.

Some memory modules might need to be removed in order to put higher-capacity ones into the bank. Look at what is already installed in the system, refer to the documentation, and remove any existing modules, as necessary, to upgrade the memory.

TECH TIP

Memory safety reminder

Before installing a memory module, power off the computer, disconnect the power cord from the back of the computer, and use proper antistatic procedures. Memory modules are especially susceptible to ESD.

Removing/Installing Memory

When removing a DIMM and using proper ESD-prevention techniques, push down on the retaining tabs that clasp over the DIMM. Be careful not to overextend the tabs when pushing on them. If a plastic tab breaks, the only solution is to replace the motherboard or hope the DIMM stays in place. A DIMM lifts slightly out of the socket. Always ensure that you are grounded to prevent ESD by using an antistatic wrist strap or maintaining contact between a bare part of your arm and metal within the computer (self-grounding). Lift the module out of the socket once it is released. Figure 6.12 shows how to remove a DIMM.

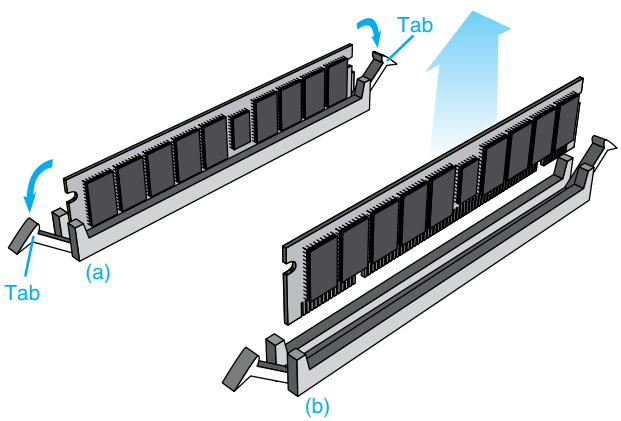


FIGURE 6.12 DIMM removal

A DIMM has one or more notches on the bottom, so that the module inserts into the memory socket only one way. Verify that the notches on the bottom of the module align with the notches in the motherboard memory slot. The DIMM will not insert into the memory socket unless it is oriented properly.

Make sure the side tabs are pulled out before you insert the DIMM and close the tabs over the DIMM once it is firmly inserted into the socket. If the DIMM does not go into the slot easily, do not force it and check the notch or notches for correct alignment. Once the DIMM is aligned correctly into the slot, push the DIMM firmly into the slot, and the tabs should naturally close over the DIMM or on the sides of the DIMM. Figure 6.13 illustrates how to insert a DIMM. Figure 6.14 shows a close-up of how the tab needs to fit securely in the memory module notch.

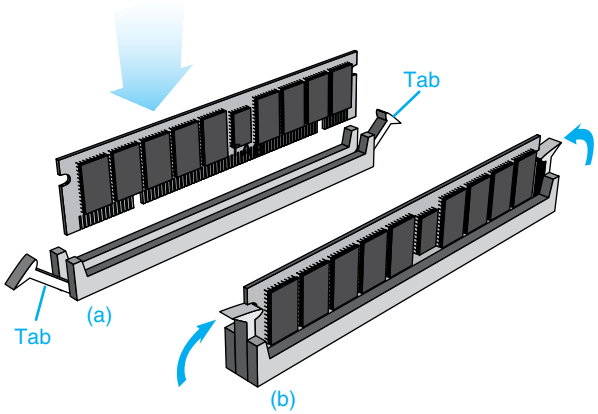


FIGURE 6.13 DIMM installation

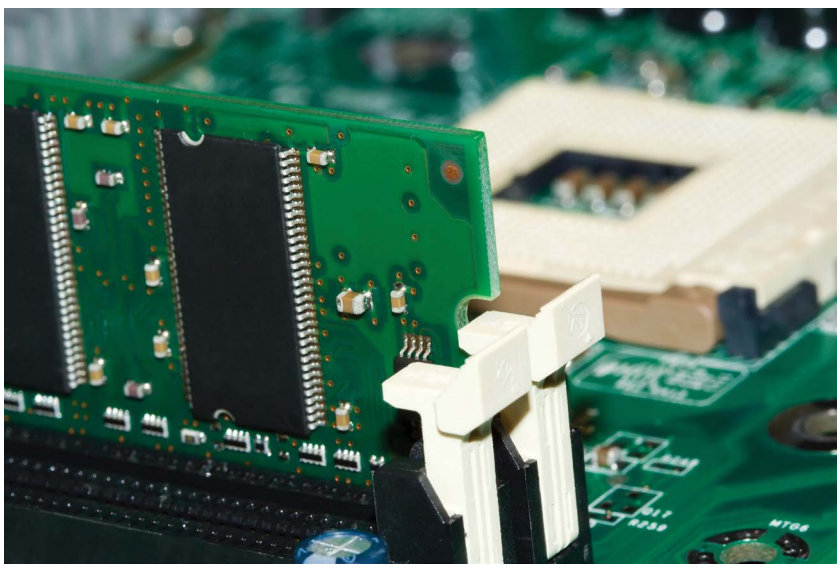


FIGURE 6.14 Secure DIMM tab

TECH TIP

POST error codes are normal after a memory installation/upgrade

Some computers show a POST error message or automatically go into the Setup program after memory is installed. This is normal. The important thing to notice during POST is that the memory shown in the BIOS/UEFI should equal the amount of memory installed.

Adding more RAM can make a noticeable difference in computer performance (up to a point, of course). When a computer user is sitting in front of a computer waiting for a document to appear or waiting to go to a different location within a document, it might be time to install more RAM. If you have several opened applications on the taskbar, click one of them. If you have to wait several seconds before it appears, it might be a good idea to upgrade the RAM.

Virtual RAM

Virtual RAM (virtual memory) involves using hard drive space as if it were RAM. Virtual memory allows the operating system to run larger applications and manage multiple applications that are loaded simultaneously. The amount of hard drive space used is dynamic—that is, it increases or decreases as needed. If the system begins to page frequently and is constantly swapping data from RAM to the hard drive, the cache size automatically shrinks. In Figure 6.15, notice how each application has its own memory space.

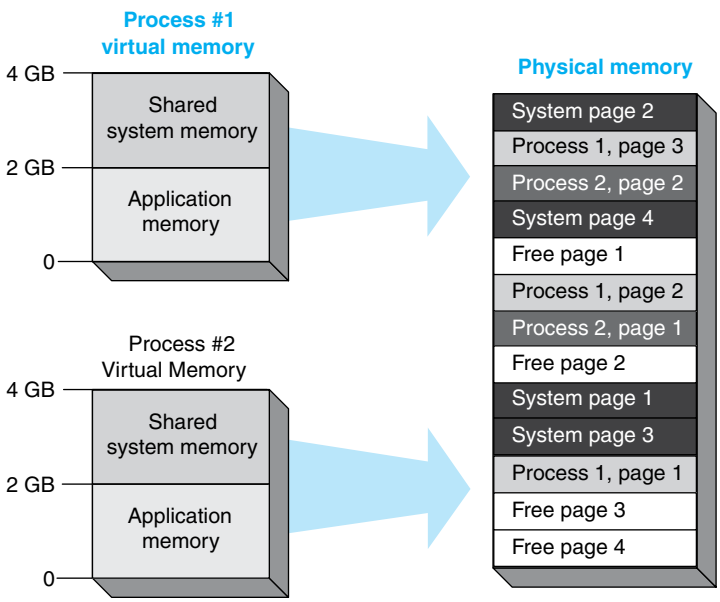


FIGURE 6.15 Windows virtual memory usage

A **paging file** is a block of hard drive space that applications use as if it were RAM. Other names for the paging file include pagefile, pagefile.sys, page file, and swap file. Look back at Figure 6.6, which shows the System Information screen, and you can see the data related to the paging file next to Total Virtual Memory, Available Virtual Memory, and Page File Space. For optimum performance in any Windows operating system, set aside as much free hard drive space as possible to allow ample room for virtual memory and caching. Keep the hard drive cleaned of temporary files and outdated files/applications.

TECH TIP

Hard drive paging file tips

If multiple hard drives are available, a technician might want to move the paging file to a different drive. Always put the paging file on the fastest hard drive unless that hard drive lacks space.

The amount of virtual memory is dynamically created by the operating system and does not normally need to be set manually. In Windows, search for the word `performance` > select the *Adjust the Appearance and Performance of Windows* link > *Advanced* tab > *Change* button. Change the parameters and click *OK* twice. Figure 6.16 shows how virtual memory relates to RAM and hard drive space.

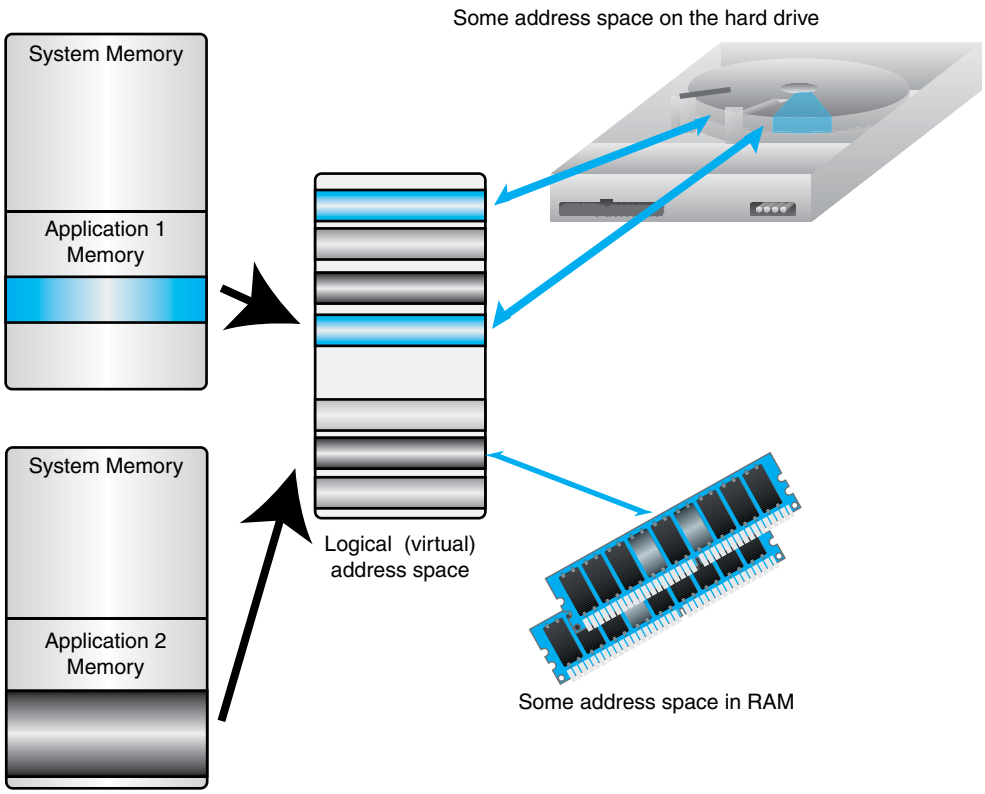


FIGURE 6.16 Virtual memory

Monitoring Memory Usage in Windows

Windows has a **Performance utility** in Task Manager for monitoring memory usage. Right-click on the taskbar > *Task Manager* > select the *Performance* option. The Performance utility has graphs that visually demonstrate the CPU and memory usage.

Figure 6.17 shows Task Manager, and Table 6.8 details some of the fields related to memory. In the Memory Composition section, there are several sections separated by vertical bars. You can place the pointer inside a space, and the name of the section appears. The sections, from left to right, are as follows:

- **In Use:** The shaded section that shows the amount of memory currently being used
- **Modified:** Another (smaller) section that show the amount of memory that holds data that must be written to the drive before the memory location can be used by something else
- **Standby:** The amount of memory that is cached and currently is not being used
- **Free:** The available memory

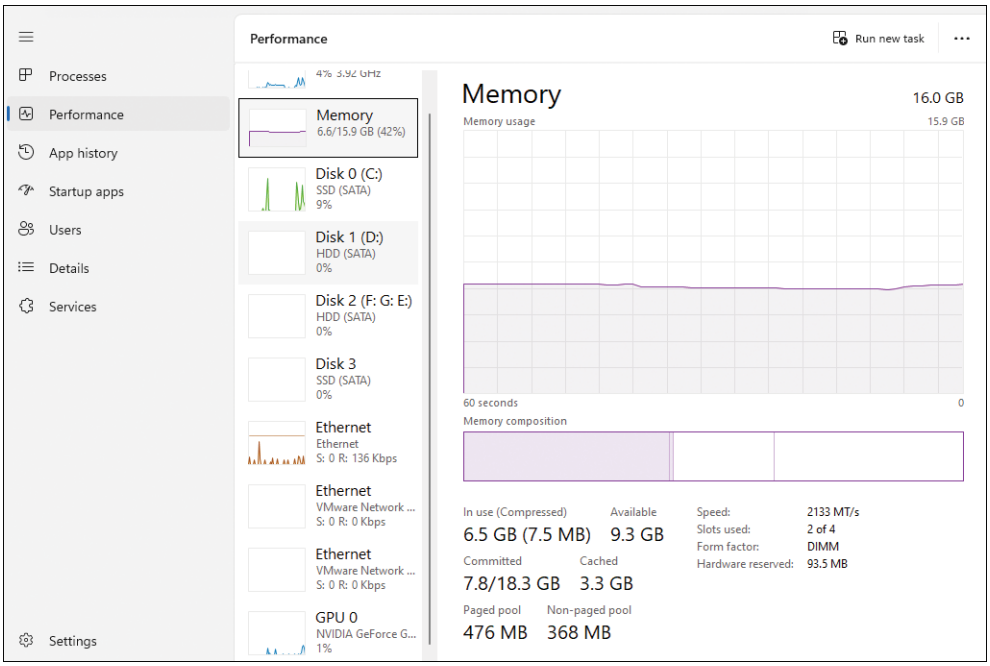


FIGURE 6.17 Windows Task Manager Performance tab Memory section

TABLE 6.8 Windows Task Manager Performance tab memory-related fields

Field	Description
In Use	The amount of memory currently being used by applications, the operating system, drivers, and processes.
Available	The amount of physical memory for application/operating system use.
Committed	Two numbers, with the first showing how much memory the operating system has identified that needs memory (and that might get removed or paged out of RAM if other, more important, processes need the space) and the second showing the amount of physical and virtual memory available.
Cached	The memory space that includes data that needs to be written to disk before being available, as well as cached data that is currently not being used.
Paged Pool	Memory set aside for operating system functions or device drivers that could be written to disk, if necessary.
Non-Paged Pool	Memory set aside for operating system functions or device drivers that must remain in physical memory (that is, cannot be paged out).
Speed	Speed of the RAM chips.
Slots Used	Number of memory slots used for memory modules and total number of slots.
Form Factor	Type of memory module, such as DIMM or SODIMM (used in laptops). Chapter 11, "Computer Design and Troubleshooting Review," covers mobile devices and SODIMMs.
Hardware Reserved	Memory reserved for device drivers or firmware that cannot be used by Windows for any other function.

Older Applications in Windows

Older applications are sometimes challenging in newer versions of Windows. Some older applications do not operate in newer Windows versions because they make direct calls to hardware, which Windows 7 and higher do not allow. These programs might also require that you change the color depth and resolution settings through the Display Control Panel.

For Windows 7 and higher, Microsoft states that some older software might not run properly and offers **Compatibility mode**. Right-click the application icon from the *Start* menu or right-click the program executable file and select *Properties*. Use the *Compatibility* tab to select the Windows version for which the application was written. If you do not know the version, you can select the *Run Compatibility Troubleshooter* button and then select the *Try Recommended Settings* link. Figure 6.18 shows the Compatibility tab.

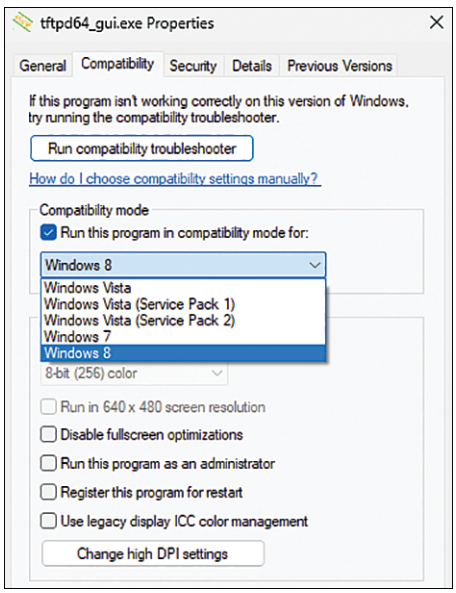


FIGURE 6.18 Windows Compatibility tab

You can also configure virtual machines by using virtualization software such as Microsoft's Virtual PC, Hyper-V, Oracle VM VirtualBox, or VMware Workstation to run older operating systems as well as run older applications. A **virtual machine** (VM) allows you to reduce hardware costs by running multiple operating systems simultaneously on a single computer (without one interfering with the other). Virtualization is covered in more detail in Chapter 12, "Internet Connectivity, Virtualization, and Cloud Technologies."

Troubleshooting Memory Problems

Memory problems can cause "out of memory" errors, **POST beeps**, motherboard diagnostic lights or codes, system lockups or **random shutdowns**, **sluggish performance**, a spinning **pinwheel** (indicating that an application is not responding), and **application crashes**. With any of these issues, no matter which operating system is being used, check the amount of available memory and free hard drive space. Sometimes you must close all applications, reboot the computer, and open only the application that was running when the out-of-memory error occurred because some applications do not release the memory space they hold. Use Task Manager or the Apps setting to halt the application.

The following tips and troubleshooting steps help with memory management:

- Add more RAM. To see the amount of physical memory (RAM) currently installed, access *File Explorer*, right-click (or tap and hold briefly) *This PC*, and select *Properties*.
- If you just installed new memory and an error appears, this is normal. Enter *Setup* because the system BIOS/UEFI knows something has changed.
- If you just installed new memory and the computer will not boot, check your installation by carefully pushing harder on the memory module (after shutting down and removing power, of course) to ensure that the module is fully seated into the slot. Check for loosened cables near the memory module(s). Ensure that you are installing the right memory type.
- Use the **Windows Memory Diagnostic Tool** to determine the issue. Use one of the following methods:
  - In Windows 10, search using the words `memory diagnostic`. Select the *Windows Memory Diagnostic* (Windows 10) link.
  - Boot into the *Advanced Boot Options* menu (by pressing F8 upon startup). Press Esc. Press Tab to move to the *Tools* section > *Windows Memory Diagnostic Tool*.
  - Use the original Windows operating system disc to boot the computer. Enter the language requirements and then click the *Repair Your Computer* link. From the *System Recovery Options* window, select *Windows Memory Diagnostic Tool*.
  - Use the command `mdsched`.
- Delete files/applications that are no longer needed and close applications that are not being used. Empty the Recycle Bin.
- Adjust the size of the virtual memory.
- Do not put the paging file on multiple partitions that reside on the same hard drive. Use multiple hard drives, if necessary.
- Put the paging file on a hard drive partition that does not contain the operating system.
- Put the paging file on the fastest hard drive.
- Remove the desktop wallpaper scheme or use a plain one.
- Adjust your Temporary Internet Files setting. For Microsoft Edge in Windows 10, search for Internet Explorer (not Microsoft Edge) and select the *Tools* > *Internet Options* > *Settings* button. Adjust how much drive space is set aside for caching web pages.
- Defragment the hard drive. See Chapter 7, "Storage Devices," for the steps.

TECH TIP

Upgrading memory is an easy solution

Upgrading memory is one of the easiest ways to solve performance issues. Keep in mind that sometimes you simply must buy more RAM, but you should try the previously mentioned tips before resorting to that.

If you receive a message that SPD device data is missing or inconclusive, your motherboard is looking for SPD data that it cannot receive from the memory module. If this is a new module, ensure that it supports SPD. If it is an older module, you need to replace one of your memory modules.

POST usually detects a problem with a memory chip, and most systems show an error code or message. The motherboard might also contain diagnostic lights or a code. In either case, turn off the computer, remove the cover, press down on any memory modules, and reboot. Another option is to clean the memory module slots with compressed air and reinstall the module. The key to good memory chip troubleshooting is to divide and conquer. Narrow the problem to a suspected memory module and then swap banks, if possible. Keep in mind that most memory problems are not with the hardware but in the software applications and operating system.

TECH TIP

When adding more memory doesn't help

Today's operating systems rely almost as much on hard drive space as they do on RAM because of multitasking. Lack of hard drive space is almost as bad as insufficient RAM. If the system still runs slowly after adding RAM, look at used hard drive space and delete files to free up space, upgrade drive storage, or add another drive.

Removable Storage

Removable storage is very important to users today, for PCs, laptops, mobile devices, cameras, and smartphones. Removable memory comes in many forms and capacities. Common removable storage includes flash drives and memory cards.

Flash memory is a type of nonvolatile solid-state memory that holds data even when the computer power is off. Network devices, smartphones, and tablets use flash memory to store the operating system and instructions. Some tablets can use external flash media for storage. Solid-state drives (SSDs) also use flash memory (see Chapter 7). Digital cameras use flash memory to store pictures, scanners use flash memory to store images, and printers use flash memory to store fonts. Unlike DRAM, flash memory does not have to be refreshed, and unlike SRAM, it does not need constant power. Figure 6.19 shows various flash memory devices.

USB **flash drives** (sometimes called thumb drives, memory bars, or memory sticks) allow storage up to 16 TB, and higher capacities are expected in the near future. In Figure 6.19, the two white devices and the blue device in the middle are USB flash drives, and the rest are storage for digital cameras and recorders. Flash drives connect to USB ports. After attaching a flash drive to a USB port, a drive letter is assigned by the operating system, and File Explorer can be used to manipulate the files on the drive.

FIGURE 6.19 Flash memory

TECH TIP

The number-one cause of flash drive failure is improper removal

When you are finished using a flash drive, double-click the *Remove Hardware* icon in the notification area. The icon has a white check mark on a green field. You might have to click the left arrow or up arrow to see this icon. Click *Safely Remove Hardware and Eject Media*. Select the appropriate flash drive. When you see a message that says you can safely remove the drive, remove the flash drive from the USB port.

If you cannot find the Safely Remove Hardware icon in Windows 10, right-click the taskbar and select *Taskbar settings*, and in the notification area, access the *Select which icons appear on the taskbar* link and ensure that the *Windows Explorer Safely Remove Hardware and Eject Media* option is set to *On*. In Windows 11, right-click the taskbar and select *Taskbar settings*, and in the *Other system tray icons* section, ensure the *Safely Remove Hardware and Eject Media* option is set to *On*. Note that not all flash drives show up in this area, and you might need to right-click a drive in File Explorer and select the *Eject* option.

Security features that are available on flash drives include password protection for drive and data encryption. Flash drives are a very good memory storage solution; they are inexpensive and easy to use. Figure 6.20 shows the interior of a flash drive. Chapter 11 goes into more detail about the types of flash memory used with such devices.

FIGURE 6.20 Inside a USB flash drive

Memory cards contain flash memory and are used in cell phones, digital recorders, cameras, and just about any type of mobile device you can find. Table 6.9 lists memory cards you might see or need to install.

TABLE 6.9 Memory cards

Storage type	Comments
CompactFlash (CF)	Introduced by SanDisk; uses flash memory; does not require a battery to store photos after power is removed; includes CF-I and CF-II
SmartMedia	Developed by Toshiba; smaller and lighter than CF; adapter cards with PC Card/ExpressBus ATA are available for data transfers
Memory Stick	Created by Sony; small in size; can read/write with a Memory Stick reader; includes Memory Stick (MS), Memory Stick Duo (MSD), Memory Stick Micro (M2)
Secure Digital	Size of a postage stamp; does not require power to retain data; uses flash memory technology; supports cryptographic security; different types include SD, miniSD, microSD, and SDHC
MMC (multimedia card)	A type of flash memory used in many portable devices, including cameras; works in many devices that support SD cards and is less expensive; types include MMC, eMMC, RS-MMC, MMCmicro, dual voltage (DV-MMC), MMCplus, MMCmobile, and MiCard

Related to removable storage is copying data that is on the card. You may be called on to install or use a memory card reader. A **memory card reader** or multi-card reader attaches externally or is integrated into a computer or laptop. A reader has multiple slots that allow different memory media to be read. These devices have many names, such as 15-in-1 reader, 8-in-1 reader, or 5-in-1 reader (depending on how many different slots or types of memory modules the device accepts). A memory card reader instantly recognizes inserted memory cards, whose contents can be copied to the computer and manipulated. The media card slots are assigned drive letters that are accessible through File Explorer. Figure 6.21 shows one of these readers.

TECH TIP

No drive letter

If the media does not appear in Windows/File Explorer, the reader may have been temporarily uninstalled. Use the Safely Remove Hardware and Eject Media tool in the notification area, unplug the cable from the port, and re-insert the cable to ensure that the operating system recognizes the reader. If the card reader or ports are still not available or if they are integrated into the computer, restart the computer.

FIGURE 6.21 Memory card reader

Memory is one of the most critical components of a computer, and it is important for a technician to be well versed in the different memory technologies. Because memory is one of the most common upgrades, becoming proficient and knowledgeable about populating memory is important.

SOFT SKILLS: TEAMWORK

Technicians tend not to like working in teams as much as they like working on their own. Much of a technician's job is done alone. However, a technician normally has one or more peers, a supervisor, and a network of partners involved with the job, such as suppliers, subcontractors, and part-time help. It is easy to have tunnel vision in a technical support job and lose sight of the mission of the business. Many technical jobs have the main purpose of generating revenue—solving people's computer and network problems for the purpose of making money. Other technicians have more of a back-office support role—planning, installing, configuring, maintaining, and troubleshooting technologies the business uses to make money.

Technicians must focus on solving customers' problems and ensuring that customers feel that their problems have been solved professionally and efficiently. However, you cannot lose sight of the business-first mentality; remember that you play a support role whether you generate revenue or not. You are a figure on someone's balance sheet, and you need to keep your skills and attitudes finely tuned to be valuable to the company. No matter how good you are at your job, you are always more valuable to a company if you are part of a team than if you're on your own. Make sure to **be on time**, **maintain a positive attitude**, and **project confidence**. Being a person who is late, takes off early, chats too much with customers, blames others, and so on is not being a good team member. If you are going to be late for work or leave early, inform your supervisor and coworkers so they can take care of any issues that arise while you're gone. If you are going to be late for a customer appointment, contact the customer and let them know you are running late.

Technicians need to be good team players and see themselves as a reflection of their company when on the job (see Figure 6.22). Employers see **teamwork** as an important part of a technician's skill set—just as important as technical skills. Think of ways that you can practice teamwork even as a student and refine those skills when you join the workforce.

FIGURE 6.22 Teamwork

Chapter Summary

- Memory on a motherboard is SDRAM, a type of RAM that is cheaper and slower than SRAM, the type of memory inside the CPU and processor housing.
- Each type of DDR module will only fit in that type of module's motherboard slot. For example, a DDR5 module requires a DDR5 slot.
- Unbuffered non-ECC memory is the RAM normally installed in computers.
- ECC is used for error checking and is commonly found in high-end computers and servers.
- The CL rating or the timing sequence's first number shows how quickly the processor can access data in sequential memory locations. The lower the first number, the faster the access.
- SPD is a technology used so the memory module can communicate specifications to the BIOS/UEFI.
- Dual-rank memory is one module that acts like two modules and is shown as 2R in advertisements. Single-rank memory is the norm, and a memory advertisement usually does not show this feature.
- Before installing memory, plan your strategy: Read the manual to determine the type of memory; determine the total amount of memory; determine whether any memory is to be removed; determine the memory to purchase; and be mindful of getting the most out of your memory by implementing dual-, triple-, or even quad-channeling.
- When implementing dual-, triple-, or quadruple-channeling, buy matching memory modules.
- Particular versions of Windows have memory limitations.
- RAM is very susceptible to ESD events. Use proper handling procedures, including using an antistatic wrist strap.
- Before removing or installing memory, disconnect the power cord and remove the battery on a mobile device.
- Having as much RAM in a system as possible is an important performance factor, and so is having free hard drive space because hard drive space is used as memory. This is called virtual memory, and the information stored temporarily on a hard drive is stored in an area known as a paging file, page file, or swap file. The paging file should be on the fastest drive that has the most free storage.
- Use Task Manager to monitor memory performance.
- Use POST, motherboard LED/display output codes, BIOS/UEFI diagnostics, and the Windows Memory Diagnostic Tool to diagnose memory problems.
- Flash media is used to provide memory or additional storage space for computing devices and includes USB flash drives.
- A technician is part of a business and should contribute to the team. A technician should professionally represent a company.

A+ CERTIFICATION EXAM TIPS

- ✓ Be able to install the correct RAM. Know the difference (in terms of numbers of pins, speeds, etc.) between the DDR iterations (DDR3, DDR4, and DDR5, for example) for both DIMMs and SODIMMs and know that a DDR3 socket, for example, will not accept a DDR4 or DDR5 module.
- ✓ Know how to calculate what memory is needed for an upgrade or a new install.
- ✓ Be able to identify memory slots on a motherboard.
- ✓ Know how to populate memory when single-, dual-, triple-, or quad-channeling is being implemented.
- ✓ When populating memory, consult the motherboard documentation before you go any further.
- ✓ Be able to describe the difference between non-ECC and ECC memory.
- ✓ Know that memory chips are especially susceptible to ESD and how to prevent ESD damage when installing or removing memory. Review Chapter 5, "Disassembly and Power," for tips on dealing with ESD.
- ✓ Remember that if any application is slow to respond, the computer may need more RAM. POST error codes, application crashes, and random shutdowns can indicate a memory problem.
- ✓ Review the troubleshooting symptoms and tips at the end of the chapter.
- ✓ Know when and how to use Compatibility mode and the Windows Memory Diagnostic Tool.
- ✓ Keep in mind that the following professionalism skills are part of the 220-1202 exam: (1) Maintain a positive attitude, (2) project confidence, (3) be on time, and (4) if you will be late, contact the customer.

Key Terms

application crash, be on time, buffered memory, cache memory, CL rating, Compatibility mode, DDR iterations, DDR3, DDR4, DDR5, DIMM, DRAM, dual rank, dual-channel, ECC RAM, flash drive, flash memory, maintain a positive attitude, memory card, memory card reader, non-ECC RAM, non-parity, paging file, Performance utility, pinwheel, POST beep, project confidence, quad-channel, RAM, random shutdown, single rank, sluggish performance, SODIMM, SPD, SRAM, teamwork, triple-channel, unbuffered memory, virtual machine, virtual RAM, Windows Memory Diagnostic Tool

Review Questions

The following specifications for motherboard RAM are used for Questions 1–5:

- Four DDR4 SDRAM DIMM sockets arranged in two channels and supporting up to 128 GB (32 GB single DIMM capacity) of system memory
- Support for DDR4 3200/2933/2667/2400/2133 MHz memory modules DIMMs
- Support for ECC unbuffered DIMM 1Rx8/2Rx8 memory modules
- Support for non-ECC unbuffered DIMM 1Rx8/2Rx8/1Rx16 memory modules
- Support for extreme memory profile (XMP) memory modules
- Support for up to 16 GB of system memory

1. Of the given features, which would be applicable to this computer? (Choose all that apply.)

   [unbuffered | registered | 204-pin SO-DIMM | 288-pin DDR5 DIMM | 288-pin DDR4 DIMM | ECC | non-ECC | single rank | dual rank]

2. Pretend that this computer has 4 GB of memory installed. Write all combinations of memory population when inserting RAM into the slots.

   _____

3. [T | F] The technician who is recommending memory for this motherboard could recommend memory that does not perform error checking.

4. What does the statement "four DDR4 SDRAM DIMM sockets arranged in two channels" mean?

   _____

   _____

5. Would there be an issue if this motherboard contained 6 GB of RAM and the computer had 32-bit Windows 10 installed? If so, explain the issue.

   _____

   _____

Consider the following memory advertisements for desktop memory used in Questions 6–11:

a. 2 GB 240-pin SDRAM DDR3L 1600 (PC3L 12800) Desktop Memory

b. 4 GB DDR3-1600 (PC3-12800) CL11 240-pin DIMM

c. 4 GB ECC registered DDR3 SDRAM CAS latency 9

d. 4 GB 240-pin DDR3 SDRAM 1333 (PC3 10600) CAS 9

e. 8 GB (1x8 GB) 1333MHz PC3-10600 CL9 ECC registered dual-rank low power

f. 8 GB (2x4 GB) DDR4 SDRAM 2133 (PC4 17000)

g. 16 GB PC4L-2666

h. 16 GB kit (2x8 GB) DDR4 2666 MHz PC4-21300 CL19 unbuffered non-ECC 1.2V UDIMM

i. 16 GB 1Rx16 DDR4 UDIMM 3200MHz

6. In these advertisements, which DDR4 option(s) would hold the most data in a single memory module and be best suited for a desktop computer?

   _____

   _____

   _____

7. In option g, what does the L in DDR4L mean?

   _____

   _____

8. A customer wants to dual-channel 8 GB of RAM on a desktop computer. Which memory module(s) would be best to buy, given the following documentation from the motherboard manual? (Memory module slots are in order from closest to the CPU: 1, 3, 2, and 4.)
   - Do not install ECC memory modules.
   - The memory configurations are as follows:
     - A pair of matched modules in DIMM connectors 1 and 2
     - A pair of matched modules in DIMM connectors 1 and 2 and another pair in connectors 3 and 4
   - If you install mixed pairs, the memory modules function at the speed of the slowest memory module installed.

_____

_____

9. Considering the answer given to Question 8, which motherboard DIMM connectors would be used?

_____

10. What type of memory feature will be needed if data accuracy is paramount for a new computer?

    [buffered | ECC | registered | XMP]

11. When comparing options b and d and imagining that both modules cost the same, which one would be the better purchase? Explain your reasoning.

_____

_____

12. What method is most effective for preventing an ESD event when installing RAM?
    - **a.** Placing the computer on an antistatic mat
    - **b.** Wearing an antistatic wrist strap
    - **c.** Staying in contact with an unpainted metal part of the computer
    - **d.** Wearing rubber-soled shoes and using the buddy system by having another technician standing by
13. Which of the following would be the first sign that a computer needs more RAM?
    - **a.** The computer is slow to respond.
    - **b.** The computer makes a ticking noise.
    - **c.** A POST error message appears.
    - **d.** A recommendation to use the *Windows Memory Diagnostic Tool* appears.
14. How can you tell the maximum amount of memory a motherboard can support?
    - **a.** Look at the memory options in BIOS/UEFI.
    - **b.** Use the Windows Task Manager > *Performance* tab.
    - **c.** Use the Windows Memory tool.
    - **d.** Look at the motherboard documentation.
15. What is one easy way to tell how much RAM is installed in a computer?

_____

_____

16. [T | F] A DDR4 DIMM can fit in a DDR3 memory expansion slot.
17. You have just added two new memory modules to a computer, but now the system will not boot and is beeping multiple times. What will you check first?

_____

_____

_____

18. Give an example of how a technician might project confidence while working on a help desk.

_____

_____

_____

19. A system already has two 3200 MHz memory modules installed, and a technician adds two more modules that operate at 4800 MHz. What will be the result of this action?

    a. The computer won't boot.

    b. The computer might freeze at times.

    c. The memory will operate at the 4800 MHz speed.

    d. All memory will operate at the 3200 MHz speed.

20. A technician has received a complaint that a computer is not performing as well as it used to. Which Windows tool would the technician ask the user to open to quickly tell how much RAM is currently being used by the open applications?

    [Performance Monitor | Device Manager | System Information tool | Task Manager]

Exercises

Exercise 6.1 Configuring Memory on Paper

Objective: To be able to determine the correct amount and type of memory to install on a motherboard

Parts: Internet access or access to magazines or ads that show memory prices

Procedure: Refer to Table 6.10 to answer the questions. This motherboard supports 1600/1333/1066 MHz DDR3 memory modules. The capacities supported are 1, 2, 4, and 8 GB, for a total of 16 GB maximum. Memory channel speed is determined by the slowest DIMM populated in the system.

TABLE 6.10 Motherboard single-/dual-channel combinations

		Sockets	
Mode	**Scenario**	**DIMM1**	**DIMM2**
Single-channel	1	Populated	
	2		Populated
Dual-channel	1	Populated	Populated

1. What memory modules are needed if the customer wants 5 GB of RAM? What capacities and how many modules of each capacity are required?

   _____

2. How many memory slots does this motherboard have? [1 | 2 | 3 | 4]

3. Using the internet, a computer parts magazine, or a list of memory modules, determine the exact part numbers and quantities of memory modules you would buy to populate this motherboard with 5 GB of RAM. List them as well as the location where you obtained the information.

   _____

   _____

4. This motherboard already has 4 GB of RAM installed in the DIMM1 slot. The customer would like to upgrade to 8 GB total memory, use the existing module if possible, and use dual-channeling. What capacity and number of memory modules are needed to get up to the 8 GB total? List any concerns to consider.

_____

_____

_____

5. What memory slot will be used to install the memory module, based on the documentation provided?

_____

_____

6. What does the documentation mean when referencing DDR3 1600/1333/1066 MHz RAM?

_____

_____

7. How do you know which one of the 1600, 1333, or 1066 modules to use?

_____

_____

_____

_____

_____

8. Using the internet, a computer parts magazine, or a provided list of memory modules, determine the exact part numbers and quantities of memory modules that you would buy to get this computer from 4 GB to 8 GB. List the module information along with the location where you obtained the information.

_____

_____

Exercise 6.2 Configuring Memory on Paper

Objective: To be able to determine the correct amount and type of memory to install on a motherboard

Parts: Internet access or access to magazines or ads that show memory prices

Procedure: Refer to Figure 6.23 and Table 6.11 to answer the questions. This motherboard supports the following memory configurations:

> Up to 64 GB memory

> DDR4 26666/2400/2133 MHz memory modules

> ECC unbuffered DIMM 1Rx8/2Rx8 memory modules (which operate in non-ECC mode)

> Non-ECC unbuffered DIMM 1Rx8/2Rx8/1Rx16 memory modules

The desktop board supports either single- or dual-channel memory configurations. The board has four DDR4 SDRAM DIMM connectors with gold-plated contacts.

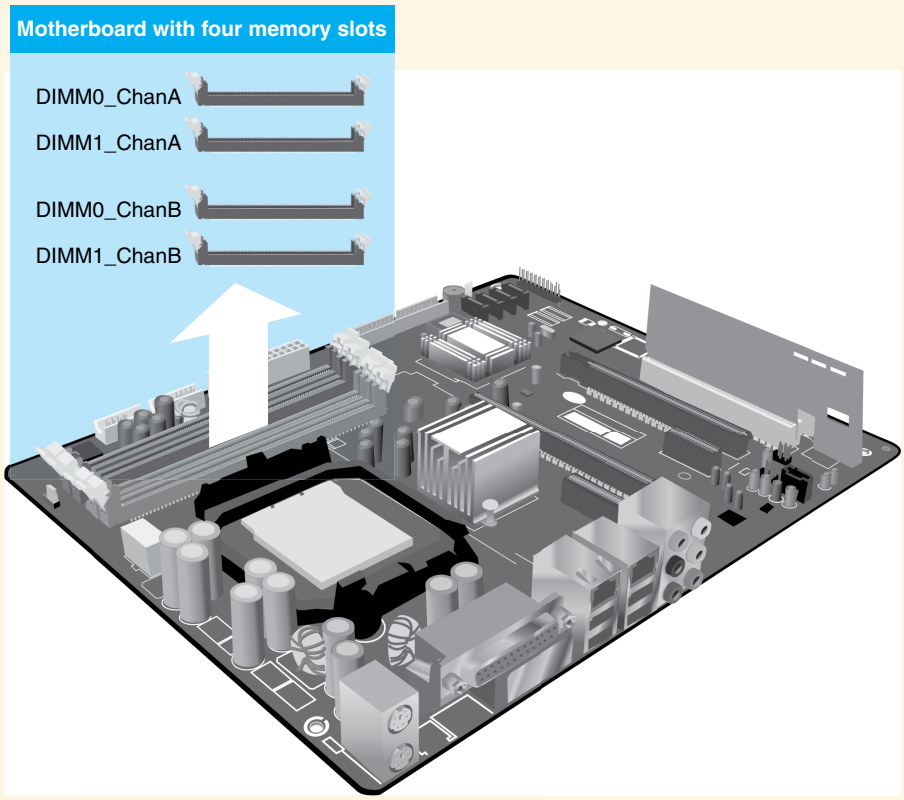


FIGURE 6.23 Motherboard with four memory slots and two channels

TABLE 6.11 Motherboard single-/dual-channel guidelines

Installed memory	Guidelines
2 DIMMs dual-channel	Install a matched pair of DIMMs equal in speed and size in DIMM0 of both Channel A and Channel B.
4 DIMMs dual-channel	Follow the directions for two DIMMs and add another matched pair of DIMMs in DIMM1 of both Channels A and B.
3 DIMMs dual-channel	Install a matched pair of DIMMs equal in speed and size in DIMM0 and DIMM1 of Channel A. Install a DIMM equal in speed and total size of the DIMMs installed in Channel A in either DIMM0 or DIMM1 of Channel B.
Single-channel	All other memory configurations result in single-channel memory operation.

1. In the documentation, what does 1Rx8/2Rx8/1Rx16 mean?

_____

_____

_____

2. What memory features, if any, can be used? (Choose all that apply.)

   [non-ECC | non-parity | ECC | registered | fully buffered | unbuffered | SPD]

3. What memory modules are needed if the customer wants 32 GB of dual-channel RAM? (What capacities and how many of each capacity are required?)

_____

4. What memory slots will be used to install the 32 GB of dual-channeled memory, based on the information provided?

_____

_____

5. Using the internet, a computer parts magazine, or a list of memory modules, determine the exact part numbers and quantities of memory modules you would buy to populate this motherboard with 32 GB of RAM. List them, along with the location where you obtained the information.

_____

_____

6. What does unbuffered mean?

_____

7. Can DDR3 memory modules be used with this motherboard? How can you tell?

_____

_____

8. If this motherboard already has 8 GB of RAM installed in the DIMM0_ChanA slot and the customer would like to upgrade to 16 GB of dual-channel RAM, what memory modules are needed? (What capacities and how many of each capacity are required?)

_____

9. What concerns would you have regarding dual-channeling before researching prices?

_____

_____

10. What memory slots will be used to install the 16 GB of total memory, based on the information provided and the upgrade scenario presented in Question 8?

_____

11. Using the internet, a computer parts magazine, or a list of memory modules, determine the exact part numbers and quantities of memory modules that you would buy to get to the total of 16 GB (from 8 GB) and do dual-channeling. List them, along with the location where you obtained the information.

_____

_____

Exercise 6.3 Configuring Memory on Paper

Objective: To be able to determine the correct amount and type of memory to install on a motherboard

Parts: Internet access or access to magazines or ads that show memory prices

Procedure: Refer to Figure 6.24 to answer the questions. The motherboard supports the following memory configurations:

- 1 GB, 2 GB, 4 GB unbuffered and non-ECC DDR3 DIMMs can be used in the DIMM slots (1, 2, 3, and 4) for a total of 32 GB max using DDR3 1066/1333 MHz modules.
- Recommended memory configurations are modules in DIMMs 1 and 3 or modules in DIMMs 1, 2, 3, and 4.
- Single- and dual-channel modes are supported.
- You may install different sizes in Channel A and B. The dual-channel configuration will be the total size of the lowest-sized channel. Any excess memory will operate in single-channel mode.
- >1.65 V DIMMs are recommended.
- Use the same CAS latency and obtain from the same vendor, if possible.
- The default memory operation frequency is dependent on SPD.

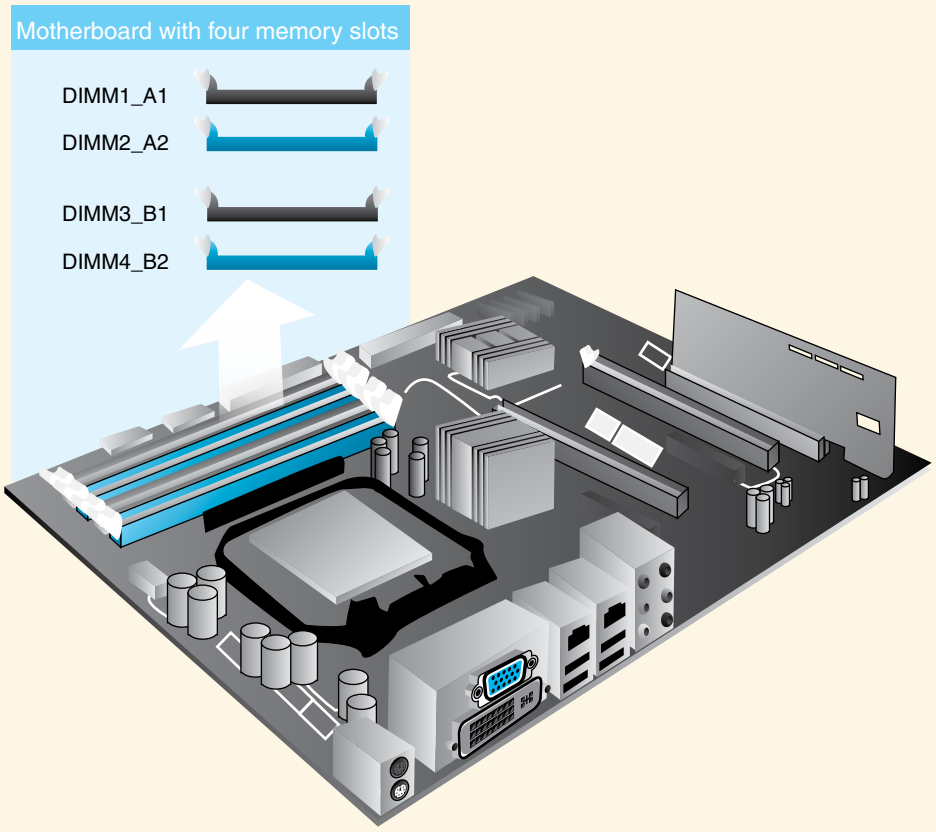


FIGURE 6.24 Second motherboard with four memory slots and two channels

1. What memory features, if any, are used? (Choose all that apply.)

   [parity | non-parity | ECC | registered | unbuffered | SPD]

2. The customer wants 4 GB of RAM. What memory modules are needed? (What capacities and how many of each capacity are required?)

   _____

3. What memory slots will be used to install the memory suggested in Question 2?

   _____

   _____

4. Using the internet, a computer parts magazine, or a list of memory modules provided by the instructor, determine the exact part numbers and quantities of memory modules that you would buy. List them, along with the location where you obtained this information.

   _____

5. In what type of systems would ECC modules most likely be required and used?

   [student desktop | smartphones | tablets | servers | laptops]

6. What is the purpose of ECC modules?

   _____

7. What is the purpose of SPD?

   _____

Exercise 6.4 Configuring Memory on Paper

Objective: To be able to determine the correct amount and type of memory to install on a motherboard

Parts: Internet access or access to magazines or ads that show memory prices

Procedure: Refer to Figure 6.25 to answer the questions. The motherboard supports the following memory configurations:

- Max memory supported: 16 GB
- Memory types: DDR4-4600/4400/4266/4200
- Memory channels: 3
- Number of DIMMs: 4
- ECC supported: Yes
- Connectors use gold-plated contacts
- Unbuffered, non-registered single- or double-sided SPD DIMMs with a voltage rating of 1.65V or less
- Optimal performance can be achieved by installing three matching DIMMs in the ChanA, ChanB, and ChanC memory slots.
- Dual-channel operation can be achieved by installing matching DIMMs in ChanB and ChanC or all four memory slots.

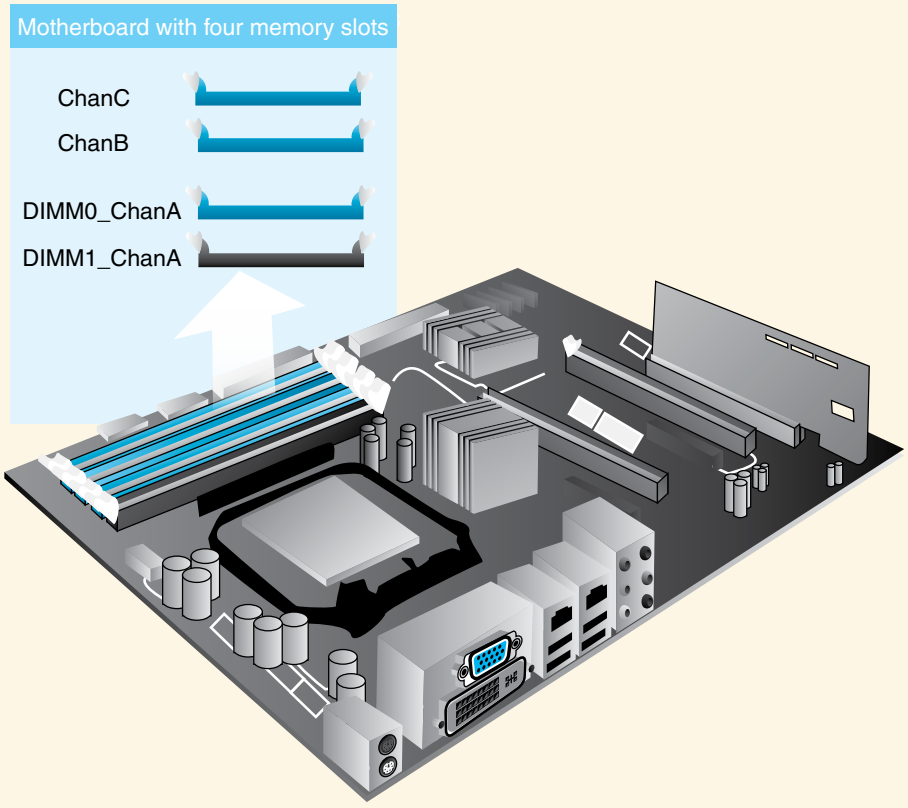


FIGURE 6.25 Triple-channel motherboard

1. What memory features, if any, are used? (Choose all that apply.)

   [parity | non-parity | ECC | registered | unbuffered | SPD]

2. The customer wants 8 GB of RAM performing triple-channeling. Can this be done? Why or why not?

   [Yes | No]

   _____

   _____

3. What memory modules are needed to put 8 GB of memory on the motherboard? (What capacities and how many of each capacity are required?) Justify your choice.

_____

_____

_____

_____

4. What memory slots will be used to install the memory suggested in Question 3?

_____

_____

5. Using the internet, a computer parts magazine, or a list of memory modules provided by the instructor, determine the exact part numbers and quantities of memory modules that you would buy. List them, along with the location where you obtained this information.

_____

6. The user has 32-bit Windows 10 installed on this computer. Will there be any issues with the 8 GB of RAM? If so what might those issues be?

_____

_____

7. List one method a technician could use to ensure that the 8 GB are recognized by the system.

_____

_____

Activities

Internet Discovery

Objective: To become familiar with researching memory chips using the internet

Parts: A computer with internet access

Procedure: Use the internet to complete the following procedure:

> Power on the computer and start an internet browser.

> Using any search engine, locate two vendors that sell memory chips.

> Create a table like the one below and fill in your findings for each of the memory sites.

	Site 1	Site 2
URL		
Type of DIMM		
Largest-capacity DIMM		
Pros of website		
Cons of website		

Soft Skills

Objective: To enhance and fine-tune a future technician's ability to listen, communicate in both written and oral forms, and support people who use computers in a professional manner

Activities:

1. On your own, use the internet to find a utility that tests soft skills or your personality. Compare your scores with those of others in the class. Make a list of how you might improve in specific weak areas. Present your findings to a group and share your group findings with another group.
2. Note that this activity requires two computers. In groups of two, have one person describe in great detail to the other person how to upgrade the computer's memory by removing memory from one computer and adding it to the other. The person doing the physical installation can do nothing except what the partner says to do. Reverse roles and carry out the same process for removing the memory and reinstalling it in the original computer. At the end of the exercise, the two participants describe to the teacher what they experienced.
3. In small groups, find a video that describes how to do something on a computer. Critique the video in terms of how the speaker might do a better job communicating to people who are not technicians. Share the video with the class, along with your recommendations for doing it better. As an option, script a short presentation for how to do something. Tape/record it if possible and have the class critique each group's presentation.

Critical Thinking Skills

Objective: To analyze and evaluate information as well as apply learned information to new or different situations

Activities:

1. Using the documentation of any computer, compare and contrast two dual-channeling scenarios/solutions for a pretend customer. List three recommendations you would have for the customer. Write a list of your findings and share them with the class.

   _____

2. List the repercussions of discovering that a motherboard supports both single-rank and dual-rank memory modules. How does a single-rank memory module compare with a dual-rank memory module?

   _____

   _____

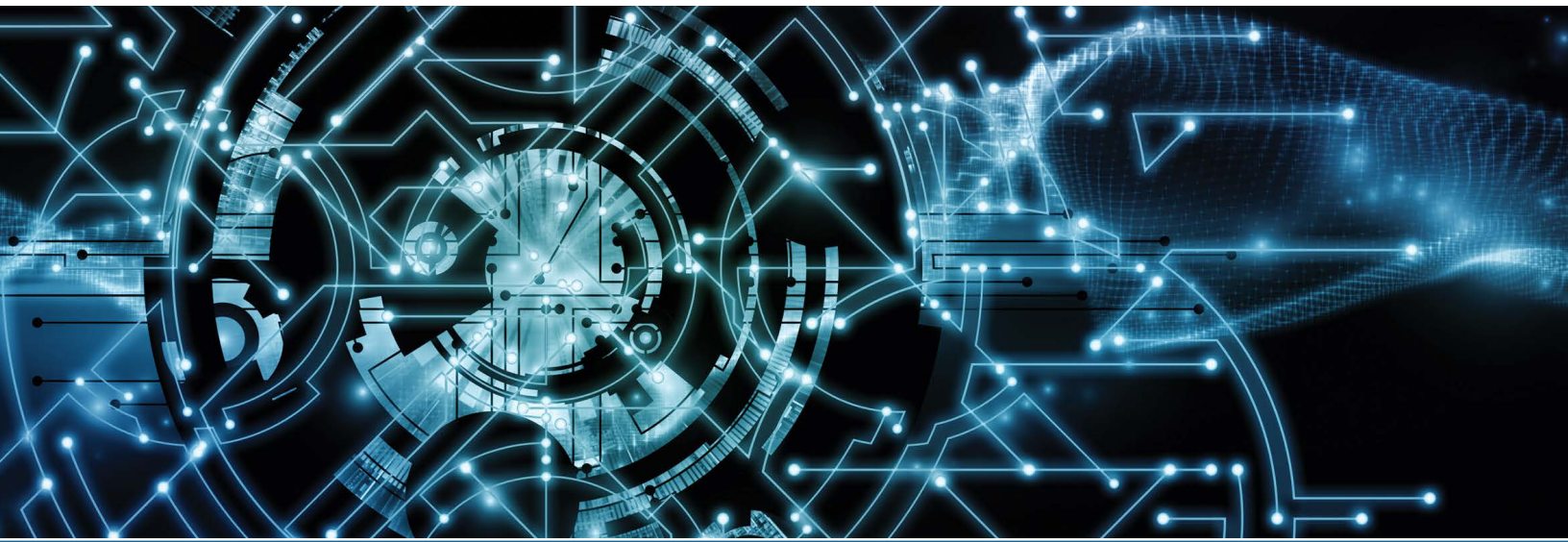
   _____

   _____

   _____

3. Download a motherboard manual from the internet or use one provided in the classroom. Find the memory section and make a list of any terms or directions that are given that you do not understand. In groups of four or five, share your lists and come up with as many solutions as possible. Share your group list with the class. Write any unsolved questions on the board and bring back the answers to those questions in a week.

7 Storage Devices



In this chapter you will learn:

- Basic storage terms
- About SATA, eSATA, SSD, and SSHD technologies
- How to install and configure storage devices, including RAID
- How to fix storage device problems
- How to keep a drive healthy
- How to create and troubleshoot RAID issues
- How to create and use Windows Storage Spaces
- Effective phone communication

CompTIA Exam Objectives:

- ✓ 1201-3.2 Summarize basic cable types and their connectors, features, and purposes.
- ✓ 1201-3.4 Compare and contrast storage devices.
- ✓ 1201-5.2 Given a scenario, troubleshoot drive and RAID issues.
- ✓ 1202-1.1 Explain common operating system (OS) types and their purposes.
- ✓ 1202-1.2 Given a scenario, perform OS installations and upgrades in a diverse environment.
- ✓ 1202-1.4 Given a scenario, use Microsoft Windows operating system features and tools.
- ✓ 1202-1.5 Given a scenario, use the appropriate Microsoft command-line tools.
- ✓ 1202-2.9 Compare and contrast common data destruction and disposal methods.
- ✓ 1202-3.1 Given a scenario, troubleshoot common Windows OS issues.
- ✓ 1202-4.7 Given a scenario, use proper communication techniques and professionalism.

Storage Devices Overview

Storage devices hold the data we are so fond of generating and keeping—photos, PDFs, movies, word processing documents, spreadsheets, and whatever else we can think to save. Data can be stored on optical media, flash media, or magnetic media such as hard drives, as shown in Figure 7.1.

FIGURE 7.1 Storage devices

Many folks, especially those who travel frequently, use data storage servers at their company. Data can also be stored "in the cloud." This means that there are storage devices available on remote servers to store data. Some storage is provided by an internet provider or as a service for a mobile device. Companies such as Amazon, Microsoft, Google, SugarSync, and Dropbox provide cloud storage. Some companies charge for cloud storage, and others offer limited amounts of cloud storage for free and have an option to pay for more. The services of such a site include backing up the data stored on their drives and having redundant hard drives in their servers. This is known as *cloud storage* or *offsite storage*. Microsoft, Google, Apple, Amazon, and other companies have made it very easy to store (or automatically store) data in the cloud, synchronize data to the cloud, back up your storage device data, and recover data. More information on how to do this is provided in Chapter 12, "Internet Connectivity, Virtualization, and Cloud Technologies," and Chapter 17, "macOS and Linux Operating Systems." Figure 7.2 illustrates this concept, but keep in mind that "in the cloud" is just a ton of hard drives, servers, and other devices in remote locations.

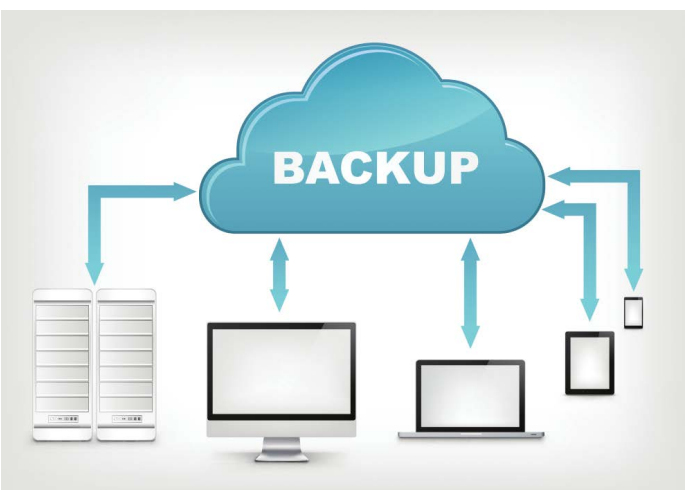


FIGURE 7.2 Cloud storage

Hard Drive Overview

A hard drive can be mounted inside a computer case or attached externally to a USB, eSATA, or eSATAp port. Hard drive capacities extend into the terabytes. Hard drives are frequently upgraded in computers, so it is important for you to understand all the technical issues and be able to recognize the parts of the hard drive subsystem, how the operating system and the BIOS/UEFI work together with a hard drive, and how to configure and troubleshoot a hard drive.

Hard drives come in different physical sizes (form factors). For desktop and small server models, 5.25-inch (not very popular) and **3.5-inch drives** are available. The **2.5-inch drive** form factor is designed for laptops, but can also be found in some PCs. A 1.8-inch form factor is available for solid-state drives (SSDs), tablets, and portable devices. Figure 7.3 shows two hard drive sizes.

FIGURE 7.3 Desktop hard drive form factors

A hard drive can also be placed inside an external enclosure and attached using a USB, eSATA, or eSATAp combo port. Figure 7.4 shows a Sabrent hard drive enclosure into which you could insert an internal drive and attach the drive to an external computer port.

FIGURE 7.4 Sabrent external hard drive enclosure

Magnetic Hard Drive Geometry

Traditional mechanical hard drives are magnetic hard drives. These hard drives have multiple hard metal surfaces called *platters*. Each platter typically holds data on both sides and has two read/write heads: one for the top and one for the bottom. The read/write heads float on a cushion of

air without touching the platter surface. Data is written by using electromagnetism. A charge is applied to the read/write head, creating a magnetic field. The metal hard drive platter has magnetic particles that are affected by the read/write head's magnetic field, allowing 1s and 0s to be placed, or *induced*, onto the drive. Figure 7.5 shows the major components inside a mechanical hard drive.

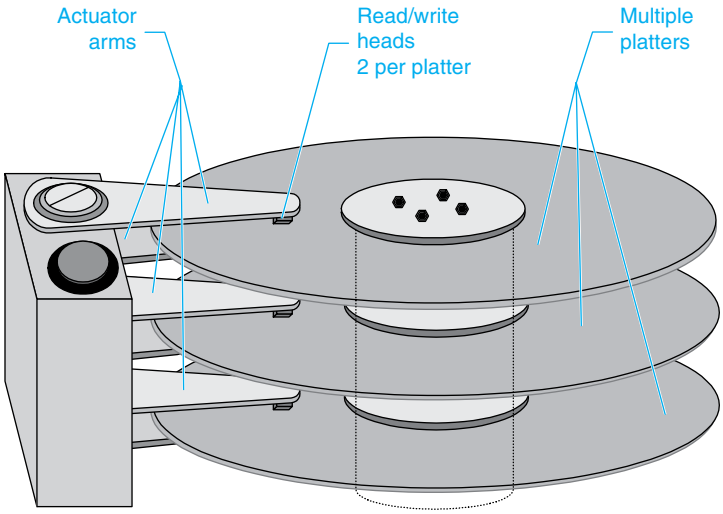


FIGURE 7.5 Hard drive geometry

If a read/write head touches the platter, a **head crash** occurs. This is sometimes called HDI (head-to-disk interference), and it can damage the platters or the read/write head, causing data corruption. Another important concept is mean time between failures (**MTBF**)—the average number of hours before a drive is likely to fail. Mechanical hard drives do fail, and that is why it is so important to back up the data stored on them. Figure 7.6 shows the inside of a hard drive. You can see the top read/write head and the platters. Keep in mind that you should not remove the cover from a hard drive because by doing so, you could allow particles into the sealed drive area.

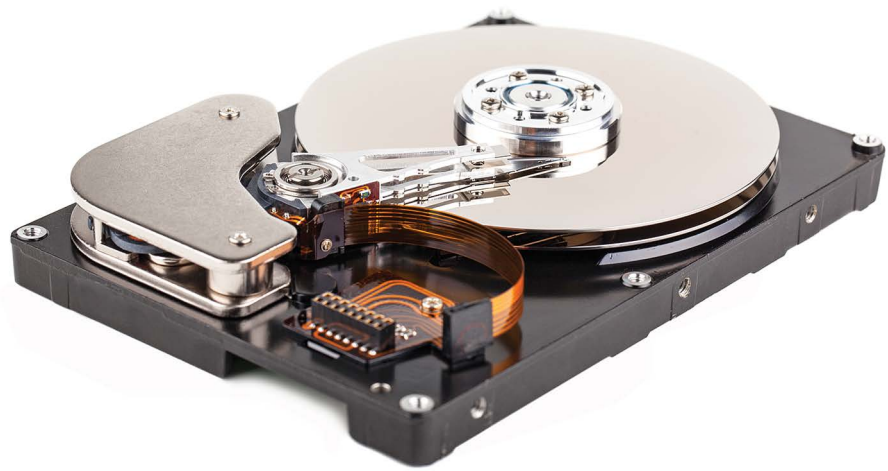


FIGURE 7.6 Hard drive with cover removed

Magnetic hard drives typically have two motors: one to turn the platters and one to move the read/write heads. A hard drive spins at different rotational rates called revolutions per minute (RPMs). Common speeds are **5,400 RPM**, **7,200 RPM**, **10,000 RPM**, and **15,000 RPM**. The faster the drive RPM, the faster the transfer rate and generally the higher the cost.

Solid-State Drive (SSD) Overview

SSDs are storage devices that use nonvolatile flash memory technologies instead of traditional mechanical hard drive technologies. SSDs eliminate the number-one cause of hard drive failure: moving parts. SSDs produce little heat and are reliable, quiet, secure, long-lasting, and fast. SSDs are installed in laptops and desktop models as internal and external units. SSDs are commonly used in tablets and some mobile devices. They are also used in environments such as temperature extremes or where a drive might be jolted. SSDs can be used in conjunction with mechanical hard drive storage.

TECH TIP

Don't use an SSD for archival storage

SSDs slowly lose their charge if left for a long time without power.

The main drawback to SSDs is cost. SSDs are expensive compared to mechanical hard drives. As with flash drives, each memory block of an SSD has a finite number of reads and writes. An SSD that writes data across the entire memory capacity will last longer. Some companies include software with an SSD that helps with installation, configuration, performance, and monitoring and that tracks or estimates end of life. Figure 7.7 shows the inside of an SSD.

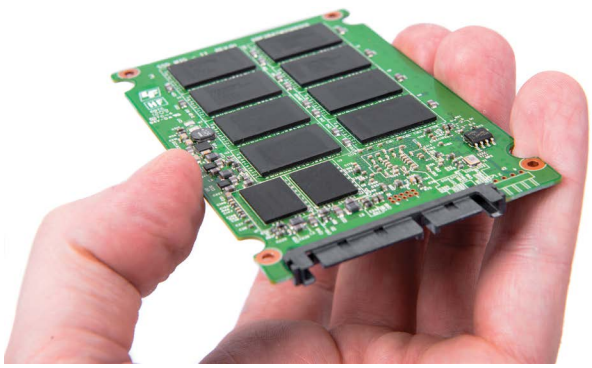


FIGURE 7.7 Solid-state drive without a cover

Today, hybrid SSDs are available. A hybrid SSD, or solid-state hybrid drive (**SSHD**), uses a combination of mechanical and flash technologies. An SSHD has some flash memory integrated with a traditional mechanical drive (see Figure 7.8).

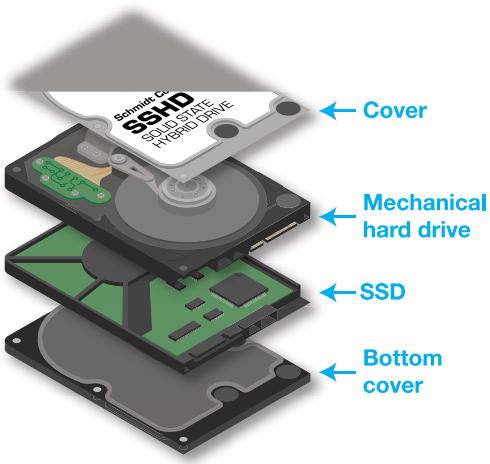


FIGURE 7.8 SSHD

The flash memory in an SSHD typically contains the most frequently used data that would be sent to the host interface. Advanced algorithms are used to predict this data. Only if requested data were not in flash memory would data be pulled from the slower mechanical drive. SSHDs provide the best of both worlds: Costs are lower per byte because you have a little bit of really fast memory storage, thanks to the SSD, and there is a lot of storage space, thanks to the traditional mechanical drive. In addition, you do not require a faster RPM traditional drive with an SSHD.

M.2 and NVMe

An **M.2** slot allows SSDs and Wi-Fi/Bluetooth modules of varying sizes to be connected. An M.2 slot can interface with SATA 3.0 and higher, PCIe 3.0 and higher, and USB 3.0 and higher. Note that currently a single M.2 slot can use a maximum of four PCIe lanes, and it may use fewer. Refer to the motherboard documentation for the exact specifications.

Common card sizes include 2242, 2260, 2280, and 22110. In these sizes, 22 refers to the width, in millimeters, and the next two or three numbers refer to the length. The device or motherboard documentation indicates which sizes are accepted.

M.2 devices are also keyed, which means there are separations between the gold connectors. The three most common keys used are B, M, and B+M. A module using the B key uses up to two PCIe lanes, and the M key uses up to four PCIe lanes. Figure 7.9 shows four sizes of M.2 cards; one of the cards has an M key, and the other cards have the B+M key.

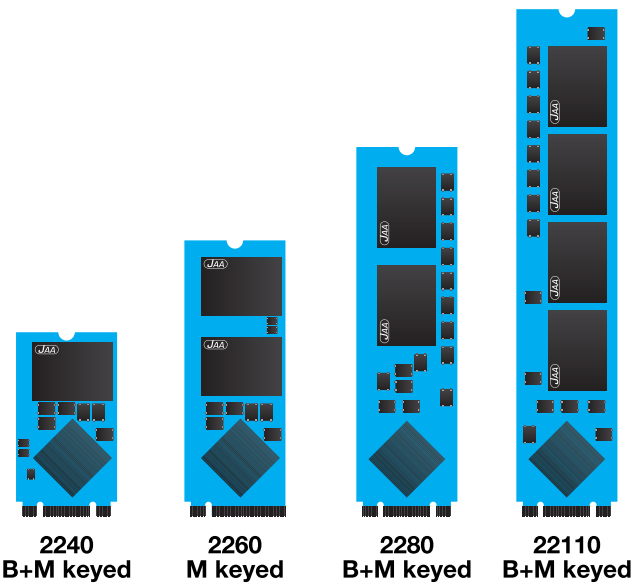


FIGURE 7.9 M.2 SSD sizes and keys

TECH TIP

SSDs that are B+M keyed fit in B or M slots

An SSD that is B+M keyed can fit in a socket that is B keyed or in a socket that is M keyed.

SSDs can also use Non-Volatile Memory Express (**NVMe**), which provides faster performance when accessing the flash memory in SSDs. SSDs perform better when attached to the PCIe four-lane NVMe standard. To use NVMe, an SSD is usually mounted on a PCIe card or attached through an M.2 connector (see Figure 7.10). Make sure the motherboard supports an NVME SSD before buying and installing one.

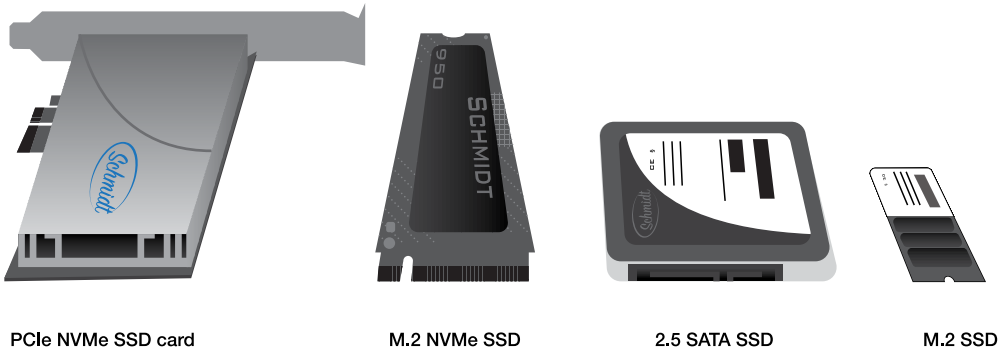


FIGURE 7.10 NVMe and non-NVMe SSDs

TECH TIP

M.2 device could cause a PCIe card to not work

The M.2 slot may share PCIe lanes with a PCIe slot and cause a PCIe card to not be recognized in Device Manager. If this happens, move the PCIe card to a different slot.

Mechanical Drive Interfaces Overview

A hard drive system must use a set of rules in order to operate. These rules make up a standard called an *interface* that governs communication with the hard drive. There are two major hard drive interfaces: AT Attachment (ATA commonly referred to as Serial ATA, or **SATA**) and Small Computer System Interface (SCSI). SATA is the most common in home and office computers. SCSI is more commonly found in storage networks or used with network servers. The SCSI interface has a standard known as Serial Attached SCSI (**SAS**).

Both SATA and SAS drives are used with network-attached storage (NAS) devices, servers, and storage area networks (SANs). A **NAS drive** runs at higher RPMs and stores data for one or more servers and/or computers and is designed to run 24/7 with optimized performance. Figure 7.11 shows SAS drives used in a data center.

FIGURE 7.11 SAS drives

Note that other interfaces can also be used to attach external storage devices. Almost everyone has seen a flash drive or an external hard drive attached to a USB port. This chapter focuses on internal storage interfaces.

SATA and SAS Connectivity

The SATA interface supports both internal and external devices. The original SATA specification transfers data at 1.5 Gb/s and is called SATA 1 or SATA I. The 3 Gb/s version is known as SATA 2 or SATA II, and the latest release, SATA 3 or SATA III, runs at a maximum of 6 Gb/s. These devices are commonly seen marked as SATA 1.5 Gb/s, 3 Gb/s, and 6 Gb/s.

One SATA motherboard port supports only one device. A power cable from the power supply attaches to the SATA device. A data cable attaches between the SATA device and the motherboard. Figure 7.12 shows the two SATA connectors. The data connector is the smaller of the two.

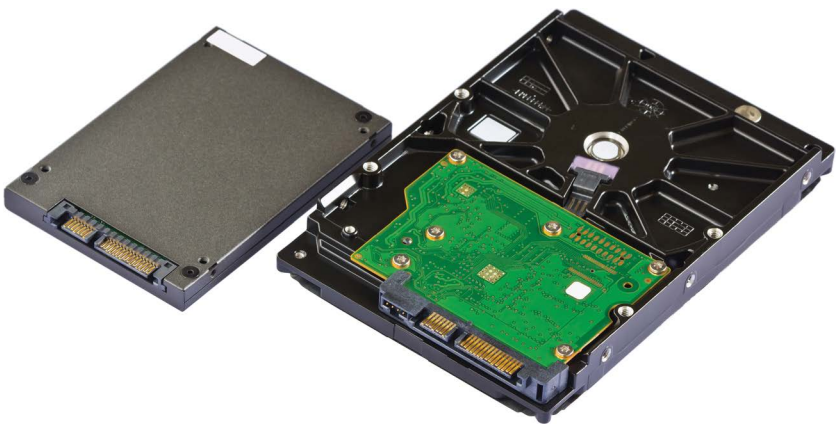


FIGURE 7.12 SATA connectors

Desktop motherboards, laptops, and mobile devices can make use of an mSATA connector for installation of an SSD. The **mSATA** standard only allows use of the SATA standard, whereas the M.2 form factor can make use of SATA or PCIe. Figure 7.13 shows an installed mSATA SSD.

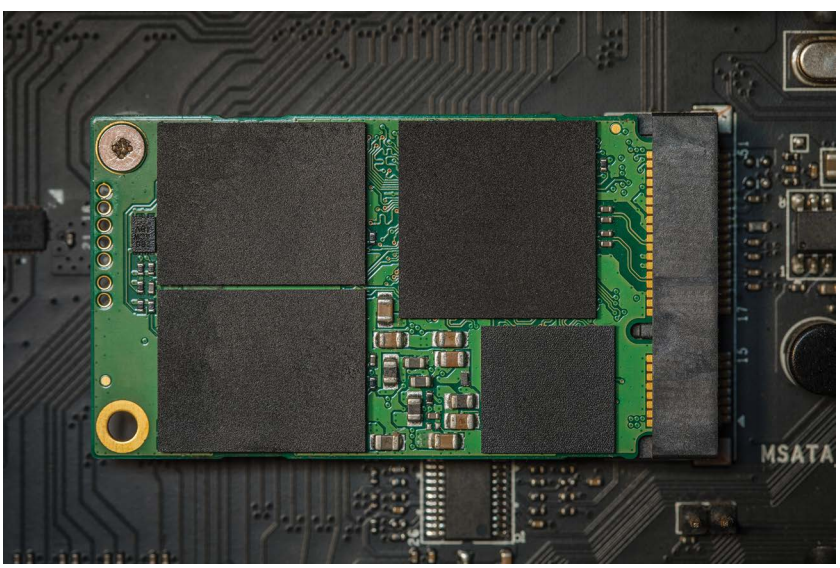


FIGURE 7.13 mSATA SSD and connector

An internal SATA device commonly uses a 15-pin SATA power connector rather than the Molex connector used by older hard drives. However, some drives do ship with Molex connectors. A

Molex-to-SATA converter can be purchased, but the connector can only provide 5V and 12V, not 3.3V. The good news is that most SATA drives do not need the 3.3V line. Figure 7.14 shows an older Molex power connector and an internal SATA power connector.

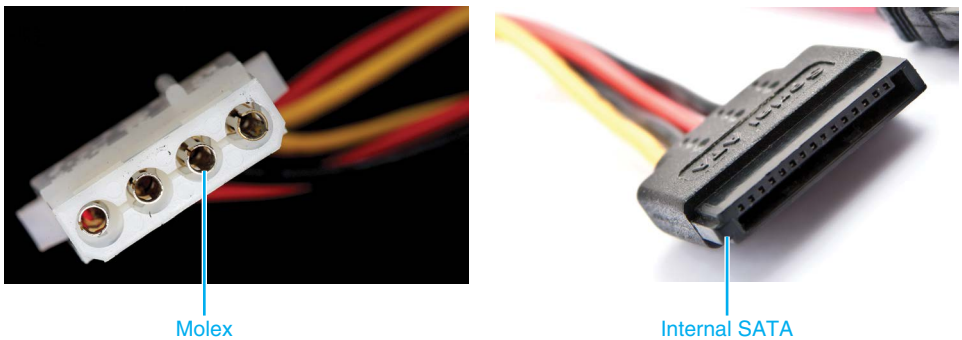


FIGURE 7.14 Drive power connectors

Internal SATA data cables are limited to a maximum of 3.3 feet (1 meter). An internal SATA data cable is more likely to be inadvertently unplugged or partially unplugged than an older drive cable. Special cables with locking mechanisms are in an L shape for hard-to-reach places, and low-profile form factor cases can also be purchased. Figure 7.15 shows these 7-pin internal SATA device cables.

FIGURE 7.15 Internal SATA data cables

External SATA (**eSATA**) provides external device connectivity. It allows shielded cable lengths up to 6.56 feet (2 meters), with faster connections than USB 2.0 or 3.0. Although a standard eSATA connection does not provide power to external devices, an eSATAp combo (USB and eSATA) port can provide power. Note that eSATA is currently not faster than USB 3.1 generation 2.

Figure 7.16 shows an eSATA cable and eSATA port. An eSATA cable can be rated for 1.5 Gb/s, 3 Gb/s, or 6 Gb/s. eSATA cables are limited to 3.3 feet (1 meter) for 1.5 Gb/s devices and 6.56 feet (2 meters) for 3 Gb/s or 6 Gb/s transfers.

FIGURE 7.16 eSATA port and cable

There are several connectors for SCSI drives, but the one most commonly seen by PC technicians is the SCSI connector for a Serial Attached SCSI (SAS) drive. The older SAS connector looks similar to the connectors on a SATA drive, as shown in Figure 7.17.

FIGURE 7.17 Serial Attached SCSI (SAS) connector

A SAS cable is used to connect hard drives or tape drives, and it can be used to connect an SSD to a SAS controller. One cable provides both power and data connections. Figure 7.18 shows the older SAS cable and a newer style.

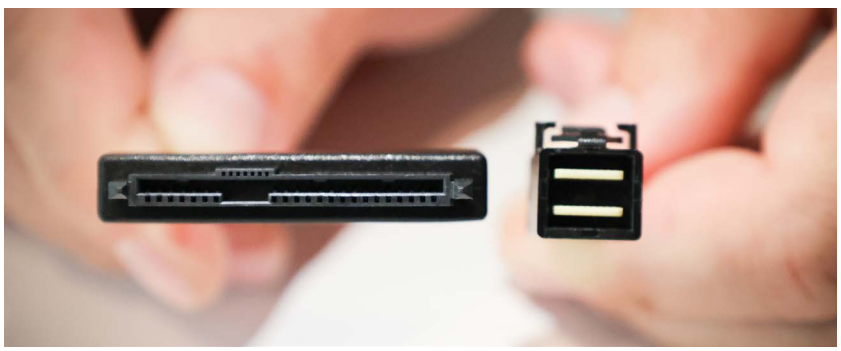


FIGURE 7.18 SAS (Serial Attached SCSI) cable

Storage Device Configuration Overview

Individual drive manufacturers may develop their own configuration steps. Refer to the documentation included with the drive, adapter, or motherboard for installation information. The overall steps for installing a storage device are as follows:

Step 1. Keep the drive in the protective antistatic container until you are ready for the installation. Then use proper antistatic handling procedures when installing the drive and handle the drive by the edges; avoid touching the drive electronics and connectors.

Step 2. Turn off the computer and remove the computer power cord before installing the drive.

Step 3. Physically mount and secure the device in the computer and attach the proper cable.

Step 4. Reconnect the power cord and power on the computer. Configure the BIOS/UEFI, if necessary.

Step 5. If a hard drive is being installed, prepare the drive for data, as described later in this chapter.

SATA Physical Installation

SATA drives are easy to install. A 7-pin **SATA data cable** attaches from the motherboard or SATA card to the internal SATA drive. A 15-pin power supply cable connects to the drive. The internal SATA power connector is unique but could possibly be an older Molex connector. A cable converter can be obtained if a Molex connector is the only one available from the power supply. Figure 7.19 shows how a data cable (on the left) and a power cable (on the right) connect to an internal SATA drive. Figure 7.20 shows how each SATA drive has its own motherboard connector.

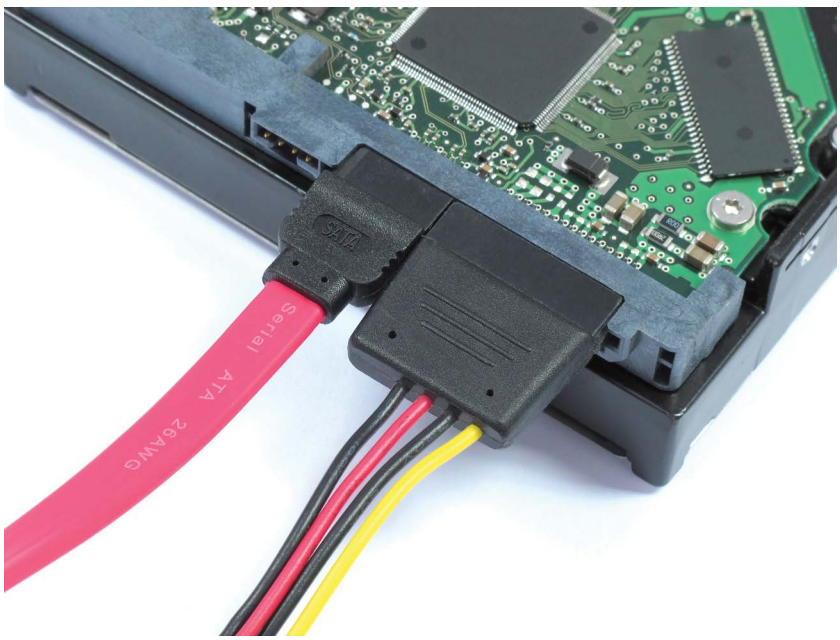


FIGURE 7.19 SATA data (left) and power (right) cabling

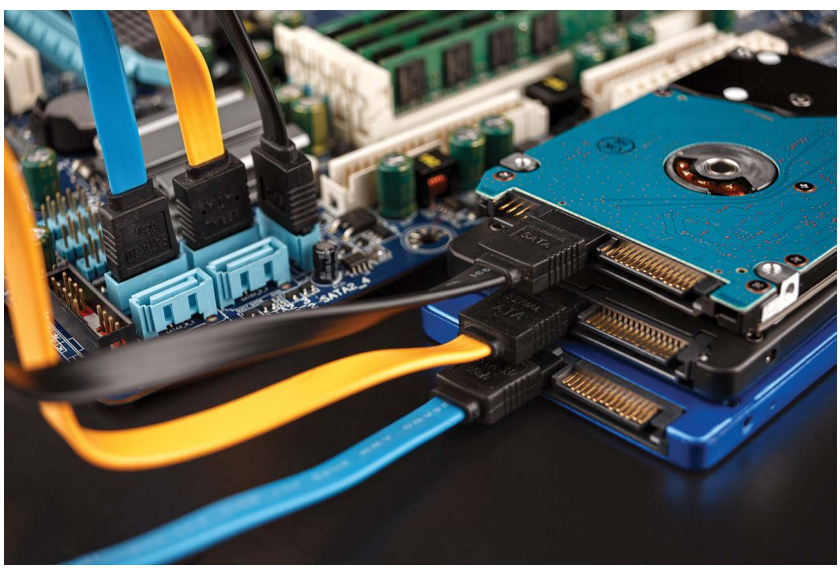


FIGURE 7.20 SATA data connectivity to the motherboard

Figure 7.21 shows an eSATA adapter with two ports. (To see an eSATA card that has both internal SATA ports—on top of the card—and eSATA ports, look back at Figure 4.17 in Chapter 4, "Introduction to Configuration.") To install a SATA/eSATA host adapter, power off the computer

and remove the computer power cord. Remove the computer cover and locate an open expansion slot. Some adapters have jumpers for configurable options. The default settings will work for most adapters, but refer to the adapter's documentation for details.

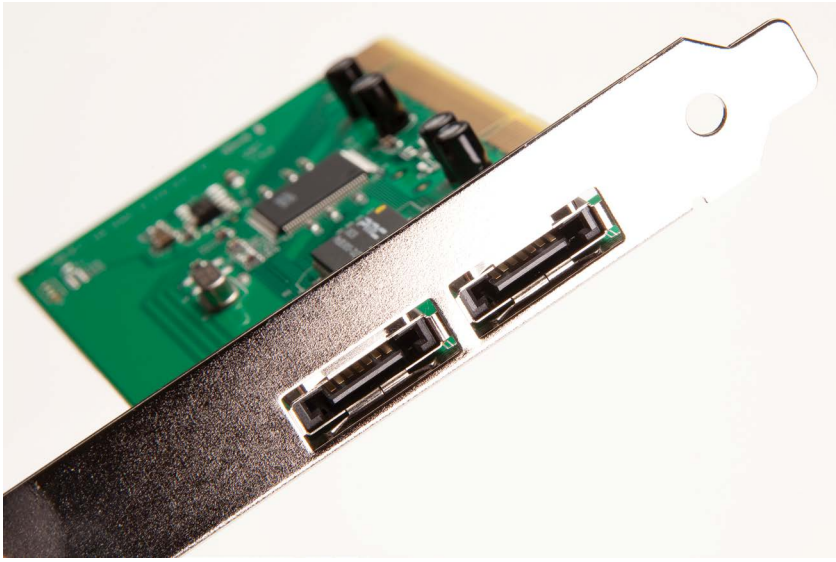


FIGURE 7.21 eSATA card

TECH TIP

Enabling a SATA port in BIOS/UEFI

Some manufacturers require that you enable the motherboard port through the system BIOS/UEFI before any device connected to the port is recognized.

To install an internal SATA hard drive, power off the computer and remove the computer's power cord. Physically mount the drive into a drive bay. Note that you may have to install rails (refer to Figure 5.14 in Chapter 5, "Disassembly and Power") on the side of the drive to slide it into the case or attach screws to the case and hard drive to mount the drive, as shown in Figure 7.22.

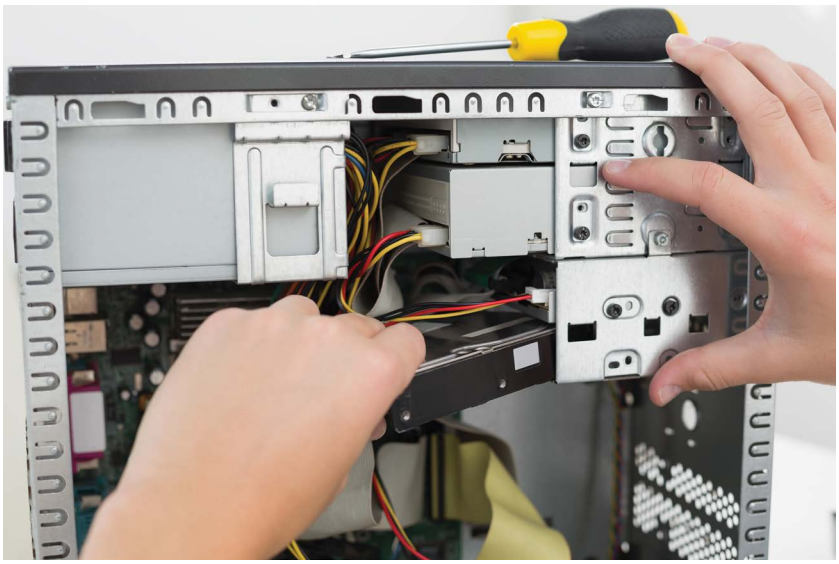


FIGURE 7.22 Installing a hard drive

To add an mSATA module, power off the computer, remove the cover, and locate the mSATA motherboard connector. Insert the card into the connector and attach screws at the opposite end, as shown in Figure 7.23. Power on the computer and make sure the BIOS/UEFI recognizes the module.

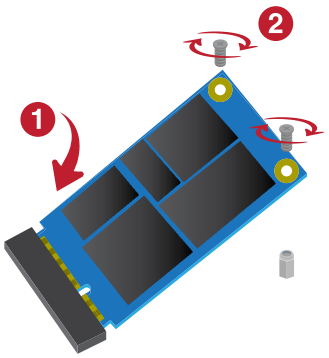


FIGURE 7.23 mSATA Installation

An external (eSATA) drive normally has no jumpers, terminators, or switches to configure. However, when connecting a faster drive to a slower port—such as when installing a 3.0 Gb/s drive in a 1.5 Gb/s port—a jumper may need to be configured so the drive is compatible with the port. Refer to the drive manufacturer's documentation when installing a drive. Attach the power cord to the drive, if applicable, and insert the other end of the power cord into a wall outlet. Attach one end of the eSATA cable to the drive. Plug the other end of the cable into an eSATA port on the computer. Figure 7.24 shows an external hard drive that supports IEEE 1394 (FireWire), eSATA, and USB, as you can see from the ports on the back of the unit.

FIGURE 7.24 External hard drive

Before switching on eSATA drive power, ensure that the drive is positioned where it will stay during operation and that all data and power cords are attached securely. Switch on the drive power. The drive will **mount**. When a drive mounts, a communications channel is opened between the drive and the operating system. Whenever the drive is to be disconnected, it is to be unmounted. Use the Windows *Disk Management* tool to ensure that the drive is recognized. The Disk Management tool is covered later in this chapter.

TECH TIP

Unmounting an eSATA drive

To unmount an eSATA drive, click the *Safely Remove Hardware* icon in the notification area and select the appropriate drive letter. Remove the drive when prompted by the operating system. If you cannot find this icon in Windows, use *File Explorer* to locate the drive, right-click on it, and select *Eject*.

SSD Physical Installation

For a desktop computer, an SSD can be installed using several methods:

- Internally mounted and connected to a SATA motherboard port and installed the same as any other SATA device
- Inserted into an mSATA connector, as described earlier
- Inserted as an NVMe module on a PCIe card or inserted into an M.2 slot
- Inserted as a SATA SSD module inserted into an M.2 slot
- Connected as an external device to an eSATA, eSATAp, or USB port

Figure 7.25 shows an internal SSD that connects to a SATA port and is mounted in a drive slot. Figure 7.26 shows an NVMe module being inserted into an M.2 slot. Be sure the computer is powered off and press the module firmly into the slot. Usually a screw is needed to attach the far end of the module.

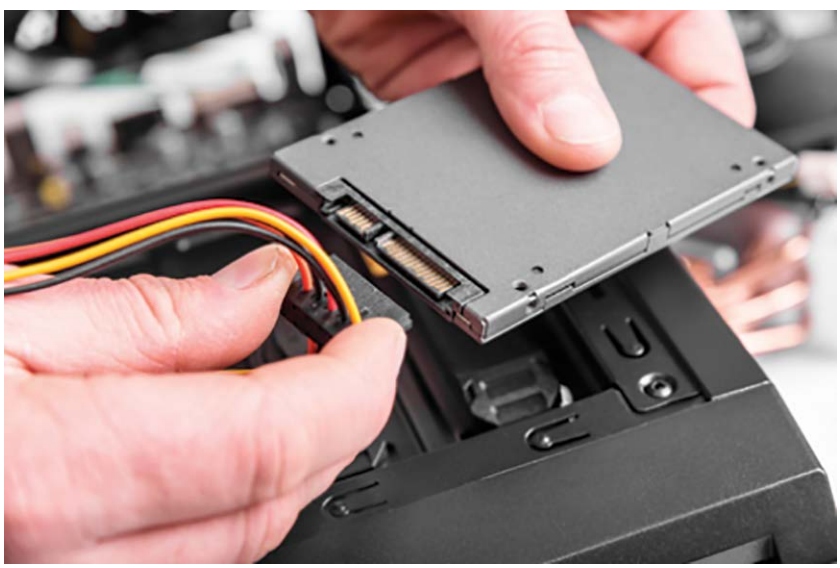


FIGURE 7.25 Internal SATA SSD

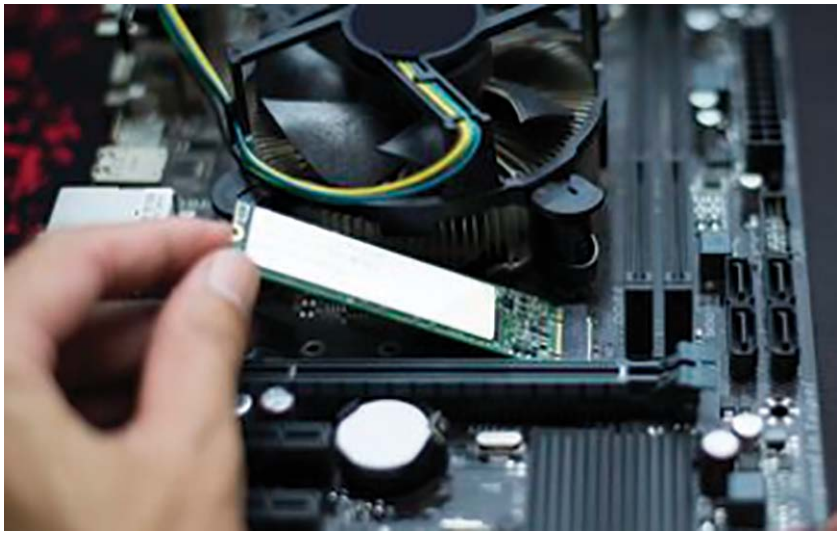


FIGURE 7.26 Internal NVMe SSD in an M.2 slot

SSDs do not normally require special drivers. Refer to the SSD mounting directions provided by the manufacturer. The following steps are generic ones:

Step 1. Power off the computer, remove the power cord, and locate an empty drive bay, mSATA connector, M.2 connector, or PCIe expansion slot, depending on the type of SSD you are installing. If using a SATA connector, ensure that there is an available power connector.

Step 2. Use proper antistatic procedures. If installing into a drive bay, attach mounting brackets to the SSD; the brackets may have to be purchased separately, may be provided with the drive, or may be provided with the computer.

Step 3. Slide the SSD into the drive bay, connector, or expansion slot and secure it, if necessary.

Step 4. If a SATA drive is being installed, connect the data cable from the motherboard or adapter to the drive and attach a power connector.

Step 5. Reinstall the computer cover, reattach the power cord, and power on the computer.

Step 6. Ensure that BIOS/UEFI recognizes the drive

TECH TIP

Beware of static electricity

SSDs are flash memory and are susceptible to static electricity. Use proper ESD handling procedures when installing an SSD.

If installing an external SSD, use the following steps:

Step 1. Attach the appropriate USB or eSATA cable from the drive to the computer.

Step 2. Power on the SSD. The system should recognize the new drive.

TECH TIP

Wanting to upgrade an SSD with another SSD?

When upgrading an SSD that already has the operating system installed on it, you need some space on the original SSD to clone (copy) the drive and some cloning software (which may come with the new drive). During the process, you may need to ensure that the software knows that an SSD is being used. If the cloning process doesn't go well, you might need to boot from a Linux flash drive and use `GParted` to remove sections of the drive before trying the process again. Consider cloning the drive and then resizing the partition.

System BIOS/UEFI Configuration for Storage Devices

A hard drive is configured through the system BIOS/UEFI Setup program. Setup is accessed via keystrokes during the boot process. In today's computers, the BIOS/UEFI automatically detects the hard drive type. The drive type information is saved in CMOS.

TECH TIP

Configure BIOS/UEFI according to the drive manufacturer's instructions

Drive manufacturers normally include documentation describing how to configure the drive in BIOS/UEFI Setup. Also, they provide software for any system that does not recognize the drive.

Hard drives are normally configured using the auto-detect feature, which automatically determines the drive type for the system. Table 7.1 shows the most commonly used device settings. SATA drives can be set in different modes of operation:

> **Legacy mode:** This mode is used in a system that does not have SATA drivers natively.
> **Advanced Host Controller Interface (AHCI) mode:** When enabled, **AHCI** mode allows SATA drives to be inserted/removed when power is on and enables you to use commands to allow the host circuits to communicate with attached devices in order to implement advanced SATA features.
> **RAID mode:** RAID is discussed later in this chapter.

Note that the BIOS/UEFI is also where you select the drive that will boot the system.

TABLE 7.1 Common storage device BIOS/UEFI settings

Device type	BIOS/UEFI setting
SATA/SCSI/SAS	AUTO
SATA	SATA mode: IDE mode (no AHCI or RAID)
SATA	SATA mode: SATA or AHCI (AHCI enabled)
SATA	SATA mode: RAID (AHCI and RAID enabled)
mSATA	AUTO
NVMe SSD	May have to set the PCIe bandwidth to x2 or x4
M.2 SSD	May have to enable; may have to go into a specific PCIe slot and configure the mode to M.2

It is important to ensure that the BIOS/UEFI recognizes a device before you prepare the device to accept data or attempt to have the device store data. No matter the type of storage device, go into BIOS/UEFI and ensure that the device is recognized and configured as needed. You may have to use the advanced settings to access the storage device options.

Hard Drive Preparation Overview

After a hard drive is installed and configured properly and the hard drive type is recognized and seen within the Setup program, the drive must be prepared to accept data. The two steps of hard drive preparation are as follows:

Step 1. Partition the drive.

Step 2. Perform a high-level format on the hard drive.

TECH TIP

Low-level formatting

Low-level formatting may be done at the hard drive factory. Some manufacturers provide software that enables you to do low-level formatting on the drive, but you should do this only at the direction of the manufacturer.

Partitioning a hard drive involves selecting a drive letter to be assigned to one or more sections of the hard drive. **High-level formatting** involves preparing the drive for use for a particular file system and allows the drive to accept data from the operating system. For today's computers, a drive cannot be used until it has been partitioned and had high-level formatting done; thus, technicians must be very familiar with these steps.

Partitioning

As just mentioned, the first step in preparing a hard drive for use is partitioning. Partitioning a hard drive means dividing the drive into separate sections so the computer system sees the hard drive as more than one drive. Each drive section gets a drive letter. Figure 7.27 shows a hard drive platter with some colored sections. Each section between the colored lines can be a volume and can receive a different drive letter.

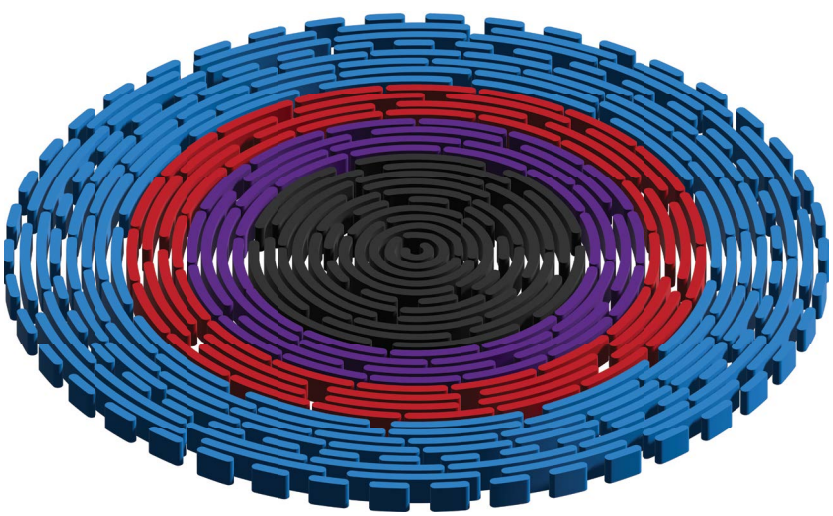


FIGURE 7.27 Visualization of partitioning

Partitioning can be done during the Windows installation process or by using the Windows **Disk Management** program. Similarly, the `diskpart` utility can be used from the command prompt. Disk Management is normally used to partition additional hard drives and to manage all of them. The first hard drive in a system is normally partitioned as part of the Windows installation process. Additional partitions can be created using Disk Management after the operating system is installed.

Partitioning provides advantages such as the following:

> Dividing a hard drive into separate subunits that are then assigned drive letters, such as `C:` or `D:`, by the operating system
> Organizing the hard drive to separate multiple operating systems, applications, and data
> Providing data security by placing data in a different partition to allow ease of backup as well as protection
> Using the hard drive to its fullest capacity

TECH TIP

How to determine what file system is being used

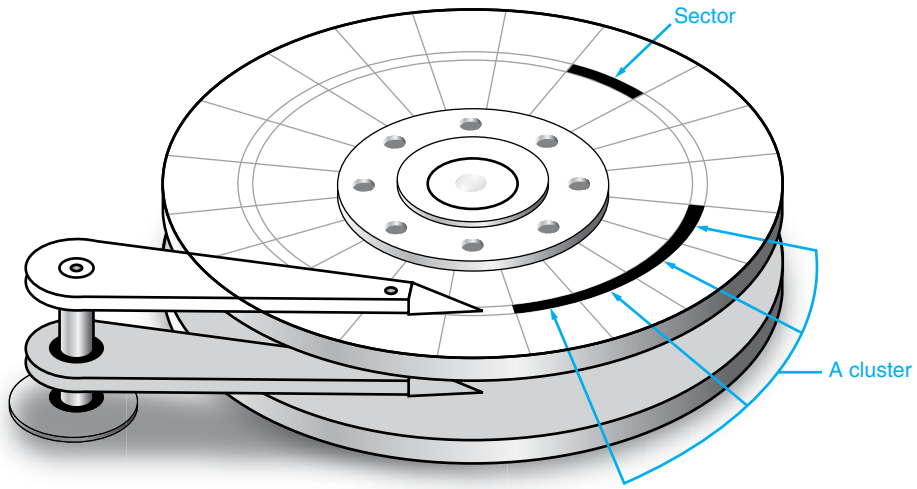
Right-click any drive in *File Explorer* > *Properties*. The *General* tab shows the type of file system being used.

The type of partition and the maximum size of the partition depends on the file system being used. A **file system** defines how data is stored on a drive. The most common Windows file systems are FAT16, FAT32, exFAT, NTFS, and ReFS. What file system can be used depends on what operating system is installed, whether the device is an internal device or external, and whether files are to be shared. Table 7.2 lists file systems and explains a little about each one.

TABLE 7.2 File systems

File system	Description
FAT	Also called FAT16. Used with all versions of Windows. 2 GB partition limitation with old operating systems. 4 GB partition limitation with XP and higher versions of Windows.
FAT32	Supported with all versions of Windows. Commonly used with removable flash drives. Supports drives up to 2 TB. Can recognize volumes greater than 32 GB but cannot create them that big.
exFAT	Commonly called FAT64. A file system made for removable media (such as flash drives and SD cards) that extends drive size support up to 64 ZB in theory, but 512 TB is the recommended max. Made for copying large files such as disk images and media files. Supported by all versions of Windows.
NTFS	Used with Windows and supports drives up to 16 EB, but in practice is only 16 TB. Supports file compression and file security (encryption). Supports individual file compression and has the best file security.
ReFS	Mostly used with Windows Server. Has options to recover corrupt data and is used with larger drives.
Apple File System (**APFS**)	Owned by Apple, designed with encryption in mind, and works across all Apple platforms. It uses GPT partitions, covered later in this chapter, and allows disk cloning.
ext4	An update to ext3 that allows for larger volumes and file sizes within Linux-based operating systems.

The type of file system determines the efficient use of drive space. An operating system sets aside at least one cluster for every file. A **cluster** is the smallest amount of space reserved for one file, and it is made up of a specific number of sectors. Figure 7.28 illustrates the concept of a cluster. Keep in mind that the number of sectors per track varies. The outer tracks hold more information (that is, have more sectors) than the inner tracks.



One cluster is the minimum amount of space for a file.

FIGURE 7.28 Cluster

TECH TIP

How to convert partitions

Use the `convert` program in Windows to convert a FAT16, FAT32, or exFAT partition to NTFS without loss of data. Access a command prompt window and type the command `convert x: /fs:ntfs`, where *x* is the drive letter of the partition being converted to NTFS. Press [Enter] and then press [Y] and press [Enter]. You can add a `/V` switch to the end of the command for a more verbose operation mode.

Any type of partition conversion requires free hard drive space. The amount depends on the size of the partition. An efficiently partitioned hard drive allows more files to be saved because less space on the hard drive is wasted.

A best practice is to put applications in a separate partition from data files. The following are some good reasons for partitioning a hard drive and separating data files from application files:

- Multiple partitions on the same hard drive divide the drive into smaller subunits, which makes it easier and faster to back up the data (which should be backed up more often than applications).
- The data is protected from operating system failures, unstable software applications, and any unusual software problems that occur between the application and the operating system.
- The data is in one location, which makes backing up, organizing, and locating the files easier and faster.

FAT32 partitions have been around a long time and are still used. Flash drives are commonly formatted for FAT32 due to the NTFS "lazy write," which prolongs a write and might not release an external drive for some time. NTFS is the most efficient file system. Table 7.3 lists the default cluster sizes for all versions of Windows.

TABLE 7.3 NTFS partition and cluster sizes

Partition size	Number of sectors	Cluster size
0–16 TB	8	4 kB
16 TB–32 TB	16	8 kB
>32 TB–64 TB	32	16 kB
>64 TB–128 TB	64	32 kB
>128 TB–256 TB	128	64 kB

Figure 7.29 shows a screen capture of the Windows 10 Disk Management window with multiple drives (Disk 0, Disk 1, and Disk 2) and multiple partitions on Disk 1 and Disk 2.

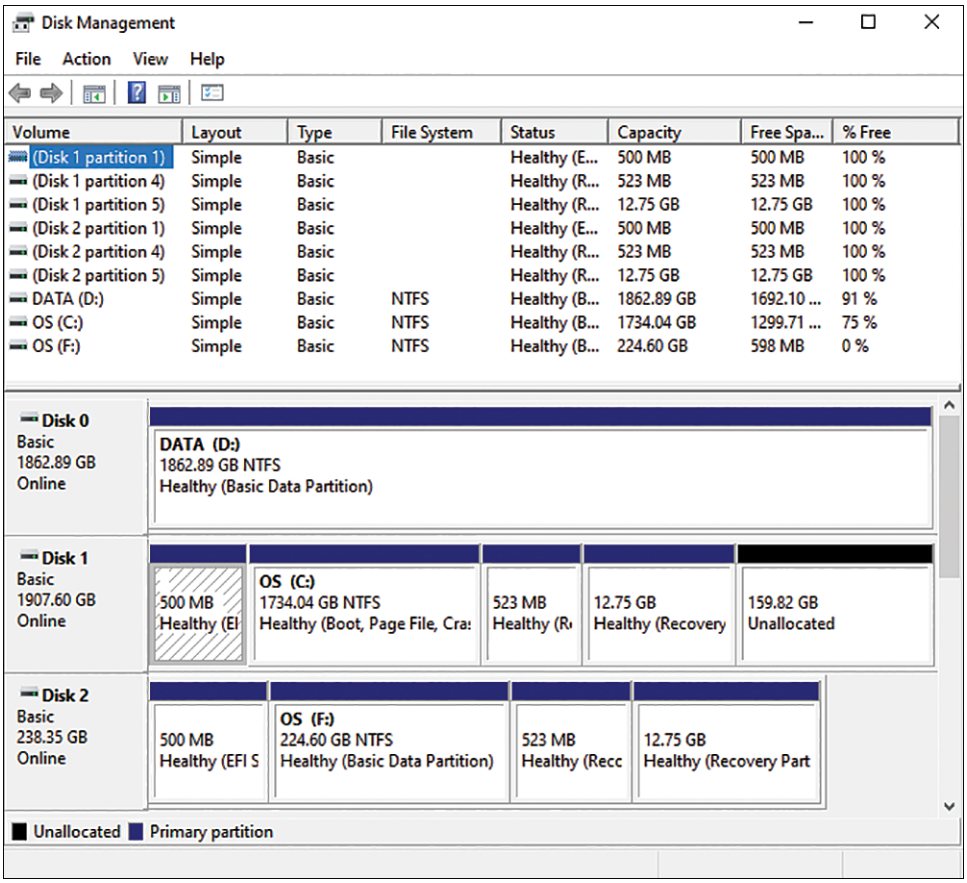


FIGURE 7.29 Windows 10 Disk Management tool

TECH TIP

Benefits of NTFS

NTFS supports disk quotas, which means that individual users can be limited in the maximum amount of usable hard drive space. NTFS can also automatically repair disk problems. For example, when a hard drive sector is going bad, NTFS moves the entire cluster to another cluster.

Partitions are defined as primary and extended. If there is only one hard drive installed in a system and the entire hard drive is one partition, it is the **primary partition**. The primary partition on the first detected hard drive is assigned the drive letter `C:`.

TECH TIP

eSATAs are already partitioned

Most eSATA drives are already partitioned and formatted, but these drives can be repartitioned and reformatted as necessary via the *Disk Management* tool.

If a drive is divided, only part of the drive is the primary partition. In older operating systems, the rest of the cylinders can be designated as the **extended partitions**. An extended partition allows a drive to be further divided into **logical drives**. Figure 7.30 shows a hard drive divided into a primary partition and an extended partition that is further subdivided into two logical drives.

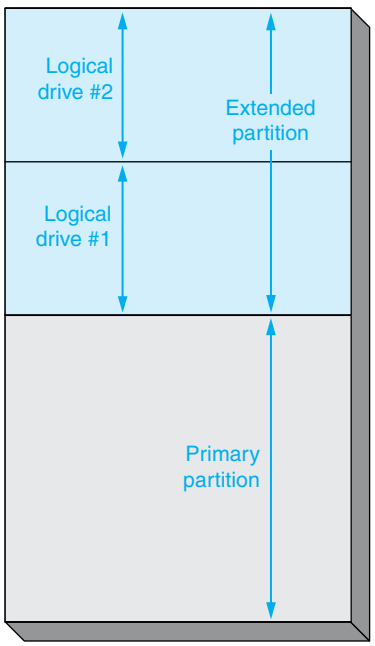


FIGURE 7.30 Two logical drives

A logical drive is sometimes called a **volume**. A volume is assigned a drive letter and can include a logical drive and removable media such as a CD, DVD, BD, or flash drive. There can be only one extended partition per drive. Using this method of dividing up a drive, a single drive could be divided into a maximum of four primary partitions. Remember that a partition is a contiguous section of storage space that functions as if it is a separate drive.

The first drive in a computer system must have a primary partition, but an extended partition is not required. If the drive has an extended partition, it can be further subdivided or split into logical drives that appear as separate hard drives to the computer system. Logical drives created in the extended partition are assigned drive letters such as `D:` or `E:`. The only limit for logical drives is the number of drive letters. A second operating system can reside in a logical drive.

If two drives are installed in a computer, the first hard drive *must* have a primary partition. The second hard drive is not required to have a primary partition and may simply have a single extended partition. If the second hard drive does have a primary partition, it can have an extended partition, too.

When a hard drive is first installed and partitioned, the outermost track on the platter (cylinder 0, head 0, and physical sector 1) is reserved for the partition table. The partition table holds information about the types of partitions created and in what cylinders these partitions reside. The partition table is part of the master boot record (**MBR**), which contains a program that reads the partition table, looks for the primary partition marked as active, and goes to that partition to boot the system. Figure 7.31 shows the locations of important parts of the hard drive that allow booting, reading partitions, and accessing files.

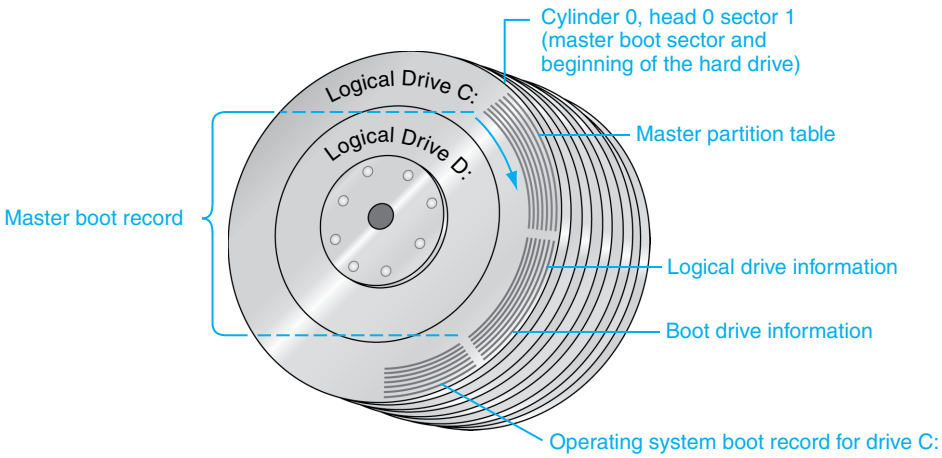


FIGURE 7.31 Hard drive structure

NTFS has two additional terms that you need to be aware of as a technician:

> **System partition:** The **system partition** is the partition on the hard drive that holds the hardware-specific files needed to load the operating system.

> **Boot partition:** The **boot partition** is the partition on the hard drive that contains the operating system.

In Windows, the boot partition and the system partition can be on the same partition.

TECH TIP

What happens when different types of partitions are deleted?

When a partition is deleted, all information in the partition is lost. When logical drives in an extended partition are deleted, all data is lost. The other logical drives within the extended partition retain their information.

The Host Protected Area (**HPA**) is a hidden area of a hard drive that is used to hold a copy of the operating system; sometimes installed applications use the HPA when the operating system becomes so corrupt that a reinstallation is necessary. Many manufacturers provide a BIOS/UEFI setting or a keystroke that can be used when the system boots in order to access this area. The HPA is commonly found on the hard drive beyond the normal data storage locations; it reduces the amount of storage space available for data.

The GUID, or globally unique identifier, partition table (**GPT**) is available with 64-bit Windows operating systems. GPT partitioning is accomplished using the Disk Management tool or using the `diskpart` command-line utility. Table 7.4 compares MBR and GPT disks.

TABLE 7.4 MBR and GPT disk features

Feature	MBR	GPT
Partition size	Up to 2 TB	Up to 9.4 ZB
Types of partitions	Up to 4 primary; supports extended partitions	Up to 128 primary
Firmware	BIOS or UEFI	UEFI
Operating system	Windows	Windows 64-bit or higher
Partition table	Only one partition table	Has a backup partition table

TECH TIP

You lose data when converting to GPT

MBR-based partitions can be converted to GPT and vice versa, but data is not preserved. This is seen only with systems that have a UEFI BIOS. Back up data if you convert!

Special products can be used to partition a hard drive and also repartition without any data loss. Examples include Acronis's Disk Director, EaseUS's Partition Master, and Avanquest's Partition Commander.

How Drive Letters Are Assigned

An operating system assigns drive letters to hard drives during the partitioning step. The order in which partitions are assigned drive letters depends on three factors: the number of hard drives, the type of volume on the hard drives (primary or extended), and the operating system.

If a new drive is installed, drive letters for devices, volumes, partitions, or logical drives are added afterward. Drive letters can be changed through the Disk Management tool or by using the `diskpart` command-line utility. Be careful, though, because some applications have pointers to specific files on specific drive letters.

High-Level Formatting

As mentioned earlier, the second step in preparing a hard drive for use is high-level formatting. High-level formatting must be performed on all primary partitions, logical drives located within extended partitions, and GPT partitions before data can be written to the hard drive. The high-level format sets up the file system so it can accept data.

NTFS allows support for multiple data streams as well as support for every character in the world. NTFS also automatically remaps bad clusters to other sections of the hard drive without any additional time or utility. During the installation process, Windows allows for a **quick format** (where you see "(quick)" after the option) or a full format (sometimes called a standard format). A **full format** scans for and marks bad sectors. This prevents the operating system from being installed on a sector that may cause operating system issues. A quick format simply prepares the drive for data and takes a lot less time than a full format. Use a full format if you suspect that the drive has issues. Figure 7.32 shows the NTFS partition structure once it has been set up and the high-level formatting is completed.

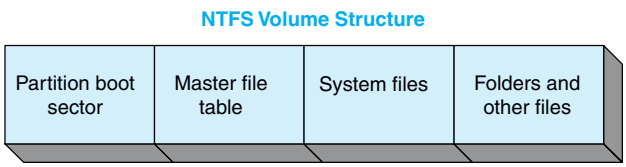


FIGURE 7.32 NTFS volume structure

High-level formatting creates two file allocation tables (FATs): one primary and one secondary. The formatting process also creates the root directory that renumbers the sectors. The **FAT** keeps track of the hard disk's file locations. It is similar to a table of contents in a book as it lists where the files are located in the partition. Table 7.5 shows the differences between the file systems.

TABLE 7.5 Comparing Windows file systems

Specification	FAT16	FAT32	NTFS	exFAT
Maximum file size	4 GB	4 GB	~16 TB	~16 EB
Maximum volume (partition) size	4 GB (2 GB, if shared with a really old computer)	32 GB (max format)	2 TB (or greater)	64 ZB (512 TB recommended)
Maximum files per volume	~64,000	~4 million	~4 billion	Not defined (but 1,000 per directory)

High-level formatting can be performed using the `format` command or by using the Windows Disk Management tool. The area of the disk that contains information about the system files, the DOS boot record (**DBR**), is located on the hard drive's cylinder 0, head 1, sector 1. The more common term for this today (because DOS is no longer a major operating system) is **boot sector**, or volume boot record.

Additional drive partitions and drives installed after the first hard drive partition is created use the Windows Disk Management tool to apply high-level formatting to the drive. The first hard drive partition normally has high-level formatting done as part of the operating system installation process.

Windows Disk Management

In the Windows environment, storage devices are managed with the Disk Management tool. With Windows, there are two types of storage: basic storage and dynamic storage. The big difference between them is that you can make partitions and resize changes with a dynamic disk but not with a basic disk. Table 7.6 explains these and other associated terms. Figure 7.33 shows some of these concepts.

TECH TIP

Hibernation affects disk space

Whenever you put your computer in sleep/hibernate mode, information in RAM is stored temporarily on the hard drive. This requires free hard drive space.

TABLE 7.6 Logical disk management terms

Term	Description
Basic storage	One of the two types of storage. This is what has traditionally been known as a partition. It is the default that is used by all operating systems.
Basic disk	Any drive that has been partitioned and set up for writing files. A basic disk has primary partitions, extended partitions, and logical drives contained within the extended partitions.
Dynamic storage	The second type of storage, contrasted with basic storage. Allows you to create primary partitions, logical drives, and dynamic volumes on storage devices. It is more powerful than basic storage in that it allows creation of simple, spanned, or striped volumes using dynamic disks. It is also easy to shrink or expand.

Term	Description
Dynamic disk	A disk made up of volumes. A volume can be the entire hard disk, parts of the hard disk combined into one unit, and other specific types of volumes, such as single, spanned, or striped volumes. Cannot be on a removable drive.
Simple volume	Disk space allocated from one hard drive. The space does not have to be contiguous.
Spanned volume	Disk space created from multiple hard drives. Also known as "just a bunch of disks" (**JBOD**). Windows writes data to a spanned volume in such a way that the first hard drive is used until the space is filled. Then, the second hard drive's space is used for writing. This continues until all hard drives in the spanned volume are used.
Striped volume	Disk space in which data is written across 2 to 32 hard drives. It is different from a spanned volume in that the drives are used alternately. Another name for this is striping, or RAID 0 (covered in the next section).
System volume	Disk space that holds the files needed to boot the operating system.
Boot volume	Disk space that holds the remaining operating system files. Can be the same volume as the system volume.
RAW volume	A volume that has never had high-level formatting performed and that does not contain a file system.

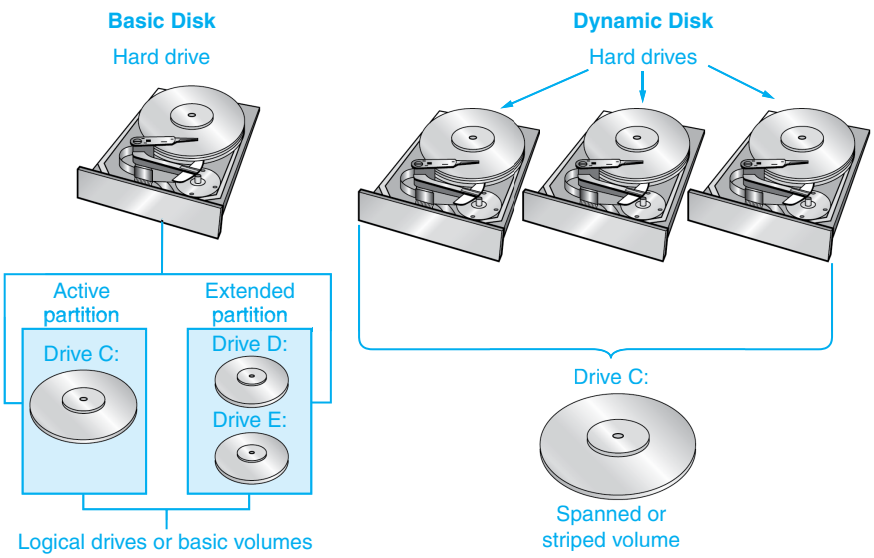


FIGURE 7.33 Disk Management concepts

A basic disk, simple volume, or spanned volume can be resized, shrunk, or expanded without affecting data. When working with Disk Management, right-click on a drive to see all the available options, such as viewing the properties of the drive, marking a partition as active, changing the drive letter and paths, formatting, extending a volume, shrinking a volume, adding a mirror, or deleting a volume.

TECH TIP

Managing disks and partitions

Use the *Disk Management* tool (from the *Computer Management* console) or the `diskmgmt.msc` command to determine what type of partition you have, to work with dynamic disks, or to convert a basic disk to a dynamic one. This conversion process cannot be reversed.

To extend (make larger), split (break into two sections), or shrink (reduce the size of) a partition, follow these steps:

Step 1. Access the Windows *Disk Management* tool.

Step 2. Right-click on the drive volume and select either *Shrink Volume* or *Extend Volume*.

Figure 7.34 shows a hard drive partition and settings used to shrink it so that another partition can be created.

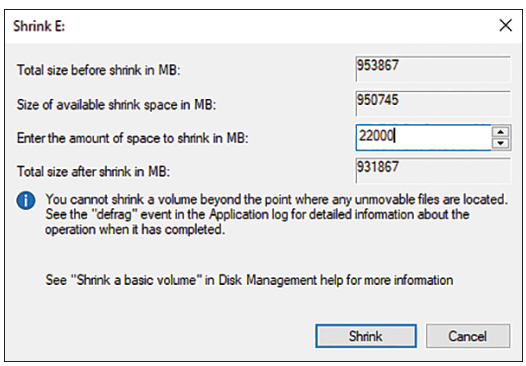


FIGURE 7.34 Resizing a partition

Fault Tolerance

With a **drive array**, two or more hard drives are configured for speed, redundancy, or both (see Figure 7.35). Redundant array of independent (or inexpensive) disks (**RAID**) allows reading from and writing to multiple hard drives for larger storage areas, better performance, and fault tolerance. Fault tolerance is the ability to continue functioning after a hardware or software failure. A RAID array can be implemented with hardware or software. Hardware RAID is configured through the BIOS/UEFI.

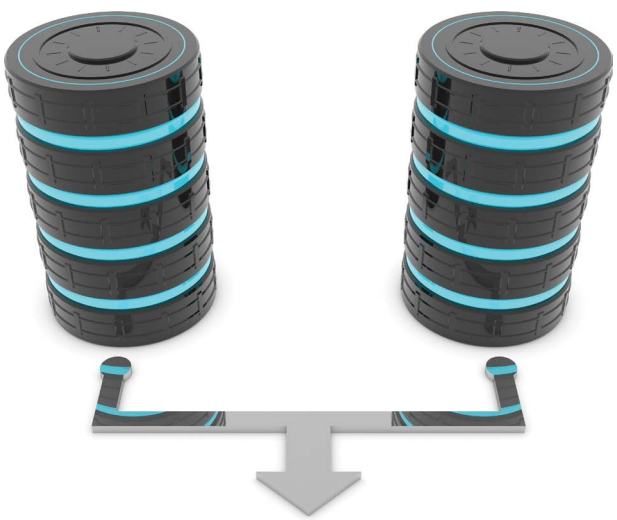


FIGURE 7.35 RAID

Generic steps for configuring hardware RAID are as follows:

Step 1. Ensure that the motherboard ports that you want to use are enabled.

Step 2. Ensure that you have RAID drivers for the hard drives used in the RAID.

Step 3. Physically install and cable the hard drives.

Step 4. Enter BIOS/UEFI and enable RAID.

Step 5. Configure RAID in BIOS/UEFI or through a special key sequence to enter the RAID BIOS configuration.

Step 6. Install Windows on a RAID by using the Custom (Advanced) Installation option.

Software RAID is configured through Windows or through software provided by the RAID adapter manufacturer. If you want to be able to control RAID through Windows and resize the volumes or make adjustments, use software RAID.

RAID can also be implemented with flash cache modules (FCMs) and a traditional mechanical hard drive. Intel has specific processors and chipsets that support RAID configurations. Software on the host device and/or device drivers provides optimization and oversight.

RAID comes in many different levels. The ones on the A+ certification exam are RAID levels 0, 1, 5, 6, and 10. Some motherboards support "nested" RAID, in which RAID levels are combined. This method also increases the complexity of the hard drive setup. Table 7.7 explains the RAID levels.

TABLE 7.7 RAID

RAID level	Description
0	Also called **disk striping** or disk striping without parity. Data is alternately written on two or more hard drives, which increases system performance. These drives are seen by the system as one logical drive. **RAID 0** does not protect data when a hard drive fails. It is not considered fault tolerant. It has the fastest read and write performance.
1	Also called **disk mirroring** or disk duplexing, **RAID 1** protects against hard drive failure by using two or more hard drives and one disk controller. The same data is written to two drives so that if one drive fails, the system continues to function. Disk duplexing is similar except that two disk controllers are used. With disk duplexing, performance is slightly degraded when writing data because it has to be written to two drives.
0+1	A striped set and a mirrored set combined. At least four hard drives are required, and they need to have an even number of disks. A second striped set mirrors a primary striped set of disks. Also called RAID 01, this mode can read from the drive quickly, but there is a slight degradation when writing.
1+0	A mirrored set and a striped set combined with at least four hard drives. The difference between 1+0 and 0+1 is that 1+0 has a striped set from a set of mirrored drives. This mode, also called **RAID 10**, can read from the drive quickly but has a slight degradation when writing.
5	Also called disk striping with parity. **RAID 5** writes data to three or more hard drives. Parity information is included with the data. If a drive fails, the data can be rebuilt based on the information from the other two drives. This level can read and write data quickly.
6	**RAID 6** is like RAID 5 but has additional parity information that allows recovery from two failed drives. It is slower than RAID 5.

Figure 7.36 shows the different types of RAID. With RAID 0, blocks of data (B1, B2, B3, and so on) are placed on alternating drives. With RAID 1, the same block of data is written to two drives. RAID 5 has one drive that contains parity information (P) for particular blocks of data such as B1 and B2.

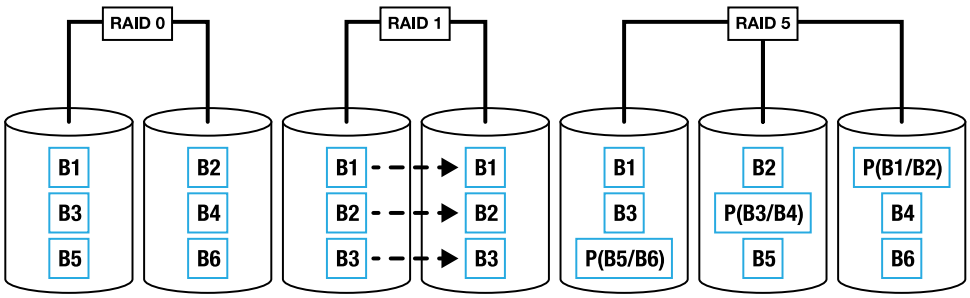


FIGURE 7.36 RAID concepts

Windows 7 Professional and higher versions support simple, spanned, striped, and mirrored volumes. Keep in mind that a spanned volume does not provide redundancy or fault tolerance, as most of the RAID levels do.

RAID drives are often hot swappable; that is, they can be removed or installed while power is applied to the computer. USB, SATA, and SAS all support hot swapping, but RAID is not required to be supported. Refer to the drive and computer manual before hot swapping any hard drive. RAID rebuilds are time and input/output (I/O) intensive. Be prepared for the system to be out of commission for a while; the amount of time the system will be unavailable depends on the size of the drive and the RAID type.

Hardware RAID for home or business computers used to require a separate RAID adapter and software to perform the RAID. Now many motherboards support RAID, and so do the Windows 7 and higher operating systems. Many times, you must configure the motherboard BIOS/UEFI for RAID as part of your initial configuration. Table 7.8 shows some common RAID BIOS configuration parameters.

TABLE 7.8 RAID BIOS/UEFI configuration settings

BIOS/UEFI setting	Description
SATA mode: AHCI Mode	A mode that may mean that hot swapping is supported. A set of commands can be used to increase storage performance.
SATA mode: RAID Mode or Discrete SATA Mode	Allows you to select a particular RAID level and the drives associated with the RAID.
SATA drives: Detected RAID Volume	Usually an information screen that shows the type of RAID configured, if any.
SATA drives: eSATA Controller Mode	Allows configuration of RAID through the eSATA port.
SATA drives: eSATA Port x Hot Plug Capability	Allows hot swapping to be enabled or disabled for eSATA ports.

Windows Storage Spaces

Microsoft Windows 10 and 11 support **Windows Storage Spaces**, which combines drives into a flexible data storage option. An administrator first creates a storage pool, which is two or more physical disks that can be different types, such as a SATA drive and a USB drive. A storage space

is a virtual disk created from available space in a storage pool. There are three types of storage spaces:

> **Simple:** Data is striped across physical disks. No resiliency is provided. This type of storage space provides the highest performance, but there is a loss of data if one disk fails.
> **Parity:** Data is striped across the physical disks and includes parity information. This type of storage space slows performance.
> **Mirror:** Data is striped across multiple disks, and the same data is copied for the highest level of resiliency.

Unlike with RAID, if you add a drive to a storage space, the data is not rewritten to include the new drive. Instead, new data uses all of the drives. To create a storage space, follow these steps:

Step 1. Access the *Storage Spaces* Control Panel link and select *Create a new pool and storage space*.

Step 2. Select the drives to be used and then select *Create Pool* (see Figure 7.37).

Step 3. Name the storage space and select the drive letter, file system, resiliency type, and pool size and then select *Create Storage Space*.

When the storage space is created, the storage drive letter appears in File Explorer.

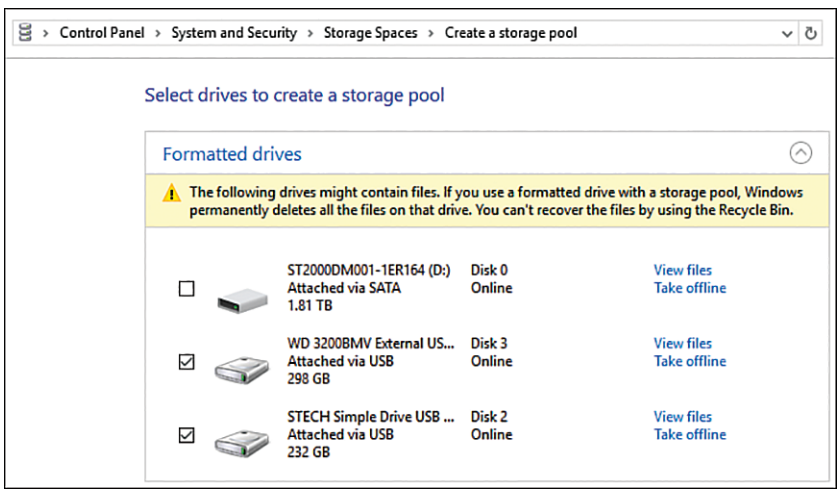


FIGURE 7.37 Windows Storage Spaces: Creating a storage pool

Disk Caching/Virtual Memory

One feature you should look at when choosing a hard drive, an optical drive, or an SSD is the amount of cache on the drive. The **disk cache** (sometime called a data buffer) is SRAM on the drive that takes in data and holds it there until the drive has time to write the data. The cache can also be used when data is requested from the drive. The drive reads more data than requested and holds that data until needed without returning to the hard drive. Figure 7.38 shows this concept.

A different way of using a hard drive is with virtual memory. Using virtual memory means using hard drive space as if it were RAM. With virtual memory, the amount of RAM installed in a system is not enough to handle the operating system and the multiple applications that are opened and being used. Only the program and data of the application that is currently being used is in RAM. The rest of the open applications and data are stored in a paging file (also called a swap file, `pagefile.sys`, or page file) on the hard drive. When you click over to a different application that is held in the swap file, data is moved from RAM into the swap file, and the data you need to look at is moved into RAM for faster access and data manipulation.

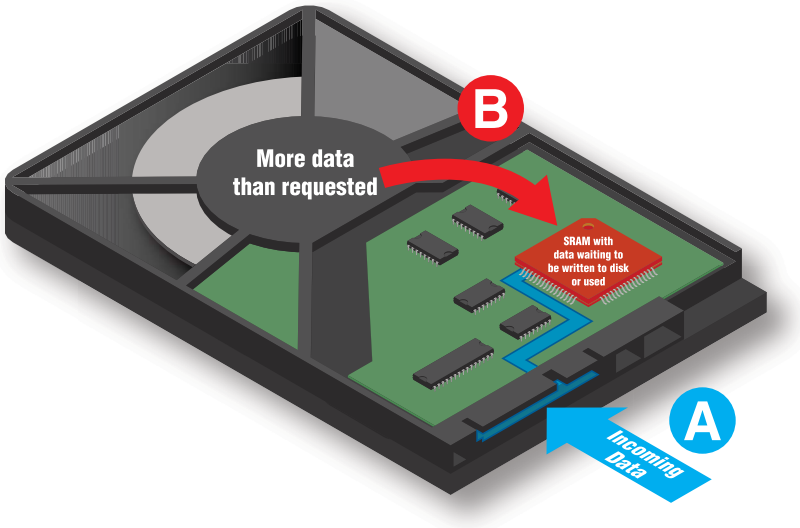


FIGURE 7.38 Disk cache

The disk cache is dynamic, which means it increases and decreases the cache size as needed. If the system begins to page (that is, constantly swap data between RAM and the hard drive), the cache size automatically shrinks. In Windows, the virtual memory swap file is called `pagefile.sys`. To adjust it in Windows 11, access *Settings*. Then, in the *Find a Setting* search textbox, type `performance`. Select the *Adjust the Appearance and Performance of Windows* link > *Advanced* tab > *Change* button (as shown in Figure 7.39). Finally, change the parameters and click the *OK* button twice.

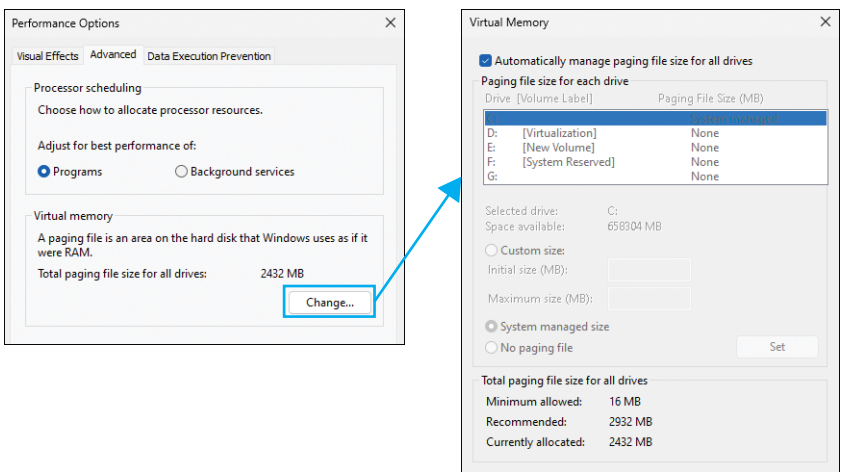


FIGURE 7.39 Windows 11 virtual memory manager

TECH TIP

Where to keep a swap file

If multiple hard drives are available, a technician might want to move the swap file to a different drive. Put the swap file on the fastest hard drive unless that hard drive lacks space. The swap file can reside on multiple hard drives. It is best to keep the swap file on a hard drive that does not contain the operating system.

Memory space is divided into 4 KB blocks of memory called *pages*. The operating system allocates as much available RAM as possible to an application. Then the operating system swaps, or pages, the application to and from the temporary swap file as needed. The operating system determines the optimum setting for this swap file; however, the swap file size can be changed.

The page file can also get corrupted. If it does, in Windows, hold down ⇧Shift while selecting *Restart* from the power icon > *Troubleshoot* > *Advanced Options* > *Startup Repair*.

TECH TIP

Adding more physical RAM helps with caching

One of the most effective ways to speed up a computer is to reduce the amount of data that has to be swapped from the hard drive to RAM. This is done by increasing the amount of motherboard RAM.

Troubleshooting Storage Devices Overview

Storage devices are critical to computer users because they hold users' data. Sadly, users do not back up their data or system frequently. Blackblaze (www.blackblaze.com) did a study of more than 25,000 mechanical drives and found that over a four-year period, 78% of the drives lasted longer than four years, but 22% of them failed during the first four years. Mechanical drives have moving parts, and moving parts fail. Expect it and plan for recovery!

Tools that a technician needs to troubleshoot storage devices include both hardware and software. The list that follows is a good starting point:

- Screwdriver to loosen or remove screws.
- External hard drive enclosure to be able to check a drive from another system or be able to determine whether the problem is the drive or the motherboard port (refer to Figure 7.4 to see one).
- Access to operating system commands and Windows tools to check a drive for physical and file structure errors and attempt to fix them.

Two things to remember when troubleshooting a storage device are to be patient with and kind to the user. A technician dealing with storage devices is often faced with angry users. Stay calm. Just because a system will not boot from the hard drive does not mean it is bad. There are things you can do, as you will soon see.

Dealing with Degraded Performance

Keeping a computer system in a clean and cool operating environment extends the life of the hard drive. Hard drive failures are due to problems with moving parts (heads and motors), power fluctuations, and/or failures. Performing preventive maintenance on an entire computer is good for all components inside the computer, including the hard drive subsystem.

Windows has three great tools to use in hard drive preventive maintenance: Error Checking (*Check Now* or the *Check* button), Disk Cleanup, and Disk Defragmenter. In Windows, you can use a disk tool to locate **lost clusters**, which are clusters that have become disassociated from data files but still occupy disk space. Error Checking/Check Now is also good for dealing with intermittent read/write errors. Locate the drive in File Explorer, right-click the drive, and then select *Properties* > *Tool* tab > *Check*.

The Windows program **Disk Cleanup** removes temporary files, removes offline internet files, empties the Recycle Bin, compresses unused files, and removes unused programs—and it prompts you before doing any of this. In Windows do a search for and access *Disk Cleanup*. In the Disk Cleanup window, select the checkboxes for the options desired and click *OK* (as shown in Figure 7.40).

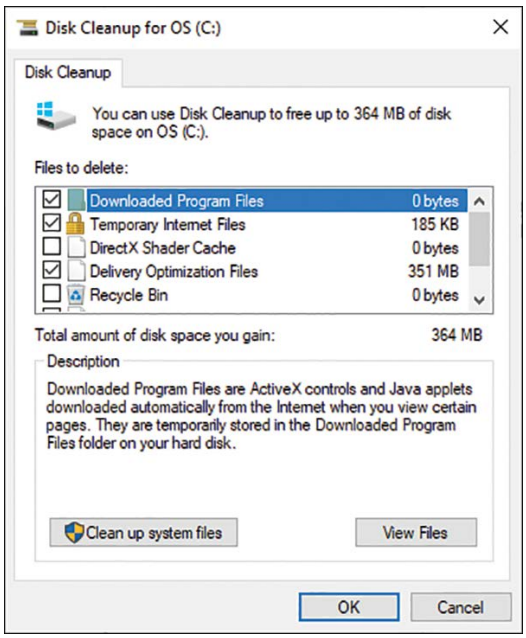


FIGURE 7.40 Disk Cleanup window

TECH TIP

Running Disk Cleanup from a command prompt

To run Disk Cleanup from a command prompt, type `cleanmgr.exe` and then press Enter.

Drive performance affects system and application performance. Some vendors list the number of input/output operations per second (**IOPS**) as a measure of storage performance, but this is not a consistent measurement. If a drive is slow to respond or has **extended read/write times**, you can use Task Manager > *Performance* tab > click on the drive and look at the average response time, read speed, and write speed data. There is also a link there that you can use, or you can open Windows Resource Monitor (`resmon.exe`) > *Disk* tab to see the specifics on the data.

Over time, as files are added to a hard drive, the files become fragmented, which means the clusters that make up a file are not adjacent to one another. Fragmentation slows down a hard drive in two ways: The FAT has to keep track of scattered clusters, and the hard drive read/write head assembly must move to different locations on the drive's surface to access a single file. Figure 7.41 illustrates fragmentation of three files (F1, F2, and F3) and the results after defragmentation has been executed on the hard drive. **Defragmentation** is the process of placing files in contiguous sectors.

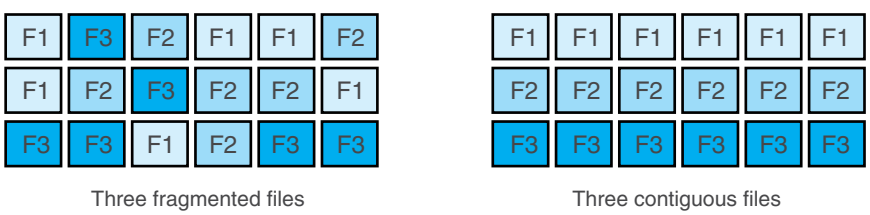


FIGURE 7.41 Fragmented hard drive/defragmented hard drive

TECH TIP

Tool order matters

Use the Error Checking (Check Now or Check) and Disk Cleanup tools before running the Disk Defragmenter tool.

Defragmenting a hard drive makes for faster hard disk access. This process also extends the life of the hard drive by reducing the drive's mechanical movements. Windows now performs hard drive optimization as needed. You can manually execute optimization by using the Disk Defragmenter tool, which you can access in several ways:

> In Windows, open *File Explorer*, locate a hard drive letter, right-click it, and select *Properties* > *Tools* tab > *Optimize*.
> From a command prompt or search textbox, use the `defrag` command.
> From a command prompt or search textbox, use the `dfrgui.exe` command

TECH TIP

SSD defragmentation kills

Do not defragment an SSD as you would a magnetic hard drive. Defragmentation causes more reads and writes, which reduces the life span of the SSD.

Data Loss and Corruption

A hard drive typically has a warranty of three years, but people use their computers longer than that. Hard drives fail, and data is lost or becomes corrupted (see Figure 7.42). The best prevention is to back up your drive. Multiple backup solutions exist for protecting your data. You can use a dedicated external drive that will back up your entire drive with one click or leverage free cloud storage services like Google Drive and Microsoft OneDrive.

FIGURE 7.42 Drive failure

In the corporate world, companies often buy **file recovery software** or hire other companies to provide it as a service. Technicians who do not have this software should at least have the name of a company they recommend or use.

Hard drives have built-in technology to mark bad sectors and move the data to different locations on the drive. The moved data may be corrupted even though it is moved. Here are some recommendations for repairing corrupt data:

- Restore the data from a backup.
- For one or more system files, use the **System File Checker** tool `sfc /scannow` command.
- If the `sfc` command does not work, reinstall the operating system by using the *Refresh your PC* option, which keeps the apps that came with the PC and the apps installed from the Microsoft Store. You can also use the *Reset this PC* option, which allows you to choose whether to keep your personal files. Note that you do have to reinstall your applications.
- Use the `chkdsk` command. Use the `/f` option to fix any errors found on the disk. Use the `/r` option to locate bad sectors and recover any readable information.

Troubleshooting New Storage Device Installation

Most problems with new drive installation stem from improper configuration of jumpers on PATA drives or problems with cabling. BIOS/UEFI and the operating system can display a multitude of symptoms, including POST error codes, beeps, and messages, such as the following:

- Hard drive not found
- No boot device available
- Hard drive not present
- Inaccessible boot device
- Invalid boot disk

The following tips assist with checking possible new drive problems:

- Check the physical settings (such as the power cable, jumper settings, secure data cable, data cable pin 1 orientation, and device placement on the data cable).
- Check the drive type setting in BIOS/UEFI Setup and ensure that the ports (especially SATA ports) are enabled.
- If everything works well, but the **drive activity LED** doesn't blink when storing/retrieving data, check your front panel cable connection to the motherboard.
- Check for other **LED status indicators** or error codes shown on the motherboard. Use the motherboard/system documentation to see what the lights/codes mean.
- If you get a **drive not recognized** error, check to see if the drive is recognized by the operating system in Disk Management. If the drive is missing, check cabling, device driver version, and BIOS/UEFI settings. Try restarting the computer.
- If after you have configured the drive, installed it, and powered it on, the BIOS/UEFI shows the drive type as "None" or "Not installed," or if it displays all 0s in the drive parameters even though you set it to automatically detect the drive, then the BIOS/UEFI is not able to detect it. Check the BIOS/UEFI SATA mode and BIOS/UEFI version. Check all jumper settings, check the cable connection(s), and check the power connection. In Setup, reduce any advanced features to their lowest values or disable them. Increase the amount of time the computer takes to initialize the hard drive by going into Setup and modifying features such as hard drive boot delay or setting the boot speed to the lowest value. This gives the hard drive more time to spin up and reach the appropriate RPM before data is read from it. Make sure the motherboard port is enabled.
- If the BIOS/UEFI recognizes the device, but you have a **missing drive in the OS**, the drive may not have been initialized or partitioned. Use the Windows Disk Management tool to fix the issue.

> Determine whether the drive has been partitioned and one partition has been marked as the active partition. Also determine whether high-level formatting has been applied to the drive.
> If the hard drive does not format to full capacity, your BIOS/UEFI may not support the larger drive and/or the BIOS/UEFI must be upgraded, you may have selected a file system that does not support larger partitions, or you may need an updated driver.
> If during power-on the hard drive does not spin up or the hard drive spins down after a few seconds, check the power connector, the data cable, the drive recognized in BIOS/UEFI, jumper settings, energy management jumpers or settings in Setup, and any software that came with the drive that enables power management. Disable power management in BIOS/UEFI and/or the operating system. Try installing the drive in another system.
> If the system locks or you get a blue screen of death (**BSOD**), write down the message or code, if any, and try a warm boot (Ctrl+Alt+Del). If the drive is recognized after the warm boot, the Setup program may be running too fast for the drive to initialize. Refer to the hard drive documentation to see if the hard drive has a setting to help with this problem.
> If an SSD is not recognized by the system, try reseating the drive and ensure that it is properly inserted into the motherboard slot.

Troubleshooting Previously Installed Storage Devices

Previously installed boot devices can have all of the same symptoms as a newly installed storage device plus the following additional ones:

> **Clicking sounds**
> **Audible alarms**
> Read/write errors
> Slow to respond
> BSOD or spinning pinwheel (macOS and Windows)

Because many drives are mechanical devices, they make noises. Sometimes these noises occur because the hard drive is being used as virtual memory too much due to a lack of physical RAM. Some noises are normal, and others indicate problems, as shown in Figure 7.43.

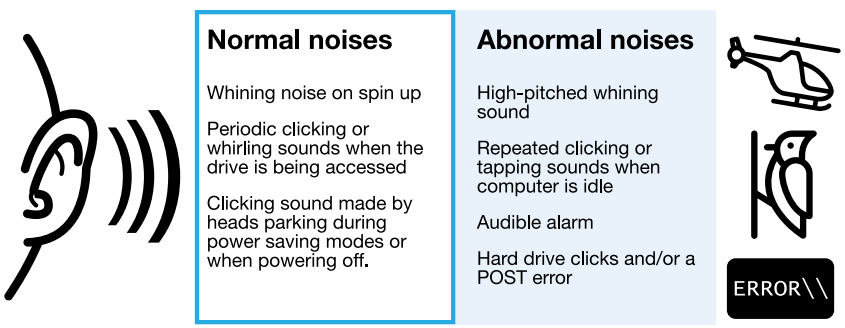


FIGURE 7.43 Hard drive noises

When a hard drive starts making a loud clicking, tapping, or **grinding noise**, back up the drive immediately and purchase a replacement drive. The drive is failing! Take the same steps if you hear an audible alarm. Something is wrong or going wrong with that drive.

The following are generic guidelines for hard drives that have worked but are now having problems or for when a computer **fails to boot**:

> Run a virus-checking program after booting from virus-free boot media. Many viruses are specifically designed to attack hard drives. If you have to wipe a hard drive to ensure that the

virus is erased before reinstalling the operating system, applications, and data, ensure that you do a full format and not a quick one as part of the operating system installation process.

> Has there been a recent cleaning of the computer, or has someone recently removed the top from the computer? If so, check all cables and verify that they are connected correctly. Check the power connection to the hard drive.

TECH TIP

Does your hard drive stick?

Place a hand on top of the drive as you turn on the computer. Does the drive spin at all? If not, the problem is probably a "sticky" drive or a bad drive. A hard drive must spin at a certain RPM before the heads move over the surface of the hard drive. To check to see whether the drive is sticking, remove the drive and try spinning the spindle motor by hand. If it is not moving, remove the drive, hold the drive in your hand, and give a quick jerk with your wrist. Another trick that may work is to remove the hard drive from the case, place the drive in a plastic bag, and put it in the freezer for a couple hours. Then remove the drive and allow it to warm up to room temperature and reinstall the drive into the system and try it.

> If the hard drive light flashes quickly on bootup, the controller is trying to read the partition table in the master boot record. If this information is not found, various symptoms are possible, such as the error messages "Invalid boot disk," "Inaccessible boot device," "Invalid partition table," "Error loading operating system," "Missing operating system," or "No operating system found." Use the `diskpart` command from the Windows Recovery Environment (WinRE) to see whether the hard drive partition table is okay. Here are a few commands to try within this utility: `list disk`, `list volume`, `list partition`, `detail disk`, `detail volume`, and `detail partition`. Try running `bootrec /fixmbr` or use a hard drive utility to repair the partition table.

> A common problem is that the operating system cannot be found, which is indicated with the "**bootable device not found**" or "**no OS found**" message (or other messages, such as "Disk Boot Failure," "Non-System Disk," and "Disk Error," that may indicate a boot record problem). The solution is to boot from a bootable disc or USB flash drive to see if drive `C:` is available. When doing this, change the BIOS/UEFI boot order settings to boot to your removable media. The operating system may have to be reloaded. Also, verify that the primary partition is marked as active and that there is not nonbootable media such as a disc or USB flash drive inserted into or attached to the system. Check the first boot option setting in BIOS/UEFI and make sure it is set to the appropriate drive.

> If you receive a message such as "Hard drive not found," "No boot device available," "Fixed disk error," or "Disk boot failure," the BIOS/UEFI cannot find the hard drive. Check cabling. Place the drive in an external enclosure and attach it to a working computer.

> If a self-monitoring, analysis, and reporting technology (**S.M.A.R.T.**) error appears, back up data and research the error to take immediate action. S.M.A.R.T. is used to monitor both mechanical hard drives and SSDs. A S.M.A.R.T. error may appear immediately before a failure. Table 7.9 lists a few of the S.M.A.R.T. errors. Keep in mind that drive manufacturers may have their own errors as well.

TABLE 7.9 S.M.A.R.T. errors

Error	Description
Re-allocated sectors count	The number of sectors that were marked as bad, causing the data within those sectors to be moved
Spin retry	The number of times the drive was not up to speed in order to read and write from the drive
SATA downshift error count or runtime bad block count	The number of data blocks that contained uncorrectable errors
Reported uncorrectable errors	The number of uncorrectable errors detected
Reallocation event	How many times data had to be remapped
Soft read error rate or TA counter detected	The number of off-track errors

> When Windows has startup problems, use the WinRE and *Advanced Options* menu (press F8 on startup). With Windows devices, if the system boots too quickly to access this menu, hold down ⇧Shift while restarting the system. Then select *Troubleshoot* > *Advanced Options* > *Startup Repair* or *Command Prompt*. Startup problems are often due to a virus. Other utilities that help with MBR, boot sector, and system files are System File Checker (SFC) and the *Advanced Boot Options* menu. Use `bootrec /fixmbr` or `bootrec /fixboot` from WinRE.

TECH TIP

Using System File Checker

You can run the System File Checker program from the command prompt by typing `sfc /scannow`. The System File Checker should also be run after removing some viruses.

> When Windows has startup problems due to incompatible hardware/software or a corrupted installation process, the *Advanced Boot Options* menu can help.

> If an insufficient disk space error appears or if there is **sluggish performance** (that is, if the computer takes a long time to respond), delete unnecessary files, including `.tmp` files, from the hard drive, empty the Recycle Bin, and save files to an optical disc, a flash drive, or an external hard drive and remove the moved files from the hard drive. Use the Disk Cleanup and Defragmenter tool. Another option is to add another hard drive and move some (or all) data files to it.

> For eSATA drives, check the power cabling and data cabling. Ensure that the data cable is the correct type for the port and device being used. Partition and format the drive before data is written to it. Ensure that the port is enabled through BIOS. The BIOS/UEFI may require an update, or a device driver may be required (especially if the drive is listed under Other Devices in Device Manager). Note that some operating systems report SATA drives as SCSI drives.

> If the computer reports that the hard drive may have a defective area or if you start getting **read/write failure** notices, right-click on the hard drive volume > *Properties* > *Tools* tab > *Check*. The drive may need to be replaced soon.

- If drives fail frequently in a particular computer, check for heat problems, power fluctuations, vibrations, improper mounting screws or hardware that might cause vibrations, and environmental issues such as dust, heat, magnetic fields, smoke, and nearby motors. Consider using an SSD if the computer is in a harsh environment.
- If a USB drive is the boot device and the system will not boot, unplug the drive, reattach it, and restart the system.
- If a **spinning pinwheel**, ball, hourglass, or other application-specific icon appears; if a message that an application is not responding (sometimes asking you if you want to wait or kill the application) appears; or if a drive takes a long time to respond within an application, use the Disk Management tool to view the status of the drive. (Note that the Mac's colored spinning pinwheel is covered in Chapter 17.) Table 7.10 shows some of the normal and problem **drive status** messages that appear in the Windows Disk Management tool. These status messages can help with drive management, troubleshooting, and recovery.

TABLE 7.10 Disk Management status states

Status state	Description
Active	The bootable partition, usually on the first hard drive, is ready for use.
Dynamic	An alternative to the basic disk, the dynamic disk has volumes instead of partitions. Types of volumes include simple volumes, volumes that span more than one drive, and RAID volumes.
Failed	The basic disk or dynamic volume cannot be started, the disk or volume could be damaged, the file system could be corrupted, or there may be a problem with the underlying physical disk (turned on, cabled correctly) or with an associated RAID drive. Right-click the disk and select *Reactivate Disk*. Right-click the dynamic volume and select *Reactivate Volume*.
Foreign	A dynamic disk from another computer has just been installed. Right-click the disk and select *Import Foreign Disks*.
Healthy	The drive is ready to be used.
Not Initialized	A basic disk is not ready to be used. Right-click the disk and select *Initialize Disk*. The **Initialize Disk** option enables a disk so that data can be stored.
Invalid	The operating system cannot access the dynamic disk. Convert the disk to a basic disk (by right-clicking the disk number and selecting *Convert to Basic Disk*).
Offline	Ensure that the physical disk is turned on and cabled correctly. Right-click it and select *Reactivate Disk* or *Activate*.
Online (errors)	Use the hard drive Error Checking tool. In Windows Explorer/File Explorer, right-click the hard drive partition and then select *Properties*, the *Tools* tab, and *Check* button.
Unallocated	Space on a hard drive has not been partitioned or put into a volume.
Unknown	A new drive has not been initialized properly. Right-click the drive and select *Initialize Disk*. The volume boot sector may be corrupted or infected by a virus.
Unreadable	The drive has not had time to spin up. Restart the computer and rescan the disk (using the *Action* menu item).

RAID Issues

When you add RAID to a computer, you increase the complexity of the disk management. When two hard drives are configured in a RAID, they are seen and managed as one volume. Because of the different types of RAID and the number of hard drives involved in the RAID, a lot of problems could occur. Symptoms of RAID problems are similar to those that occur with a hard drive failure (read/write failure, RAID partition lost, slow system performance, loud clicking noise, failure to boot, drive not recognized, operating system not found, or a BSOD).

The following suggestions can help you with RAID configurations:

- If you have done RAID through the BIOS/UEFI, you cannot manage RAID through Windows (it is grayed out and shows as no fault tolerance). If you want to manage RAID through Windows, you have to break the RAID in BIOS/UEFI (that is, remove the RAID) and then re-create the RAID in Windows. Back up your data before doing this.
- Sometimes as part of the RAID configuration, you need driver media for the Windows installation or RAID failure troubleshooting process. Follow the motherboard or RAID adapter's manufacturing directions on how to create this media (usually via a USB drive or optical disc.
- If Windows doesn't allow you or give you the option to create a RAID array, check the BIOS/UEFI settings and ensure that AHCI has been enabled for the drives.
- If disk mirroring is not an option in Windows Disk Management, check your Windows version. You must have Windows Professional or a higher edition to create a RAID array.
- If Windows no longer boots, a BSOD appears, and the Windows boot drive is part of a RAID array, reinstall Windows if you want to keep the RAID array. You may have to get drivers before doing this. If you do not care about RAID and just want Windows to boot again, remove the hardware RAID. You can also use the BSOD code shown to research the error.
- If you have an **array missing**, check for a virus, S.M.A.R.T. errors, bad drive, or failed controller. Check to see if one of the drives in the RAID array has a partition table that was previously used in a non-RAID situation.
- If you receive a message such as "**RAID not found**," check the hardware or software configuration (depending on which type of RAID was configured). A power surge can corrupt a hardware RAID configuration done through BIOS/UEFI Setup. A system upgrade, application upgrade, or new application can affect software RAID.
- If you have a **RAID failure**, use the Windows Disk Management tool to check the status of the drives. Then check the RAID configuration if the drives are okay.

SSD Issues

The BIOS should recognize an internally installed SSD. If it does not, go into the system BIOS/UEFI Setup and ensure that the connector to which the SSD attaches is enabled. Be especially careful with SATA ports and port numbering. Configure the system to automatically detect the new drive, save the settings, and reboot the system. Here are some things to try, but remember that other hard drive tips still apply, such as those related to the computer not booting or the operating system not being found:

- Restart the PC.
- Try another SATA port or cable.
- Uninstall/reinstall the driver.
- Use cloning software from the SSD manufacturer or purchases from another vendor.
- Turn off the Wake on LAN BIOS option.

SOFT SKILLS: PHONE SKILLS

Technicians must frequently use the phone in the normal course of business to speak with customers, vendors, and technical support staff. A technician's job may involve communication via the telephone full time.

Phone communication skills are different from the skills needed for in-person communication because on the phone, you have only your words and voice intonation to convey concepts, professionalism, and technical assistance. When dealing with someone in person, you can use some of the following techniques that are not as effective in a phone conversation:

- Gesture to emphasize points.
- Draw a graphic to illustrate a concept.
- Perform steps needed for troubleshooting faster because you can do them rather than step someone through them.
- Show empathy more easily with your body language, actions, and voice.

When dealing with someone on the phone, the following pointers can help. Some of the tips apply to everyday technical support as well:

- Identify yourself clearly and pleasantly.
- Smile even though they cannot see you (see Figure 7.44). It will make a difference in your tone.

FIGURE 7.44 Telephone communication skills

- Avoid using a condescending tone.
- Be patient and speak slowly when giving directions.
- Use active listening skills (covered in Chapter 2, "Connectivity"); avoid doing other tasks when on a call with someone.
- Avoid using acronyms and technical jargon.
- Avoid being accusatory or threatening.
- If the customer is irate, try to calm them down and help them; however, if the customer continues to be belligerent, turn the call over to your supervisor.
- Escalate the problem if it is beyond your skill level; do not waste the customer's time.
- Do not leave people on hold for extended periods without checking back with them and updating them.
- Speak clearly and loudly enough to be heard easily.
- Avoid having a headset microphone pulled away so it is hard to hear you; if you are asked to repeat something, speak louder or adjust the microphone or handset.
- Avoid eating, drinking, or chewing gum when on the phone.

Good interpersonal skills are even more important when on the phone than with face-to-face interactions. Before getting on the phone, take a deep breath and check your attitude. Every customer deserves your best game, no matter what type of day you have had or what customer you have previously spoken to.

Chapter Summary

- Hard drive form factors include 5.25-, 3.5-, 2.5-, and 1.8-inch drives. Hard drives come in different speeds: 5,400, 7,200, 10,000, and 15,000 RPM. Faster RPM rates mean more expensive drives but also faster data transfers.
- Common drives today are SATA drives and SSDs for desktop and mobile computers.
- SATA drives can be internal or external and connect using a 7-pin internal connector that is a maximum of 3.3 feet (1 m) long, an external eSATA connector (3.3-foot [1 m] maximum for 1.5 Gb/s devices and 6.56-foot [2 m] maximum for 3 or 6 Gb/s devices), or an eSATAp combo eSATA/USB port. SATA 1 (also called SATA I) drives operate at a maximum of 1.5 Gb/s, SATA 2 (SATA II) drives at 3 Gb/s, and SATA 3 (SATA III) drives at 6 Gb/s. SATA internal drives use a unique SATA power connector. A Molex-to-SATA converter can be purchased, but 3.3V is not supplied to the drive; most drives do not use the 3.3V line. External drives use an external power source unless plugged into an eSATAp combo port, which can provide power.
- SSDs have become more common in desktops, laptops, and tablets. They are often used in harsh environments, dirty environments, heavy movement environments, and harsh temperature environments. They are extremely fast but expensive. They connect using SATA, mSATA, eSATA, M.2, PCIe, or USB connections.
- SSDs erase data in blocks instead of by marking available clusters in the FAT with traditional drives. SSDs should not be defragmented. SSDs use various technologies to ensure functionality, such as using all the memory evenly (wear leveling) and using reserved spare memory blocks.
- An SSHD is a combination of a mechanical hard drive and flash memory that holds the most frequently used data.
- Hard drives must be partitioned and have high-level formatting applied before they can be used to store data.

- Partitioning involves separating a drive into smaller sections (volumes) that can receive drive letters and can be done through the Windows installation process or by using the Disk Management tool.
- A simple volume is the most common type of partition volume created.
- To create a spanned volume (otherwise known as JBOD), space from two or more hard drives is seen as one drive letter. One drive is filled before any other hard drives are used.
- A striped volume writes data to two or more drives but does not provide redundancy.
- The system volume (usually `C:`) holds files needed to boot the operating system.
- The boot volume (usually `C:`) holds the majority of the operating system files.
- Computer manufacturers may use an HPA or a protected partition for system recovery.
- Multiple drives can be configured in a hardware or software RAID implementation. Hardware RAID is done using the BIOS/UEFI or a RAID adapter. Software RAID is done using the Windows Disk Management tool.
- RAID 0, or disk striping, does not provide fault tolerance, but it does provide fast, efficient use of two or more drives.
- RAID 1 is disk mirroring, and this method does provide fault tolerance by ensuring an exact copy of a drive in case one drive fails.
- RAID 5 is disk striping with parity, where parity data is kept on one of the three or more drives. This parity data can be used to rebuild one drive if one of the three or more drives fails.
- RAID 6 is similar to RAID 5 except that it has additional parity that can recover from two failed drives.
- RAID 10 is a mirrored set and a striped set combined with four hard drives at a minimum. This mode can read from the drive quickly but with slight degradation when writing.
- Windows Storage Spaces can use a variety of drive types to create a single storage space that can have RAID-like qualities.
- File systems in use are FAT16, FAT32, exFAT, NTFS, ReFS, APFS, and ext4. FAT32 and exFAT are used for external drives, such as flash drives. NTFS, which is used for internal drives, provides features such as better cluster management, security, compression, and encryption. ext3 and ext4 are used in Linux-based systems.
- Two ways of changing from one file system to another are by using the `convert` command and by formatting the drive. The `convert` command preserves existing data. High-level formatting does not preserve any saved data.
- If a drive fails to be recognized as a new installation, check cabling and BIOS/UEFI settings, especially for a disabled SATA port.
- Normal mechanical drive noises include a clicking when going into sleep mode or being powered down due to self-parking heads.
- Abnormal drive noises include a couple of clicks with a POST beep and/or error, repeated clicking noises, grinding noise, high-frequency vibration due to improper or poor mounting hardware, and a high-pitched whining sound.
- If a drive fails after operating for a while, check for a virus. See if the BIOS has a virus checker. Try a warm boot to see whether the drive has not spun up to speed yet. Check cabling, especially on SATA. Review any recent changes. Use the Windows Advanced Boot Options menu, Windows Recovery Environment (WinRE), System File Checker (SFC), and the `bootrec /fixmbr` and `bootrec /fixboot` commands. Boot from an alternate source and check Disk Management for status messages related to the hard drive.
- Hard drive space used as RAM is known as virtual memory. Ensure that enough free storage space is available.
- When speaking on the phone to anyone, be clear in your statements, don't use technical jargon, keep your tone professional, and do not do other tasks, including eating or drinking.

A+ CERTIFICATION EXAM TIPS

- ✓ Make sure you know characteristics about and can recognize SATA, eSATA, SSD (mSATA, PCIe, M.2, and NVMe), and SCSI (SAS).
- ✓ Be able to recommend a hard drive based on speed (5,400, 7,200, 10,000, and 15,000 RPM) or form factor (2.5-inch vs. 3.5-inch).
- ✓ Be able to recommend an SSD based on the interface used (NVMe, SATA, SAS, or PCIe) as well as form factor (M.2 or mSATA).
- ✓ Know the purposes of the Error Checking (Check Now/Check), Disk Cleanup, and Disk Defragmenter tools.
- ✓ Use a computer to review the disk tools and how to get to them.
- ✓ Review all the troubleshooting tips right before taking the exam.
- ✓ Be familiar with the following Disk Management concepts: understanding drive status and what to do if the status is not healthy, mounting, extending partitions, splitting partitions, assigning drive letters, adding drives, and adding arrays.
- ✓ Know what a normal hard drive sounds like and what sounds a hard drive in trouble makes. Ensure that you back up the data before a drive fails.
- ✓ Know the difference between RAID levels 0, 1, 5, 6, and 10.
- ✓ Know the various file systems, including exFAT, FAT32, NTFS, ReFS, APFS, and ext4.
- ✓ Know the difference between a quick format and a full format.
- ✓ Know the differences between basic and dynamic disks and understand primary, extended, and logical partitions and volumes.
- ✓ Be able to troubleshoot common symptoms such read/write failures, sluggish performance, grinding noise, clicking sounds, audible alarms, failure to boot, drive not found or recognized, missing drives in the operating system, RAID not found, array missing, and RAID not working.
- ✓ Know the difference between normal LED behavior for drive activity and unusual behavior. Know that some motherboards have LEDs that can help when troubleshooting drives.
- ✓ Be familiar with BSOD and spinning pinwheel proprietary crash screens.
- ✓ Know how and when to use Microsoft command-line tools such as `format`, `diskmgmt.msc`, `resmon.exe`, `cleanmgr.exe`, `dfrgui.exe`, `diskpart`, `SFC`, and `chkdsk`.
- ✓ Install a couple practice drives for the exam. Misconfigure the BIOS/UEFI and leave a cable unplugged or the drive power removed so you see the POST errors and symptoms.
- ✓ Know how and when to configure RAID and the differences between the various RAID levels.
- ✓ Be able to initialize a drive, convert a file system, convert a drive to a dynamic disk, create a simple volume, and select a particular file system.
- ✓ Know how to speak on the phone professionally.

Key Terms

2.5-inch drive, 3.5-inch drive, 5,400 RPM, 7,200 RPM, 10,000 RPM, 15,000 RPM, AHCI, APFS, array missing, audible alarm, basic disk, basic storage, boot partition, boot sector, boot volume, bootable device not found, `bootrec`, BSOD, `chkdsk`, clicking sound, cluster, `convert`, DBR, `defrag`, defragmentation, `dfrgui.exe`, disk cache, Disk Cleanup, Disk Management, disk mirroring, disk striping, `diskpart`, drive activity LED, drive array, drive not recognized, drive status, dynamic disk, dynamic storage, eSATA, exFAT, ext4, extended partition, extended read/write time, fail to boot, FAT (file system type), FAT (file allocation table), FAT32, file recovery software, file system, `format`, full format, GPT, grinding noise, head crash, high-level formatting, HPA, Initialize Disk, IOPS, JBOD, LED status indicator, logical drive, lost cluster, M.2, MBR, missing drive in the OS, mount, mSATA, MTBF, NAS drive, no OS found, NTFS, NVMe, partitioning, phone communication skills, primary partition, quick format, RAID, RAID 0, RAID 1, RAID 5, RAID 6, RAID 10, RAID failure, RAID not found, RAW volume, read/write failure, ReFS, SAS, SATA, SATA data cable, `sfc`, simple volume, sluggish performance, S.M.A.R.T., spanned volume, spinning pinwheel, SSD, SSHD, striped volume, System File Checker, system partition, system volume, volume, Windows Storage Spaces

Review Questions

Consider the following internal hard drive specifications when answering Questions 1–7:

- SATA 6 Gb/s transfer rate
- 1 TB capacity
- Minimizes noise to levels near the threshold of human hearing
- 3.5-inch 7,200 RPM
- 32 MB buffer size

1. Which SATA version is being used?

   [1 | 2 | 3 | Cannot be determined from the information given]

2. Which Windows file system should be placed on this drive if encryption will be used?

   [exFAT | FAT | FAT32 | NTFS]

3. Which drive preparation steps are *required* to be done if this drive is added as a new drive? (Choose all that apply.)

   [defragmentation | low-level format | high-level format | error checking | RAID | virus checking | partitioning | striping | duplexing]

4. This drive is meant to be quiet. List two noises that the drive could make that would indicate issues.

   _____

   _____

   _____

5. Is this drive internal or external? Explain your reasoning.

   [internal | external | cannot be determined]

   _____

   _____

6. What is this drive's form factor?

   [6 Gb/s | 1 TB | 3.5-inch | 7,200 RPM | 32 MB]

7. How many other devices could be on the same cable that connects this device to the motherboard?

   [0 | 1 | 2 | 3 | cannot be determined]

8. If only two drives are available, which RAID levels can be used? (Choose all that apply.)

   [0 | 1 | 5 | 10]

9. A technician has been called to help with a problem. A S.M.A.R.T. error appears, and the user reports that the system has been running slowly for several months. Which two tools or actions should the technician use immediately?

   [chkdsk | partition the drive | apply high-level formatting to the drive | `convert` | `diskpart` | back up the data | attach external drives and configure Storage Spaces]

10. What is the difference between spanning and striping?

    a. Spanning is done in hardware, and striping is done in software.

    b. Spanning is done within RAID, and striping is done in Windows or through BIOS/UEFI.

    c. Spanning takes two drives, and striping takes three drives.

    d. Spanning fills one drive before moving to the next drive, whereas striping alternates between the drives.

    e. Spanning is RAID 0, and striping is RAID 1.

11. A tile and carpet warehouse uses several computers for the inventory process. The computers in the warehouse area have a higher hard drive failure rate than those in the office area. Which solution will help this company?
    - **a.** Replace the hard drives with SSDs.
    - **b.** Place antistatic mats under the computers and on the floor where people stand or sit to use the computer.
    - **c.** Install more powerful power supplies.
    - **d.** Install additional CPU fans.
    - **e.** Replace the drives with higher-RPM drives.

A user wants to add an SSD to a computer. Consider the following SSD specifications for the drive being purchased and the user's motherboard documentation when answering Questions 12–16.

Specifications:

- 1 TB capacity
- PCIe 3.0 x4 interface
- M.2 2280

Motherboard documentation:

- 1 x M.2_1 socket 3 with M key, type 2242/2260/2280/22110 storage devices support (SATA and PCIe 3.0 x4 mode)
- 1 x M.2_2 socket 3 with M key type 2242/2260/2280/22110 storage devices support SATA and PCIe 4.0 x4 mode)

12. Is this drive internal or external? How can you tell?

    [internal | external]

13. Will the SSD be able to be installed in the computer based on the specifications given?

    [Yes | No | Cannot be determined from the information provided]

14. When considering the motherboard documentation, what do the numbers 2242/2260/2280/22110 mean?

    _____

15. What is a drawback of SSDs?

    [installation time | MTBF | maintenance requirements | cost | speed | reliability]

16. Would the SSD work in the M.2_2 socket?

    [Yes | No | Cannot be determined from the information given]

17. Which tool do most Windows users use to check for lost clusters?

    [Error Checking (Check/Check Now) | `diskpart` | Disk Defragmenter | Disk Cleanup]

18. How would a technician use the drive LED to troubleshoot a hard drive?

    _____

    _____

19. [T | F] If you have enough RAM installed, the hard drive will not be used as cache memory.

20. You are speaking on the phone to a customer who is upset. The customer curses and starts yelling. What should you do?
    - **a.** Hang up on the caller.
    - **b.** Ask the caller if you can put them on hold while they calm down.
    - **c.** Speak to the customer using a calm, professional tone.
    - **d.** Stay calm but raise your voice level a little to show the importance and professionalism of your technical response.

Exercises

Exercise 7.1 Planning Storage Device Installation and Configuration

Objective: To be able to use motherboard documentation to plan for various storage device scenarios.

Procedure: Refer to the following figure and answer the accompanying questions.

Questions: See Figure 7.45 to answer Questions 1–10.

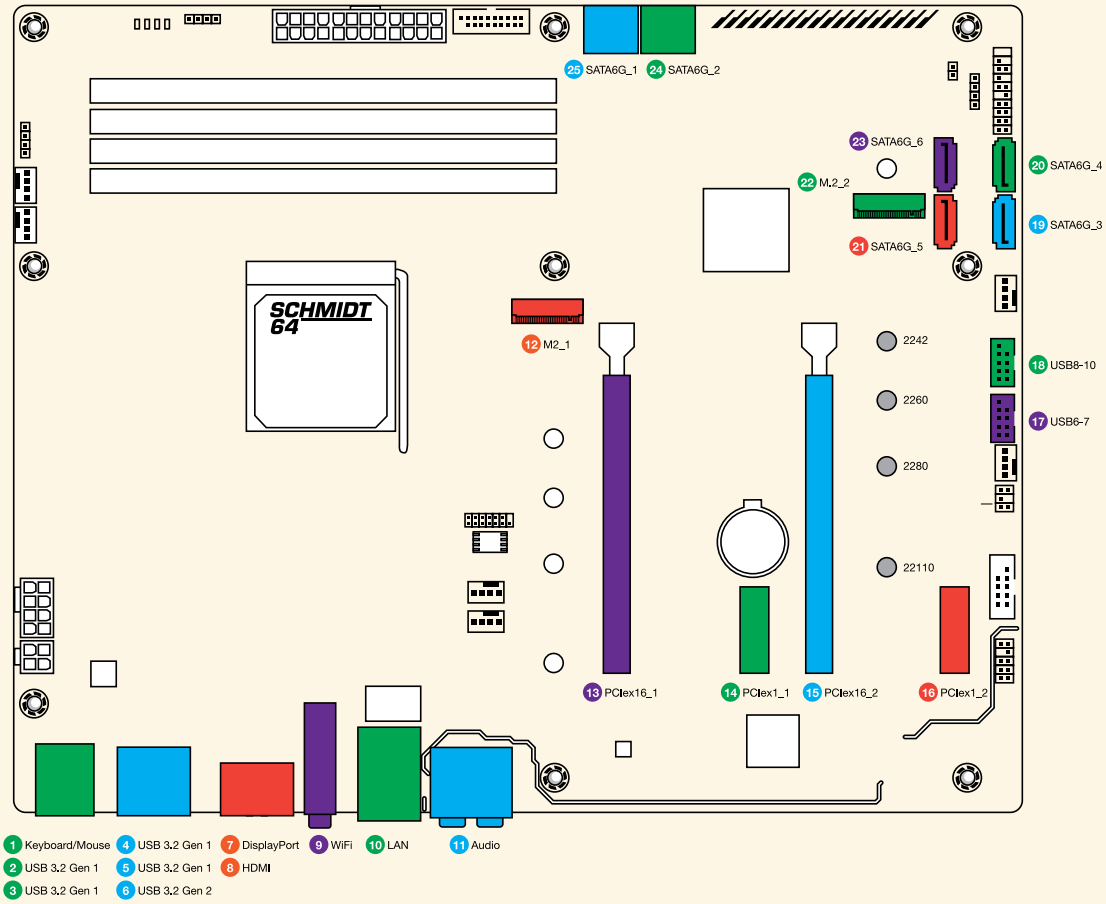


FIGURE 7.45 Exercise 7.1 documentation

1. A user has the motherboard shown and wants to install two internal hard drives. Using Figure 7.45, determine which ports should be used to connect the hard drives. (List two.)

   _____

   _____

2. Now the user wants to add a third drive, an internal SSD. List all ports that the user could use that have not been used already.

   _____

   _____

   _____

   _____

3. If the user is considering an external SSD and wants to use eSATA, how would the user cable up to this motherboard that does not have an eSATA port?

_____

_____

4. What is the significance of the 2242, 2260, 2280, and 22110 numbers on the motherboard?

_____

5. Could either of the M.2 slots be used for an internal mechanical hard drive?

   [Yes | No]

6. Could either of the M.2 slots be used for an internal SSD?

   [Yes | No]

7. If the motherboard documentation states that an NVMe SSD is supported, which ports/slots could be used?

_____

8. What is the maximum number of mechanical hard drives that could be installed using this motherboard? How did you determine the maximum number?

_____

9. Which external ports could be used for an external mechanical hard drive? List all that apply.

_____

10. Which external ports could be used for an external SSD? List all that apply.

_____

Exercise 7.2 Configuring a SATA Hard Drive on Paper

Objective: To be able to configure SATA hard drive jumpers

Parts: Internet access is needed for one question

Procedure: Refer to the following figures and answer the accompanying questions

Questions: See Figure 7.46 to answer Questions 1–3.

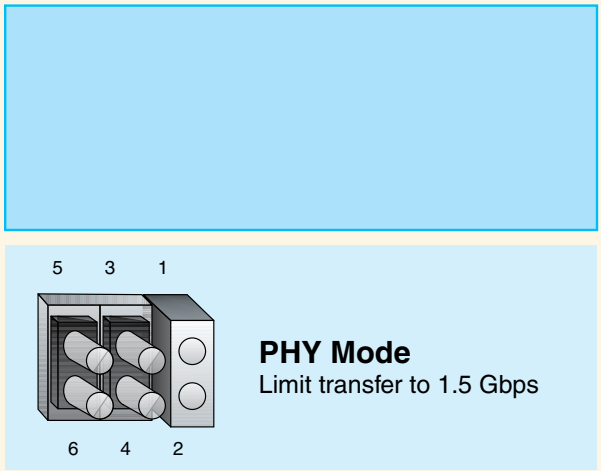


FIGURE 7.46 Exercise 7.2 documentation

1. Considering the information provided, when would you change the jumpers on this drive?

_____

_____

2. If the drive has pins 1 and 2 jumpered, what version of SATA is the drive using?

   [SATA 1 | SATA 2 | SATA 3]

3. If this hard drive were to be installed in a desktop model, what would the form factor of this drive most likely be?

   _____

4. Refer to Figure 7.47. The information provided is for a laptop computer used in a business environment. What do you think would be the effects of installing a jumper on pins 1 and 2 on this drive?

   _____

   _____

   _____

   _____

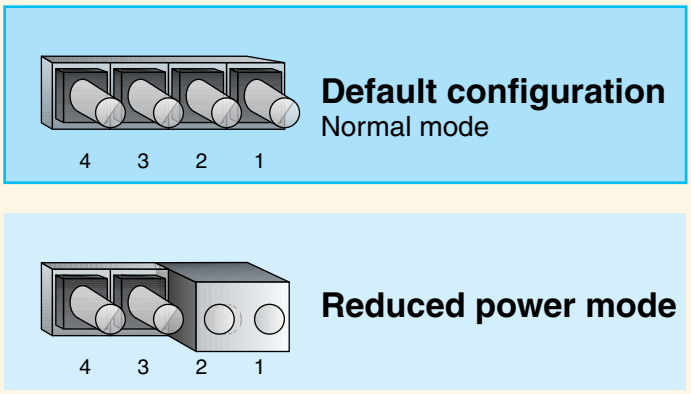


FIGURE 7.47 Exercise 7.2 documentation #2

5. Use the internet to determine SATA jumper settings for a particular vendor's replacement hard drive. Write the jumper settings and explanation for the jumpers. Write the URL where you found this information.

   _____

   _____

   _____

   _____

   _____

6. What is the form factor for the hard drive referenced in Question 5?

   _____

Activities

Internet Discovery

Objective: To use the internet to obtain specific information regarding a computer or its associated parts

Parts: Computer with internet access

Questions: Use the internet to answer the following questions. Write the answers and the URL of the site where you found information for each answer. In answering Questions 1–3, assume that you have just purchased a Seagate Barracuda 3 TB 7,200 RPM 6 Gb/s hard drive.

1. What types of cables are needed for this drive? Do they come with the drive? Write the answers and the URL where you found this information.

_____

_____

2. How much cache does this drive have?

_____

3. If the computer does not have an available SATA connector, what one recommendation could you make?

_____

_____

_____

4. A customer has a Western Digital WD Blue SN550 NVMe M.2 500 GB 3D NAND internal SSD. What is the minimum PCIe version needed to install this card? List the website where you found this answer.

   [1 | 2 | 3 | 4]

_____

5. Based on the same drive as in Question 4 and information you learned in this chapter, what slot size must the motherboard support in order to install this drive?

   [550 | 5502 | 2400 | 2280 | 22110]

6. Find an eSATA and an internal SATA hard drive that are equal or close to equal in capacity. What is the price difference between the two? Write the answer and the URL where you found this information.

_____

_____

Watch the *How to use all capacities of a new hard drive over 2TB?* DFI knowledgebase video, at https://us.dfi.com/knowledge/video/17, to answer Questions 7–10. (If this link does not work when you try to use it, find a video that shows how to install a GPT partition or search for this video at youtube.com.)

7. Which Windows tool was used to convert the partition to a GPT partition?
   [Task Manager | Disk Management | Device Manager | command prompt]

8. Even though the Disk 1 drive was originally unpartitioned, before the presenter did anything to the drive, the drive showed as having how many unallocated sections?

   [1 | 2 | 3]

9. If a drive has already been partitioned and has data on it, what must you do before converting the drive to a GPT disk?

_____

_____

10. List one comment that you found interesting and informative.

_____

Soft Skills

Objective: To enhance and fine-tune a technician's ability to listen, communicate in both written and oral forms, and support people who use computers in a professional manner

Activities:

1. In groups of two, pretend one of you has a hard drive problem. The other student should pretend to help the first student on the phone. Share your phone conversation with two other groups. Select the best group and scenario.
2. With two other classmates, come up with 10 additional tips for good phone support that were not listed in the chapter. Share your ideas with the class.

_____

_____

_____

_____

_____

_____

_____

3. As a team, plan the installation of three storage devices. The boot device will be a SATA SSD with a mechanical internal SSD used for data storage as well as an external USB mechanical drive. In your plan, detail what drives you are using for the plan, what things you will check for, how you will obtain the documentation, and what obstacles could appear as part of the installation process. The user also would like some type of redundancy. What choices might you present to the user? Share your plan with other teams.

Critical Thinking Skills

Objective: To analyze and evaluate information as well as apply learned information to new or different situations

Activities:

1. List three things that could cause a computer to lock up periodically that relate to the hard drive. What could you do to fix, check, or verify these three things?

_____

_____

_____

2. A customer wants to either upgrade or replace their hard drive. Go through the steps you would take from start to finish to accomplish this task.

_____

_____

_____

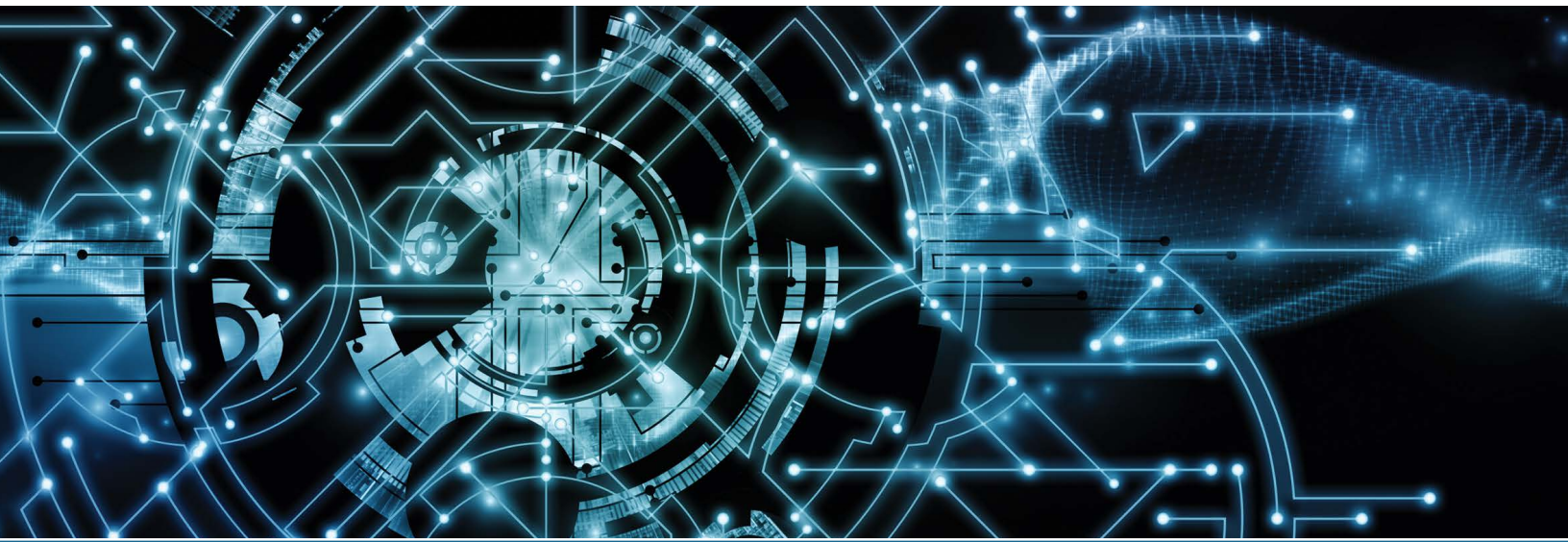
_____

3. Your team supports a department of 20 workstations. Some people store very important information on their local hard drives. Use the internet to research redundancy options as well as options presented in the chapter. Develop a list of possible redundancy plans for the department.

_____

_____

8 Video and Multimedia Devices



In this chapter you will learn:

- Basics steps needed to install, configure, and troubleshoot video cards, sound cards, and projectors
- How to install, configure, and troubleshoot optical drives and scanners
- How to use Windows to verify optical drives, sound cards, and scanners
- How to provide support with a positive, proactive attitude

CompTIA Exam Objectives:

- ✓ 1201-3.1 Compare and contrast display components and attributes.
- ✓ 1201-3.4 Compare and contrast storage devices.
- ✓ 1201-3.5 Given a scenario, install and configure motherboards, central processing units (CPUs), and add-on cards.
- ✓ 1201-5.2 Given a scenario, troubleshoot drive and RAID issues.
- ✓ 1201-5.3 Given a scenario, troubleshoot video, projector, and display issues.
- ✓ 1202-1.6 Given a scenario, configure Microsoft Windows settings.
- ✓ 1202-4.7 Given a scenario, use proper communication techniques and professionalism.

Multimedia Devices Overview

The term *multimedia* has multiple meanings because there are many types of multimedia devices. This chapter focuses on the most popular areas: displays, optical drive technologies, projectors, sound cards, scanners, cameras, and speakers. These devices collectively enable you to create and output sound, music, video, and movies. This chapter is not intended to be a buyer's guide for multimedia devices or an electronics "how it works" chapter; instead, it is a guide for technicians with an emphasis on installation and troubleshooting.

Video Overview

Video is an integral part of a computer system, and it is also part of multimedia production. Video is important to users, and many situations require different video specifications. Technicians must look at video as a subsystem that consists of the display, the electronic circuits that send the display instructions, and the cable that connects them. Figure 8.1 illustrates a computer video subsystem.

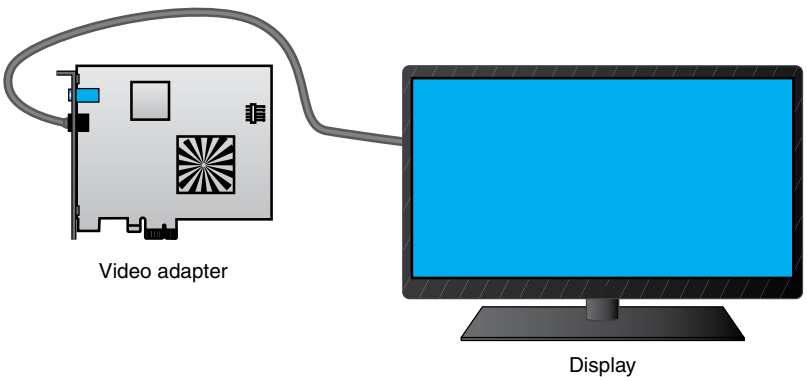


FIGURE 8.1 Video subsystem

Video Displays

The monitor/display unit is a very important part of a computer system and can use a variety of technologies, as described in Table 8.1.

TABLE 8.1 Video display technology

Technology	Description
Liquid crystal display (**LCD**)	A technology used in laptops, flat panel monitors, TVs, tablets, smartphones, and projectors in which a backlight—which can be a cold cathode fluorescent lamp (CCFL) or LED technology—extends behind the combined glass assembly, and the light is always on. This is why an LCD monitor appears to sometimes glow even when it's off and why crystals are needed to block some of the light to create the intensities of light.
Light-emitting diode (**LED** or **mini-LED**)	A low-power, low-heat, long-lasting electronic device used in many technologies, including displays. LED displays use liquid crystals as well as an LED backlight instead of a CCFL. LED displays have better color accuracy than LCDs, are thinner than the LCDs that use CCFLs, and are commonly used for large displays.
Organic LED (**OLED**)	A technology that does not require a backlight, like LCDs, but has a film of organic compounds placed in rows and columns that can emit light. OLED displays are lightweight and have fast response time, low power usage, and a wide viewing angle. Displays are used in TVs, mobile phones, and handheld game consoles.

LCDs use liquid crystals embedded into the display materials (see Figure 8.2) to create the images once the CCFL or backlight illuminates them. Liquid crystals are sensitive to temperature changes, so mobile device displays may appear distorted in cold or hot temperatures.

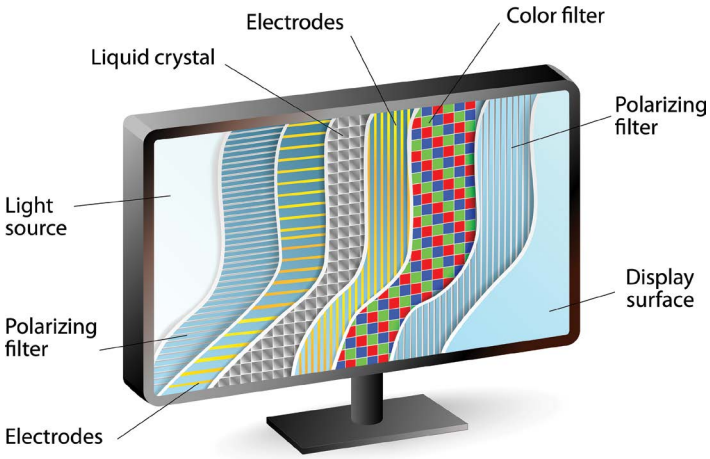


FIGURE 8.2 Inside an LCD

There are three main types of LCDs:

> **Twisted nematic (TN):** This is the cheapest type of LCD to make and the type that is most commonly used. It is the fastest to display an image, but it is best viewed from straight on rather than at an angle.

> **Vertical alignment (VA):** This type of LCD has the slowest response time but better color and wider viewing angles than TN LCDs.

> **In-plane switching (IPS):** This is the best type of LCD for viewing from an angle, and it offers the best quality and color, but it has slow response time. This type of LCD is good for graphic designers and other professionals who need consistent color reproduction.

TECH TIP

Liquid crystals are poisonous

Be careful with cracked LCDs. If liquid crystals (which are not actually liquid) get on you, wash with soap and water and seek medical attention.

Besides deciding which type of display technology to use in a monitor, technicians should also be familiar with the display attributes described in Table 8.2.

TABLE 8.2 Display attributes/features

Display attribute	Description
Pixel density (or pixels per inch [ppi], pixels per centimeter [ppcm], or dots per inch [dpi])	The higher the number, the better the display quality. Directly related to the density and seen frequently in display ads is **pixel pitch**, which is a measure of the distance from the center of one pixel to the center of the pixel next to it (in millimeters). A smaller pixel pitch means there are more pixels (less space between them) and better quality.
Refresh rate	A value shown in hertz (Hz) that describes how many times a screen is redrawn in one second. With a higher refresh rate, motion appears smoother and motion blur is minimized.

Display attribute	Description
Screen resolution	The number of pixels on the screen, such as 1,920×1,080 (which means there are 1,920 pixels in each row of pixels and there are 1,080 rows of pixels).
Color gamut or color space	The number of colors a display can handle. Standards include sRGB (standard red, green blue), Adobe RGP, and DCI-P3. sRGB is fine for normal usage. Adobe RGB has a higher color gamut and is needed in design-oriented fields. DCI-P3 is used by gamers and video editing professionals.

Touch Screens

Touch screen displays, which are used with PCs, tablets, and smartphones, respond to contact on the screen rather than (or in addition to) keyboard or mouse input. A touch screen may be integrated into a device or may be a display that attaches to a USB-C, VGA, DVI, or HDMI port; a combination of these ports; or wirelessly (on a desktop model). Special drivers and software are used to control a touch screen monitor.

Several technologies are used to manufacture touch screen displays. Two common ones are resistive and capacitive. Resistive touch screens rely on pressure to detect touch, whereas capacitive touch screens use electrostatic properties of the human body. A resistive touch screen has a flexible membrane stretched over the face of the display. These displays are used in environments where personnel wear gloves, such as manufacturing and the medical industry.

Capacitive touch screens are more durable than resistive screens. They respond to a touch or multiple touches on the display and easily detect contact. Most touch screens are the capacitive type. Some devices allow you to calibrate the screen or lock the screen orientation by using the Windows *Settings > Display* option or software from the display manufacturer. Figure 8.3 shows a touch screen.

FIGURE 8.3 Touch screen display

Video Cards

Using millions of colors, motion, sound, and video combined, computer video subsystems have made dramatic technological advances. Video can be built into the motherboard (an **integrated graphics card**), in which case the video port uses motherboard RAM. Alternatively, an integrated graphics processing unit (**iGPU**) can be on a video card. A **video card** (also known as a video adapter or dedicated graphics card) controls most of the display output. Video cards are commonly

installed into PCIe expansion slots and are more powerful than integrated motherboard video ports. A video card has its own processor called a **discrete GPU** (dGPU) and its own RAM mounted on the card, so it can provide better performance than an integrated graphics card.

A PCIe video card may require either a 6- or 8-pin connector from the power supply. A 6-pin cable can provide an additional 75W of power, whereas an 8-pin cable can provide an additional 150W. A PCIe video card may require multiple power cables. Figure 8.4 shows a video card and its power cable.

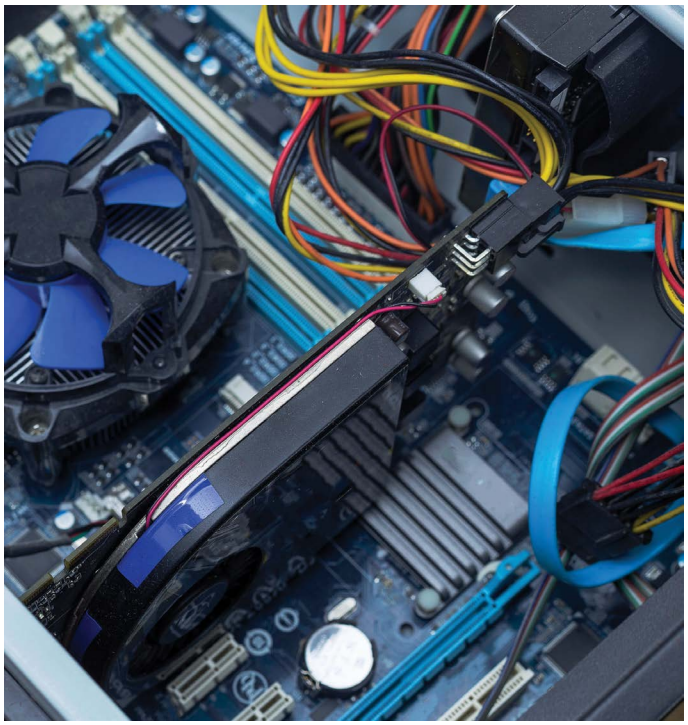


FIGURE 8.4 Video card power connector

With a video card, graphics are processed on the adapter rather than within the motherboard CPU. Figure 8.5 shows a video adapter with a video processor (covered by the fan). GPUs commonly have fans and/or heat sinks attached.

FIGURE 8.5 Video card with a GPU

TECH TIP

You might need a video card with an AMD processor

Be careful when buying or replacing AMD processors as some of the processor descriptions say "requires discrete graphics card." This means the system will not work without a video card installed. The processor does not have graphics capability and cannot send video signals to integrated motherboard video ports. Look for a G in the AMD model number if you want a processor that has an IGP.

A special type of PCIe or external device you might see is a **video capture card** that allows video to be taken from a video source such as a camera, game console (such as an Xbox or a PlayStation), TV channel, or video recorder and saved, put into a presentation or archive file, or streamed onto the internet or a home network. Teachers might use a video capture card to record or stream a lesson. Not all video capture cards support audio. You can buy video capture cards and devices that have specific input connectors, such as component video, S-video, or HDMI, and an output connector, such as USB or HDMI. Figure 8.6 shows an external video capture device.

FIGURE 8.6 Video capture device

Video Memory

One of the most important functions of a video processor is to transfer data to and from a video adapter's memory. Memory on a video adapter can be just like motherboard modules, including DDR4, DDR5, and DDR6, as well as specialized video graphics double data rate (GDDR) modules.

Video RAM is RAM that is used for video exclusively. When this RAM is insufficient, motherboard RAM is used. When motherboard RAM is being used in addition to video card RAM, the amount of motherboard RAM being used is known as **shared system memory**, or shared video

memory. You see this when you examine the video display properties. Some systems allow customization through system BIOS/UEFI or a special control panel provided by the video adapter manufacturer. Common system BIOS/UEFI options for controlling shared system memory include AGP Aperture Size and Onboard Video Memory Size. Figure 8.7 shows the properties of a video card that has 2 GB of RAM installed (listed next to Dedicated GPU Memory). The shared GPU memory amount is how much motherboard RAM is allowed to be used by the video card (and the operating system and the applications).

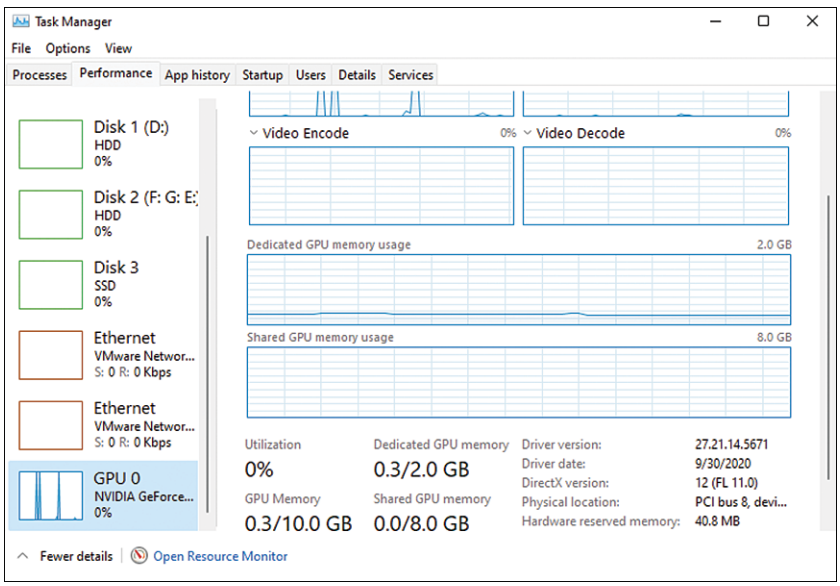


FIGURE 8.7 Shared system memory for video

TECH TIP

Checking how much video memory you have

The `dxdiag` command can be used to examine video properties. Otherwise, for Windows 10/11, use *Settings* > *System* > *Display* > *Advanced Display Settings* link > *Display Adapter Properties* > *Adapter* tab.

Installing a Video Adapter

Before installing a video adapter, do your homework:

- Make sure you have the correct interface type and an available motherboard slot. PCIe is the most common, but AGP can still be found.
- Gather tools, if needed. Use an antistatic strap or grounding techniques. You may need a screwdriver to remove the slot-retaining bracket and to re-insert the screw that holds the adapter.
- Download the latest drivers for the video adapter from the manufacturer. Make sure the adapter has a driver for the operating system you are using.
- Ensure that the power supply can supply enough power when the adapter is added. Some high-end video adapters require a PCIe 6- or 8-pin or AGP Molex power connector. Some PCIe cards can use a power cable adapter that converts two Molex power connectors to the PCIe power connector. Other video cards can receive adequate power (up to 75W) through the PCIe expansion slot.

TECH TIP

Installing a new video adapter

When you install a new video adapter, if it does not work, disable the onboard video port by accessing the system BIOS/UEFI settings.

Before installing an adapter, power off the computer and unplug it. Use an antistatic wrist strap or antistatic gloves. Remove any previously installed video adapters (if performing an upgrade). Locate the expansion slot.

Sometimes with a tower computer, it is best to lay the computer on its side to insert the video adapter properly. Line up the video adapter's metal connectors with the interface slot. Push the adapter into the expansion slot. Make sure sections of the adapter's gold connectors are not showing and that the card is not skewed. Connect the display to the video connector. Power on the display and computer. Figure 8.8 shows a video adapter being installed.

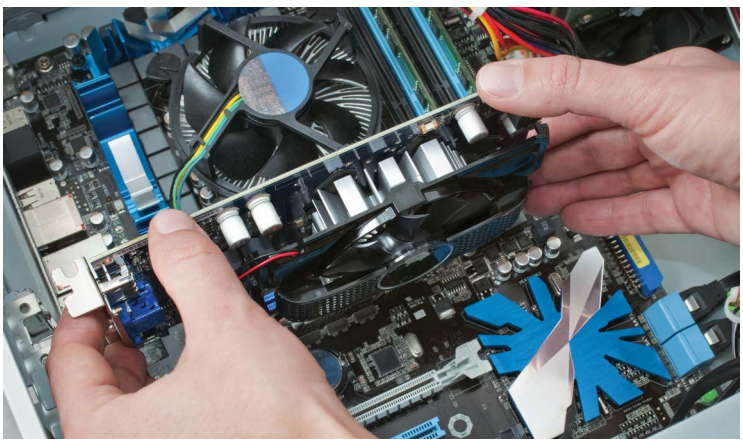


FIGURE 8.8 Video card installation

A video card has a set of drivers or software to enable the adapter to work to its full potential. Individual software drivers from the manufacturer provide system compatibility and performance boosts. A technician obtains current video drivers from adapter manufacturers' websites. Be sure to use the proper video driver for the operating system.

Troubleshooting Video

When troubleshooting a video problem, check simple solutions first. Verify that the display power light is on. If it is not, check the power cable connectors, surge strip, and wall outlet. Verify that the brightness and contrast settings have not been changed. Check or disable power-saving features while you're troubleshooting. Double-check the monitor cable connected to the video port. Use the built-in diagnostics that some displays have. Ask the user if any new or upgraded software or hardware has recently been installed, including an operating system automatic update.

TECH TIP

Keep in mind the video system

If a piece of video hardware is defective, then it is the display, adapter, motherboard port, or cable. If replacement is necessary, always attempt the easiest solution first.

Many video problems involve a software driver or improperly configured settings. Anything that is problematic on the display can be a result of a bad video driver, an incompatible driver, an incorrect driver, or an incompatible system BIOS/UEFI version. The best way to be sure is to download the exact driver for the monitor and the display adapter/port from the internet or obtain it from the manufacturer. Some troubleshooting tips related to video follow. Remember that these are only suggestions. Research the manufacturer of the display, motherboard, or video adapter for specific instructions on troubleshooting the equipment.

Common video problems include the following:

> **Physical cabling issues** that include the cable not pushed fully into the connector or bent/broken video pins can cause a flickering or **flashing screen**, horizontal or vertical lines, **incorrect colors**, **fuzzy images**, and/or **distorted images**. Use needle-nose pliers to straighten bent pins. If the video cable is okay, try resetting the display to the factory default settings and/or resetting the refresh rate. There may also be a bad monitor or card/port.

> If you suspect a video driver problem, expand the *Display Adapters* section of *Device Manager*. Locate the video card and look for any visual indications of problems. Right-click the video adapter > *Properties* > *General* tab and check the Device Status section to see if it indicates that the device is working properly. Check for a video driver update.

> For video problems in Windows, hold down [⇧Shift] while restarting and select the *Enable Low-Resolution Video* option to see if the problem is resolved and determine whether it is a software driver problem.

> For **sizing issues** such as oversized/undersized words/icons, check the Windows *Display* setting > *Resolution* or *Text size*.

> A **dead pixel** is a pixel that does not light up on an LCD screen. Dead pixels are usually present on LCDs—even new ones. LCD panels with dead pixels can still be used, but if there are too many of them, replace the display. Note that LCDs can also have bright spots when pixels are permanently stuck in the on position.

> If a display doesn't seem to look correct, set the display to the native resolution (that is, the resolution for which the display was made).

TECH TIP

What to do if a display goes black, red, dim, or pink

Check cabling. The backlight bulb might be faulty. Try swapping monitors.

> If a cursor appears momentarily before the computer boots and then nothing is displayed or a distorted display appears, check for a video driver problem.

> It is possible that a computer may start normally without allowing you to see the Windows startup screen. Sometimes a **dim image** seems to be evident or no image is displayed, but you can hear the hard drive. In such a case, ensure that the display has power, reset the display to the factory defaults, and try adjusting the brightness and contrast. If these steps do not help, the **inverter** (the component that converts DC to AC for the backlight) most likely needs to be replaced.

TECH TIP

What to do if the display is dark

If you have a **blank screen**, check to see whether the computer is in sleep mode or won't come out of sleep mode. Check the video cable. Hold down the power button and try restarting. Check the power management settings.

> If video is problematic while working in Windows, use the *Safe Mode*, *Last Known Good Configuration*, or *Enable Low-Resolution Video* option and then load the correct driver. You can also use the *Driver Rollback* option if a new driver has just been installed.

> If audio cannot be heard through the display, check cabling, ensure that the correct sound output device is selected, and check the volume controls and muting.

> If a blue screen of death (BSOD) appears, log any error message or code that appears (see Figure 8.9) and try rebooting the computer. Do not take a hammer to it. Researching the error is a much more productive way of repairing the computer. You can also boot to Safe Mode or low-resolution video mode and reload a video driver from there.

FIGURE 8.9 BSOD

TECH TIP

No image on the screen?

Check the following: Is the video card inserted fully into the slot? Are the cables properly attached? Is the adapter supported by the motherboard? Is the auxiliary power attached to the adapter? Is sufficient power coming from the power supply? Is the driver properly installed? Check the surge strip and move it to another power outlet.

> **Display burn-in** occurs when an LCD or plasma display has been left on and unchanged for too long, and the display shows an image imprint or a ghost image. In such a case, try turning off the display for a few hours. If that does not work, create an all-white image in a graphics program and use it as the screen saver. Turn the display brightness to low and leave the monitor on for a few hours.

TECH TIP

See or smell smoke or sparks?

Disconnect the display, if possible, from the power source. Use an appropriate fire extinguisher as necessary. If at work, report the incident.

- Any monitor that won't come out of power saver mode might need the video driver or BIOS/UEFI firmware updated.
- If a computer is on for a while and then the display has issues, check for overheating in the computer and/or the video adapter. Check for adequate power output from the power supply.
- An artifact is something that appears on your screen that should not appear, such as green dotted or vertical lines, colored lines on one side of the screen, tiny glitters, or an unusual pattern. Check for an overheating GPU, insufficient airflow, or a problematic video driver.
- If you are having an issue using multiple monitors and Windows does not show the *Multiple Displays* option, then Windows does not recognize the second monitor. Check *Device Manager* for possible driver issues. Check cabling. Check the adapter. Note that not all adapters work with one another, so there may be a conflict between two adapters. If an adapter and a motherboard port are used, the computer may not support this configuration.

TECH TIP

Display disposal rules

Many states and local regulations mandate that specific disposal procedures be followed for monitors and other electronic waste.

Digitizer or Touch Screen Replacement

If there are issues with unresponsive tapping or swiping or if applications randomly open on a touch screen, digitizer (covered later in this chapter) issues might be the culprit. Always try restarting the device or powering off and back on before doing anything else. If the device was dropped or jarred, the cable that connects the digitizer to the mainboard might be loose or disconnected. Dirt, dust, particles, scratches, cracks (which might allow particles down between the digitizer and the LCD), and so on might cause issues. If you have to replace the digitizer, follow the manufacturer's directions. You might need some double-sided foam tape to keep the digitizer from touching the LCD screen, which would cause it to stop working.

If the touch screen is a separate assembly, remove the retaining screws and lean the screen backward so that the screen doesn't fall forward when all screws are removed. The screen may have to be pried from the outside casing, using a metal or plastic prying tool that has a small flat edge. Gently lean the screen forward and notice the cable/connector that connects to the screen. There may be a retaining bar and/or tape or a tab on the connector.

Figure 8.10 shows a touch screen that has just been removed from a laptop. One cable is the video cable that goes to the motherboard. The other cables connect to the Wi-Fi/Bluetooth and cellular cards.

After a touch screen is replaced, use Device Manager to verify that it is recognized by the operating system. Expand the *Human Interface Devices* (HID) section and make sure the device and driver are shown. Ensure that the digitizer cable or cables are attached. A touch screen has multiple configurations that can be controlled, including how swiping is controlled, and after replacing a touch screen, you might need to calibrate it. In Windows, search for the word calibrate and select *Calibrate Display Color*.

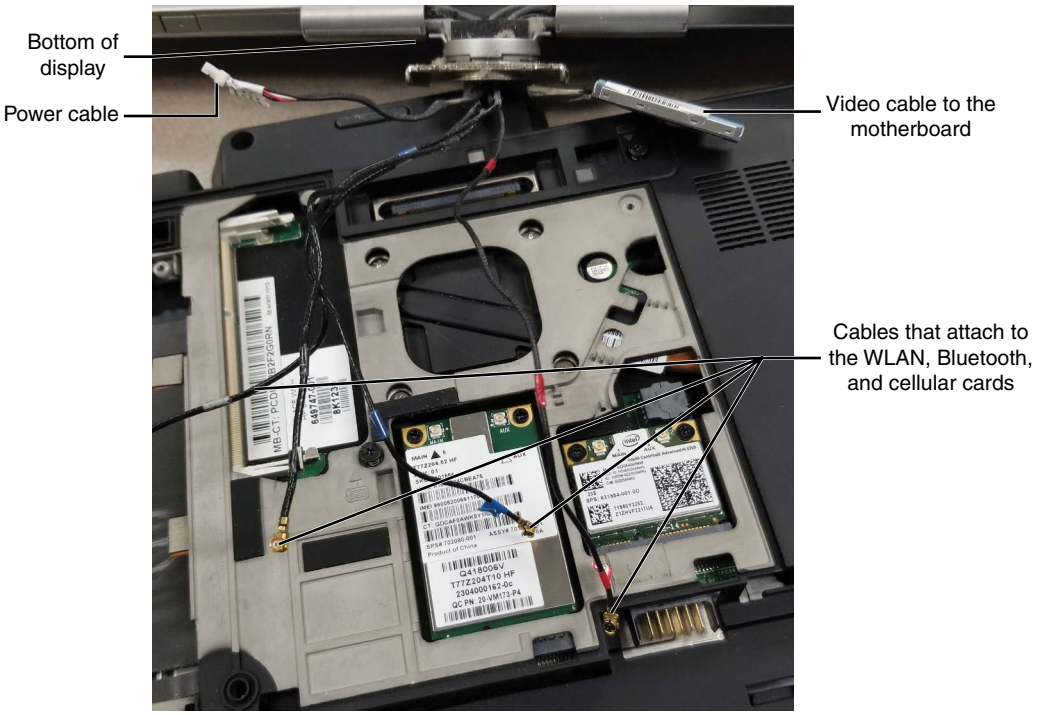


FIGURE 8.10 Removing a touch screen

Projectors

Projectors have become common devices, and technicians must be familiar with them. A projector allows information displayed on a computer, laptop, camera, or other device to be projected onto a larger screen. A projector has connections similar to those described for video cards. Cables that convert between the different formats are available. Figure 8.11 shows some of the connectors available on a projector. A projector sometimes connects to other audio and video devices besides computers, such as a document camera, speakers, optical disc players, and smart boards. The VGA in and out ports are two ports commonly seen on a projector for connecting video. S-video is also quite common. Newer projectors might also have a DisplayPort and/or USB-C port.

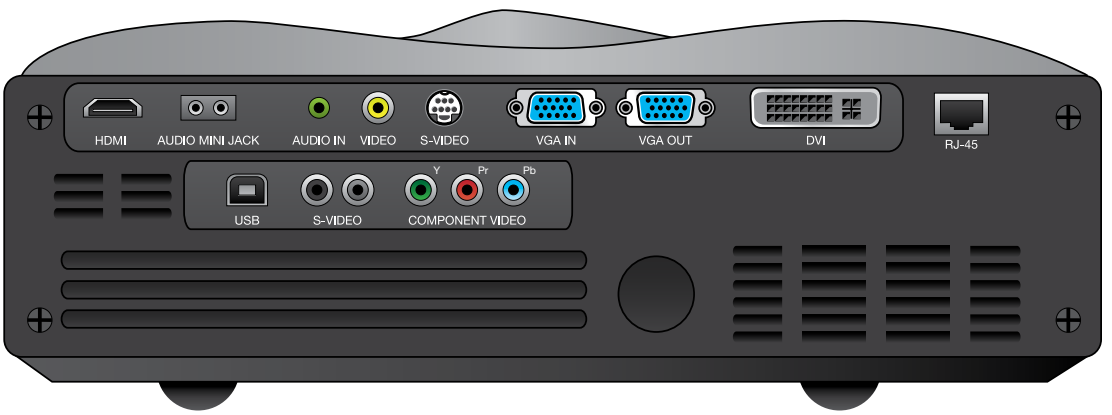


FIGURE 8.11 Projector ports

When looking at a video card, you expect to see VGA, DVI, and/or HDMI ports. The same is true with ports often seen on TVs, gaming consoles, optical disc players, stereos, and projectors. Composite video is normally a yellow port (like the one labeled VIDEO in Figure 8.11). The audio RCA ports are normally red and white. **Component/RGB video** analog ports are normally

colored red, green, and blue and have the symbols Y, Pr, and Pb above them. (Y is for the luminescence, or brightness, and Pr and Pb are for the color difference signals.) An RJ45 connector connects a projector to an Ethernet network. Some projectors also have wireless network capabilities.

To connect a projector to a PC and a monitor, you need a video distribution (sharing) device, two video ports from a PC, or a video port splitting cable/device. A laptop typically has a video port available for connecting an external monitor or a projector.

Table 8.3 lists key features to look for in a professional projector.

TABLE 8.3 Projector features

Projector feature	Comments
Brightness or luminance	How much light a monitor or projector can produce. Two factors affect brightness: how much light the projector outputs and the reflective properties of the screen being used. Some projectors have optimization, so you can't base comparisons on just lumen ratings.
Lumens	A measure of light output or brightness—how much visible light is coming out of equipment, such as lamps, lighting equipment, or projectors. This measure is important when comparing products for a room that has lots of exposure to sunlight, for example.
Resolution	The number of pixels on the screen, such as 1,920×1,080 (which means there are 1,920 pixels in each row of pixels and there are 1,080 rows of pixels). The more pixels, the higher the resolution.
Wired Ethernet capability	The ability for a projector to be connected through an RJ45 port to a wired Ethernet network.
Wireless	The ability for a projector to be connected and monitored through an 802.11 wireless network.
Remote control or desk controller	The ability to control a projector through either a remote control or a control panel mounted near a computer in the room.

Projector Maintenance

Treat your projector well. Do not immediately unplug the power to a projector after a presentation; instead, allow the projector to cool down first. You can turn off the projector, but the fan still runs on some models to quickly cool the projector. Keep the filter clean to extend the life of the projector bulb. Keep a spare bulb in stock.

Projector Troubleshooting

Troubleshooting projectors can sometimes be tricky because they might be connected through a control console, they might be mounted in the ceiling (where verifying the cabling may not be easy), and the projector may have many possible inputs. Review the "Video Troubleshooting" section, earlier in this chapter, which contains many tips that may apply to sending video through a projector. Also consider these troubleshooting tips:

> Verify the input source. An **incorrect data source** is a common issue because a projector might connect through a control console or directly through a cable or wirelessly. Use the remote or projector buttons (see Figure 8.12) to cycle through the inputs. Also check for tightened cables, if possible.

FIGURE 8.12 Selecting the input source on a projector

> If a projector is showing nothing, check to see if it is powered on. If it has recently been turned on and then off, you may have to wait a few minutes to be able to turn it back on again. This is normal behavior. Check for a **burnt-out bulb**. If the projector has power and the correct data source is chosen, then a burnt-out bulb is a likely culprit.

> If the projector has **audio issues** such as not playing sound, check the sound on the computer and ensure that the volume is not muted or set low. Use the *Sound* setting in Windows. Verify the input source and check the projector mute setting using the projector remote. Adjust the projector's volume settings. Verify the audio settings in the projector software, if applicable. If this is the first time sound has played through the projector, cabling could be an issue.

> If you see a dim image, you might have to adjust the projector brightness/contrast, clean a dirty lens, or replace a failing lamp.

> For presentation software, the *Display* setting may need to have the *Duplicate the Display* option selected so that the output can be seen on the screen. Ensure that the projector light shows (that is, that the bulb is good). If flickering occurs, check cabling.

> If you have **intermittent projector shutdowns** or the projector shuts off unexpectedly, check to make sure the power cord is securely attached or that there are batteries, if they are used for power. If the projector has gone into standby mode due to inactivity, press the projector power button to wake the projector. If the projector has been used for an extended period of time, it must have time to cool before it is turned back on. Check status indicators, if possible, for an indication of a particular overheating fault. If this occurs and the projector has not been on long, clean and/or replace the air filter.

Introduction to Audio

Video and sound technologies are important today. No multimedia chapter would be complete without mentioning sound. Sound is important to the end user, but sound is also important to a technician in many instances, such as when a computer does not boot. A motherboard might have a small integrated speaker or a speaker that attaches to motherboard pins that allows POST sounds to be heard even if the more advanced sound system is not working. Figure 8.13 shows a motherboard speaker.

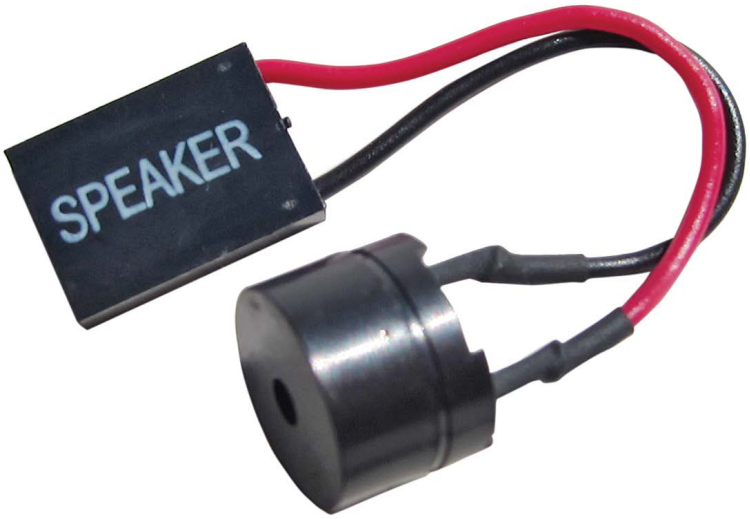


FIGURE 8.13 Motherboard speaker

On a motherboard, ports for speakers and headphones are typically 1/8-inch (3.5 mm) connectors that accept TRS (tip ring sleeve) connectors. Figure 8.14 shows common motherboard sound ports.

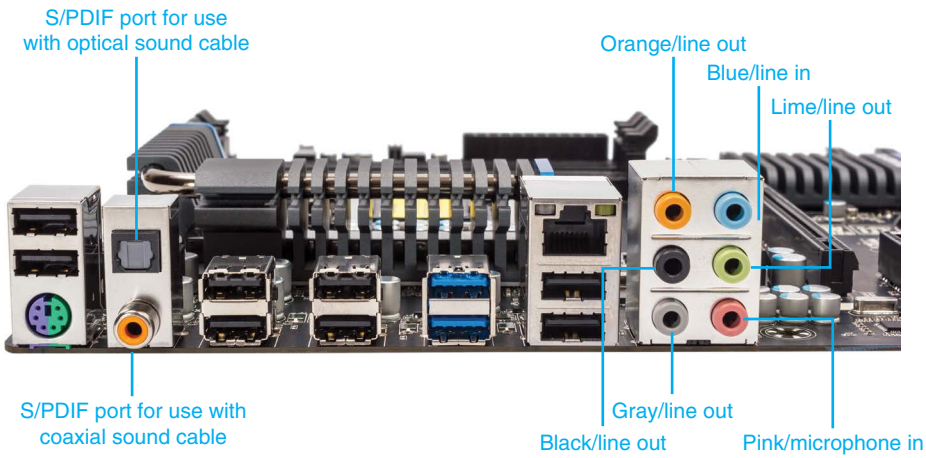


FIGURE 8.14 Motherboard audio ports

Notice in Figure 8.14 the Sony/Philips Digital Interface Format (S/PDIF) port. S/PDIF is a type of sound port that can be used to carry digital audio signals between audio devices and stereo components or the output of an optical disk drive (ODD) in a PC to a home theater or some other external output device. S/PDIF ports can attach using an RCA jack attached to coaxial cable or a TOSLINK connector attached to a fiber-optic cable.

A TV or display might have a special HDMI ARC (audio return channel) port that allows the sound to be sent to a soundbar, speakers, or receiver. Connect an HDMI 1.4 or higher cable between the HDMI ARC port and the soundbar.

Optical drives have the capability to produce sound, usually through a front headphone jack and through a connection to sound through the motherboard or an installed sound adapter. Audio discs can be played on these drives, but the audio does not sound as good through the drive's headphone jack as it does through a stereo system or speakers. Figure 8.15 shows how an audio device connects to a **sound card**. Table 8.4 shows the colors that are normally used for sound ports.

FIGURE 8.15 Audio ports on an adapter and an audio cable

TABLE 8.4 Sound port colors

Color	Purpose
Orange/gold	Center speaker or subwoofer
Black	Rear speaker
Light blue	Line in
Lime green	Line out/front channel speakers
Pink	Microphone
Gray	Side speaker

Theory of Sound Card Operation

Sound cards can include a variety of options, such as an input from a microphone, an output to a speaker, and the ability to generate music (for example, bringing sound into the computer through a microphone connected to a sound card).

Computers work with digital signals (1s and 0s), so a sound card must convert an analog signal to a digital format to send the sound into a computer. Sound cards can also take the digital data from a computer and output the sound to speakers. To convert an analog waveform to 1s and 0s, samples of the data are taken. The more samples taken, the truer the reproduction of the original signal.

The sound card frequency response is dependent on the sample rate (also known as sample frequency). For a good reproduction of sound, the sound wave is sampled at twice the range desired. The frequency response for a music CD is 44,100 samples per second—a good-quality sound reproduction for human ears. DVDs require a 48 kHz or 96 kHz sampling rate for audio output.

Installing Sound Cards

The steps involved in installing a sound card are similar to the steps involved in installing any other adapter. Refer to the manufacturer's instructions when installing devices and adapters. The basic steps are as follows:

Step 1. Power off the computer, remove the computer case and power cord, and locate an empty expansion slot (making sure it is the appropriate type of slot).

Step 2. Attach the appropriate cables.

Step 3. Attach external devices, such as speakers. Attach power to the external devices as necessary. Figure 8.16 shows typical sound card ports and the types of devices that might connect to these ports.

Step 4. Power on the computer. Windows should detect that new hardware has been installed.

Step 5. Load the appropriate device drivers for the sound card.

After a sound card is installed, there are normally other programs and utilities from the sound card manufacturer that you can install.

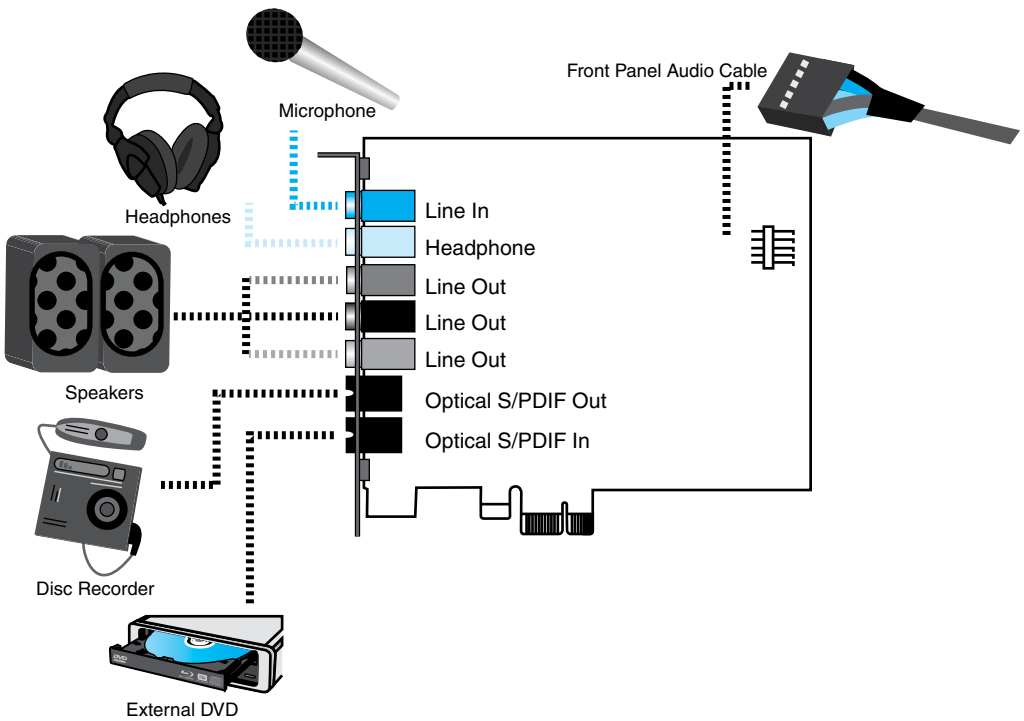


FIGURE 8.16 Sound card port connectivity

TECH TIP

Disabling motherboard sound when installing an adapter

If you install a sound card into a computer that has sound built into the motherboard, you should disable the onboard sound before installing the new adapter.

Sound Cards Using Windows

With Windows, the *Sound* setting is used to change sound and adjust multimedia settings. Most people control volume through a notification area volume control icon located in the lower-right portion of the screen.

TECH TIP

Check for muting

If sound is not coming from a computer, look for an x over the sound icon located in the notification area and ensure that the volume is not muted.

You can tell whether a device has integrated sound or a sound adapter installed by inspecting the *Sound, video and game controllers* category in Device Manager. Figure 8.17 shows a screen capture of Device Manager from a computer that has integrated sound on the motherboard. Note that integrated sound may be located in the *System devices* category or the *Other devices* category.

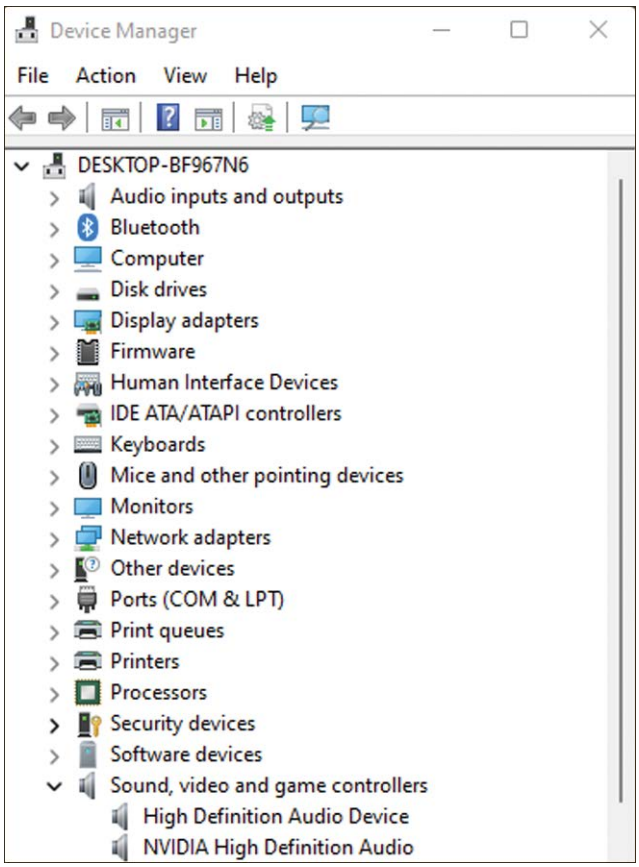


FIGURE 8.17 Integrated sound in Device Manager

Microphones are commonly used for conference calls. A microphone can be attached to a headset or a separate device, integrated into the computer display, or integrated into the device (as with mobile devices). To see microphone settings on a Windows device, use the *Settings* > *Sound* option. Figure 8.18 shows the Windows choices that appear when you click on the down arrow by *Input* in the *Sound* section.

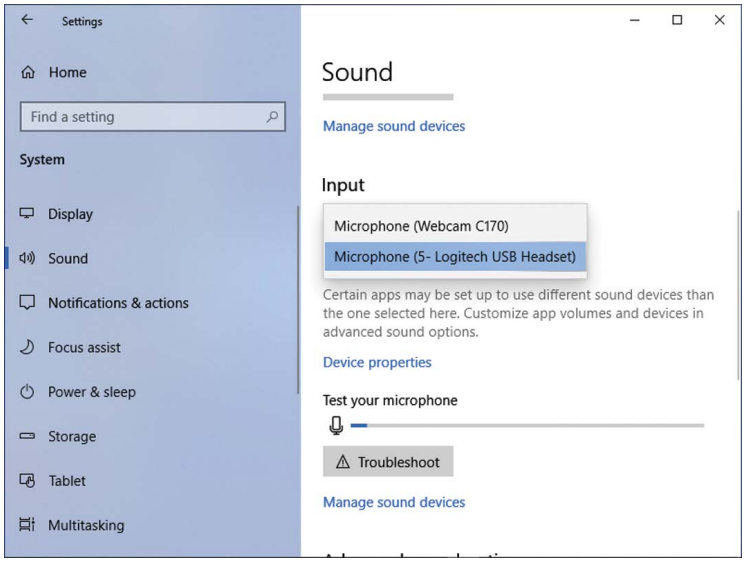


FIGURE 8.18 Choosing a microphone in Windows

Speakers

Most people connect speakers to a sound card or an integrated sound port. Others use a headset, as shown in Figure 8.19. The quality of sound is personal; sounds that are acceptable to one person are not always acceptable to others. Table 8.5 shows some features to look for in speakers.

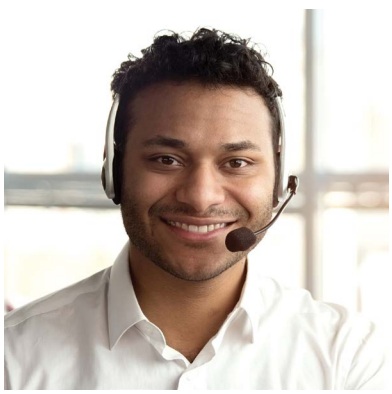


FIGURE 8.19 Sound quality is personal

TABLE 8.5 Speaker features

Feature	Description
Amplification	Increases the strength of the sound. Sound cards usually have built-in amplification to drive speakers. Amplification output is measured in watts, and most sound cards provide up to 4W of amplification (which is not enough for full-bodied sound). Many speakers have built-in amplifiers to boost the audio signal for a much fuller sound.
Power rating	Indicates how loud the volume can go without distorting the sound. Power rating is expressed in watts per channel. Look for the root-mean-square (RMS) power rating; 10W to 15W per channel is an adequate rating for most computer users.

Feature	Description
Frequency response range	Indicates the range of frequency (sounds) that a speaker can reproduce. Humans can hear from 20 Hz to 20 kHz, and the range varies for each person. Therefore, whether a computer speaker is appropriate depends on the person listening to the speaker. Speaker quality is subjective. Room acoustics and speaker placement also affect sound quality.
Shielding	Cancels out magnetic interference and keeps magnetic interference away from other devices. A speaker may have a magnet inside it that can cause distortion to a device such as a monitor. Such a magnet can also cause damage to disks and other storage media. The best optical drive and sound card combination can be downgraded by using inexpensive, poorly shielded speakers.

Most computer systems come with internal or external speakers. The external speakers could be battery or AC powered, which might not be desired. One speaker commonly connects to the sound card port, and the other speaker is usually daisy-chained to the first speaker. A speaker may have an external volume control. Be mindful of this as it is another thing to check for when sound does not work. Figure 8.20 shows computer speakers that are USB powered and connect to the sound port (green cable into green port).

FIGURE 8.20 USB speakers

TECH TIP

How to choose speakers

Listen to them without headphones, using an audio disc.

Troubleshooting Sound Problems

The best place to start troubleshooting sound problems is to check the easy potential problems first. Here are some basics to start with:

- Are the speakers plugged into the correct port on the sound card?
- Is the volume control muted? If it is, take it off mute.
- Is the volume control on the speakers turned up?
- From within Windows, check whether the device appears to be playing without sound being heard. In this case, the problem is definitely in the sound system.
- Do the speakers have power?

The following is a list of common sound problems and solutions:

- If a speaker is emitting unwanted sounds, make sure there are no empty adapter slots in the computer. Move the speakers farther away from the computer. If the speakers produce a humming noise and are AC powered, move the speaker power cord to a different wall outlet.
- If the sound card is not working, check Device Manager to see whether the sound card is listed twice. If there are two entries for the same sound card, remove both of them by clicking each entry and clicking the *Remove* button. Restart Windows.
- In Windows, if you do not see a sound icon on the screen, access *Settings* > *System* > *Notifications & Actions* > *Select Which Icons Appear on the Taskbar* link > locate the *Volume* icon > select *On*.
- If the computer emits no sound, use the Windows audio troubleshooter. Search the Windows Control Panel by typing `sound troubleshooting`.
- If the audio volume is low no matter what sound is played (see Figure 8.21), the speakers may not be amplified, or they may not be connected to the correct sound card port.

FIGURE 8.21 Low or no sound

Optical Drive Overview

Compact disc (CD), digital versatile disc or digital video disc (DVD), and Blu-ray disc (BD) drives are collectively called **optical drives**, or optical disk drives (ODDs), because they use optical discs that are read from, written to, or both. Optical discs are used when creating or playing music CDs or movie DVDs and also for backing up data. CDs are the older technology, but they are still in use today in combination with DVD and BD technologies. BDs tend to be used for movies and video games. Drives can be obtained that can handle CD, DVD, and BD media. Figure 8.22 shows a BenQ CD drive and its various front panel controls.

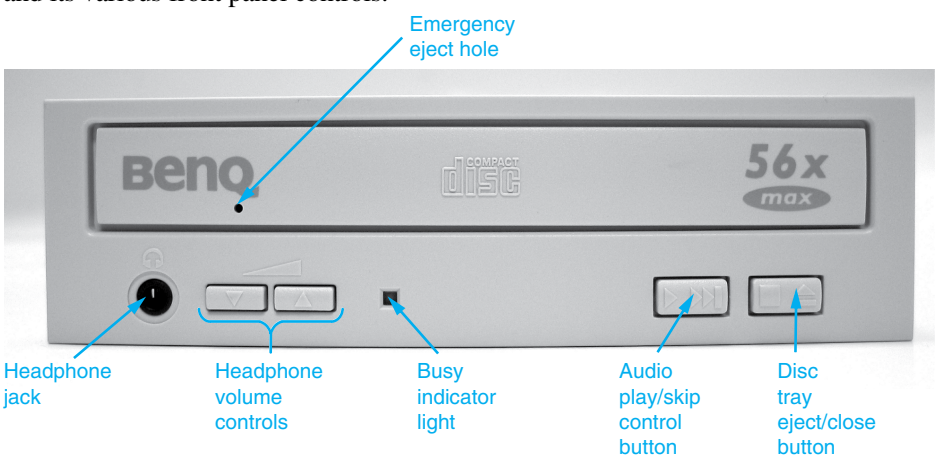


FIGURE 8.22 BenQ CD drive front panel controls

A CD has pits or indentations along the track. Flats, sometimes called lands, separate the pits. Reading information from a CD involves shining a light through the protective coating to an aluminum alloy layer, where data is stored. The laser beam reflects back through the optics to a photo diode detector that converts the reflected beam of light into 1s and 0s. CD and DVD drives use red laser technology, and Blu-ray drives use blue-violet laser technology, where smaller data pit sizes can be used to create higher disc capacities.

TECH TIP

Some optical drives cannot read Blu-ray discs

Some optical drives cannot read Blu-ray discs because CD/DVD drives use a red laser, and Blu-ray drives use a blue-violet laser. Drives that have both lasers are available.

Optical Drive Features

Optical drives that have an "R" designation can read only from a disk. Drives that have an "RW" or "RE" designation can perform both reads and writes. Drives with a "DL" designation use dual-layer technology, which means two physical layers are available on the same side of the disc. Table 8.6 lists common media types.

TABLE 8.6 Optical writable media

Media type	Capacity
CD	650 or 700 MB
CD-RW	650 or 700 MB
DVD-5/RW	4.7 GB single-sided single layer
DVD-9/RW (DVD-9DL)	8.5 GB single-sided dual-layer
DVD-10/RW	9.4 GB double-sided single-layer
DVD-18/RW (DVD-18DL)	17.1 GB double-sided dual-layer
BD/BD-RE	25 GB single-layer
BD DL/BD-RE DL	50 GB dual-layer
BD XL	100 or 128 GB multi-layer
Mini BD	7.8 GB single-layer
Mini BD DL	15.6 GB dual-layer

Optical drives come in a variety of types, classified by an x factor: 1x (single-speed), 2x (double-speed), 32x, 48x, 52x, and higher. Optical drives do not operate at just a single speed, though; the speed varies depending on the type of media being read and whether writing is being done.

TECH TIP

How to read the numbers

ODDs are frequently shown with three consecutive factor numbers, such as 52x32x52. The first number is the write speed, the second number the read/write speed, and the third number is the maximum read speed that is used when reading a disc.

Both DVD and BD drives have **region codes**. The world is divided into six regions for DVD drives and three regions for BD drives. The drive must be set for the correct region code, or the optical disc made for that area will not work. Some drives allow the region code to be changed a specific number of times. Table 8.7 shows the region codes for DVD and Blu-ray drives.

TABLE 8.7 DVD and Blu-ray region codes

DVD region code	Geographic area	Blu-ray region code	Geographic area
1	United States and Canada	A	North/Central/South America, Southeast Asia, Taiwan, Hong Kong, Macau, and Korea
2	Europe, Near East, Japan, and South Africa	B	Europe, Africa, Southwest Asia, Australia, and New Zealand
3	Southeast Asia	C	Central/South remaining Asian countries, China, and Russia
4	Australia, Middle America, and South America		
5	Africa, Asia, and Eastern Europe		
6	China		

Many drive features or capabilities can be determined by looking at the symbols on the front of the drive, as shown in Figure 8.23.

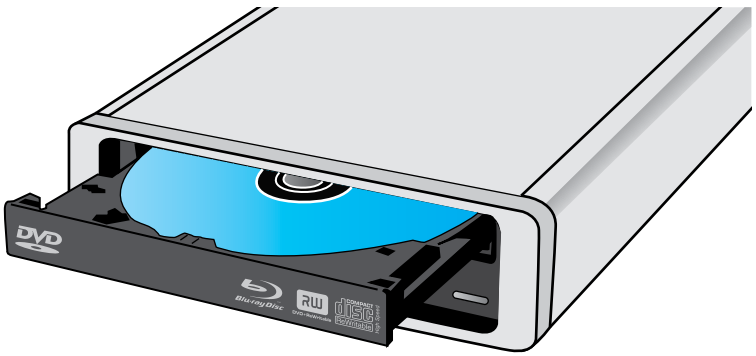


FIGURE 8.23 Optical drive symbols

TECH TIP

Using an ISO file

An ISO file/image is commonly used when installing an operating system. If you need to download and install software or an OS, then you can download the ISO image, right-click on the filename in File Explorer, and select *Burn disc image*. ISO images can also be used to boot an OS.

Optical Drive Interfaces and Connections

An optical drive can be internally mounted and attached to a SATA interface, or the drive can be externally attached to a USB, eSATA, or eSATAp (combo SATA/USB) port. The SATA interface is the most common for internal devices, and USB is most common for external devices.

Optical Drive Installation

One thing to be concerned about with an optical drive is whether the drive is to be installed horizontally or vertically. Not all drives can be installed vertically.

The steps for installing an internal optical drive are almost identical to the steps for installing a hard drive:

Step 1. Download the latest drivers before installation.

Step 2. Install any necessary mounting brackets.

Step 3. Ensure that a proper port/interface is available. Ensure that a power connector is available. Refer to the drive documentation.

Step 4. Turn off the power. Remove power cords.

Step 5. Install the drive.

Step 6. Attach the power and data cables.

Step 7. Enter BIOS/UEFI to check the drive status. Ensure that the port is enabled. Ensure that the drive is recognized.

Step 8. If necessary, install drivers and/or software as part of the installation process.

TECH TIP

Always test an installation

Test an installation by using the device to play something or write to a disc that you bring along. Ensure that the customer tries the disc and is comfortable with the changes caused by the installation.

Troubleshooting Optical Drive Issues

Windows has troubleshooting tools in the Help and Support Center. Search for the word `troubleshoot` in the search textbox.

TECH TIP

Checking the easy stuff first

Verify that the correct type of optical disc is in the drive, is inserted correctly (label side up), and is not dirty or damaged. Test the disc in another drive. Verify that the ODD has a drive letter. Check Device Manager for errors.

The following is a list of problems, along with possible solutions and recommendations:

> If a drive tray cannot be opened, make sure there is power. Use File Explorer to locate the drive, right-click the drive, and select *Eject*. A drive may have an emergency eject button or a hole you can insert a paper clip into to eject the disc. Refer back to Figure 8.22 to see an example of the eject hole.

> If a drive is not recognized by the operating system, check cables, the power cord, and the port enabled in BIOS/UEFI.

> If you hear **grinding noises** or **clicking sounds**, make sure the disc is aligned in the holder.

> If a drive cannot read a disc, ensure that the drive supports the disc being used and that the disc label faces up. Ensure that the disc is clean and free of scratches. Try the disc in another machine or try a different disc to see if the problem is with the drive or the disc.
> If a DVD soundtrack works, but video is missing or distorted, check the cabling. Verify the video drivers. Try changing the display resolution and the number of colors.
> If a message appears about an illegal DVD or BD region error or region code error, change the region, if possible. You can't use the disc unless you use a drive that matches.

TECH TIP

Seeing video but hearing no audio

If you can see video but can't hear audio or vice versa, check the cabling and verify that the computer meets the hardware and software requirements for DVD playback. Update the driver.

> Some optical drive problems are resolved by using DirectX. **DirectX** allows people who write software to not have to write code to access specific hardware directly. Access the DirectX Diagnostic Tool in Windows by entering `dxdiag` in the Search dialog box.

Preventive Maintenance for ODDs and Discs

CDs and DVDs have a protective coating that helps protect them. Fingerprints, dust, and dirt can still negatively affect the performance of CDs and DVDs. BDs are less likely to need preventive maintenance than other optical formats.

TECH TIP

Handling discs with care

Always handle a disc by the edges; never touch a disc's surface. Store discs in sleeves or cases in a cool location.

When reading information, the optical drive laser beam ignores the protective coating and shines through to the data layer. If dust or dirt completely blocks the laser beam, the laser beam could be reflected or distorted, causing distortion or data corruption. Special cleaning discs, cloths, and kits are available for cleaning optical discs. A soft lint-free cloth and water or glass cleaner works, too.

TECH TIP

Cleaning discs

When using a cleaning cloth to clean a disc, wipe the disc from the inside (near the center hole) to the outside of the disc (not in a circular motion) on the side of the disc that holds data.

The laser lens is responsible for reading information from discs. If the laser lens gets dust, dirt, or moisture on it, the drive may report data or read errors. Use a laser lens cleaning kit or use an air blower like ones used on a camera lens.

Scanners

A scanner is an input device that allows documents including text and pictures to be brought into a computer and displayed, printed, emailed, written to an optical disc, and so on. A scanner is

commonly built into a multifunction device (MFD) such as a printer, scanner, copier, and/or fax machine. These are also called all-in-one (AIO) devices. The most common types of scanners are listed in Table 8.8. Figure 8.24 shows a flatbed scanner, and Figure 8.25 shows how it works.

TABLE 8.8 Types of scanners

Scanner type	Comments
Flatbed scanner (sometimes called desktop scanner)	Can scan books, paper, photographs, and so on; can take up desk space.
ADF (automatic document feeder) or sheet feeder feature	Enables a document to be fed through an automatic document feeder similar to a fax machine; good for scanning multiple-page documents.
Handheld scanner	Slowly moves across the document; the user must have patience and a steady hand; portable unit.
Barcode scanner	A handheld device that reads a code displayed as a series of vertical lines or a quick response (QR) code that is a square and has embedded information such as a website within the displayed pattern.

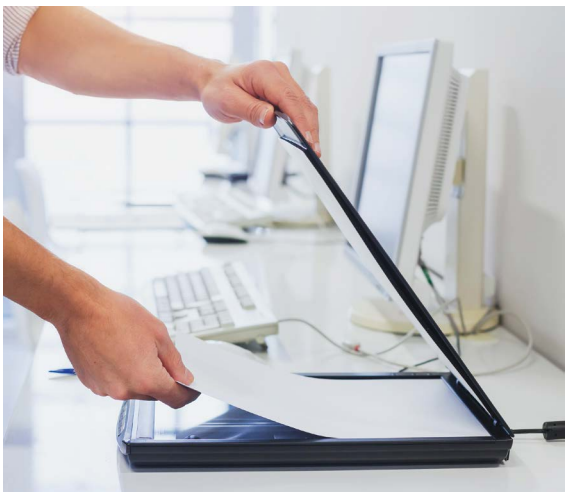


FIGURE 8.24 Flatbed scanner

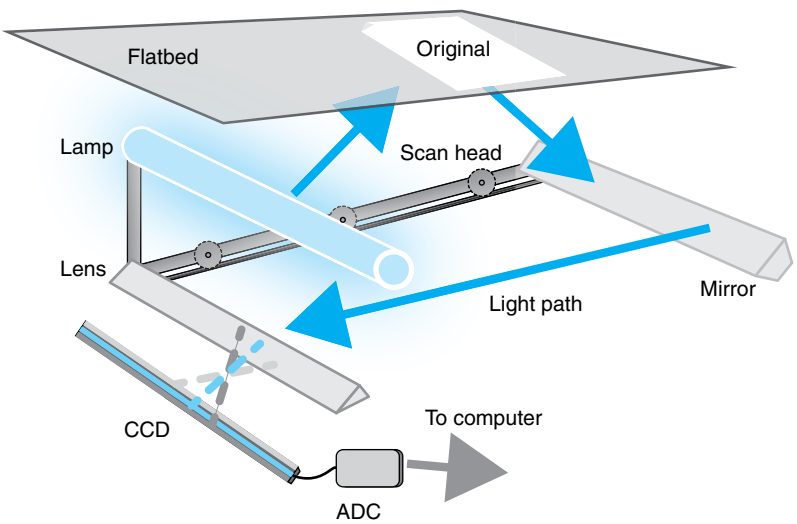


FIGURE 8.25 How a flatbed scanner works

A scanner normally attaches to a computer using one of the following options:

> USB
> RJ45 Ethernet
> Wireless

To install a USB scanner, always follow the manufacturer's directions. The following steps are generic:

Step 1. Install software and drivers.

Step 2. Unpackage and unlock or remove special packaging.

Step 3. Connect the data or network cable as well as the power cable.

Step 4. Power on the scanner. Some scanners have a calibration process that needs to be performed. There may be a special switch or push button that locks/unlocks the scan head.

Step 5. Configure options and default settings.

Step 6. Scan a document to test it.

Step 7. Ensure that the customer is trained and has all scanner documentation.

A scanner's plate glass needs to be cleaned periodically (see Figure 8.26). To test whether cleaning has been successful, scan a full page without a document loaded onto the scanner. See if the results yield any smudges or streaks. Consider these best practices:

> The best cleaning method is to put optical surface cleaning fluid on an antistatic cleaning cloth and then wipe the glass.
> Never spray cleaner directly on the glass.
> Do not use rough paper towels.
> A commercial glass cleaner or water can be used.
> Always remove all cleaner residue from the glass.
> Do not press down on the glass.
> Do not use an abrasive or corrosive solvent.
> Keep the glass dust free.

TECH TIP

Protecting scanner glass

Be careful with sharp objects such as staples around a scanner. A scratched or damaged glass surface results in marks on all scanned images.

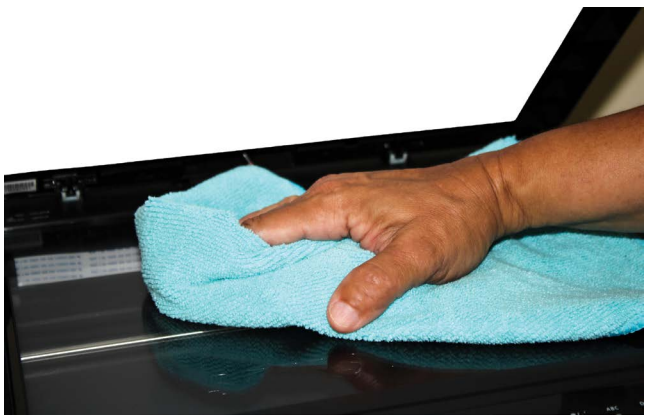


FIGURE 8.26 Scanner glass cleaning

Other Multimedia Devices

There are many multimedia devices today, and almost everything can connect to a computer. Audio and video recording capabilities can be built into a computer, can be attached to a computer, or can be standalone devices. Two multimedia devices that are common in some trades are webcams and digitizers.

Webcams

A **webcam**—short for web camera—is a digital camera that attaches or is integrated into a display or PC for use in transmitting live video or recording video. Web cameras can also be integrated into VoIP phones. A webcam may have a small visor or sliding window that can cover the lens to prevent video. Figure 8.27 shows a wired webcam, but keep in mind that webcams can connect wirelessly or can be integrated into displays or mobile devices.

FIGURE 8.27 Webcam

To access and control an integrated camera in a flat panel display, you normally use the Control Panel or software that comes with the camera, such as the Logitech Webcam Software shown in Figure 8.28. If you ever get a "Bandwidth exceeded" message when a camera is being used, try reducing the camera's resolution in whatever software is being used.

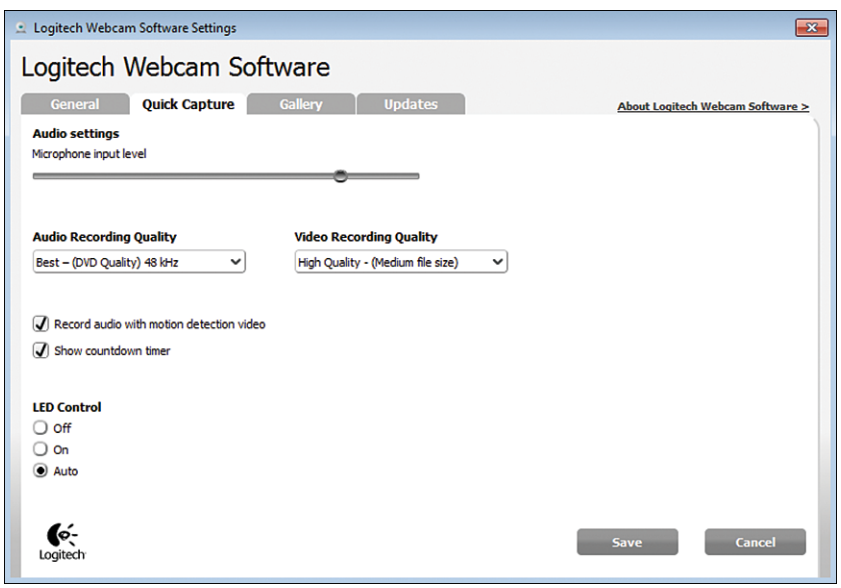


FIGURE 8.28 Logitech Webcam Software controls

Regardless of whether multimedia devices are integrated into a computer or connect to a computer, all devices attach and install similarly. When installing a new device for a customer, don't forget to allow the customer to test the device while you are still there. Also, remember to leave all documentation related to the installation with the customer. The customer paid for the device and is entitled to the documentation.

Digitizers

A **digitizer** (see Figure 8.29) provides input into documents such as architectural drawings, technical plans, and photos. It can also be used to draw electronic pictures. An instructor may use a digitizer to annotate a presentation or document.

FIGURE 8.29 Digitizer

A digitizer comes with a pen that may or may not need a battery. Some pens have replaceable ends. Digitizers either connect through a wired USB connection or can be wireless. A digitizer tablet comes with software that commonly allows the pen and digitizer tablet buttons to be customized in terms of what a button does and the speed at which a button reacts. Some digitizers come with diagnostics as part of the software.

SOFT SKILLS: ATTITUDE

A technician's **attitude** (see Figure 8.30) is one of their greatest assets. Some consider having a good attitude simply being positive at work, but that is not the entire picture.

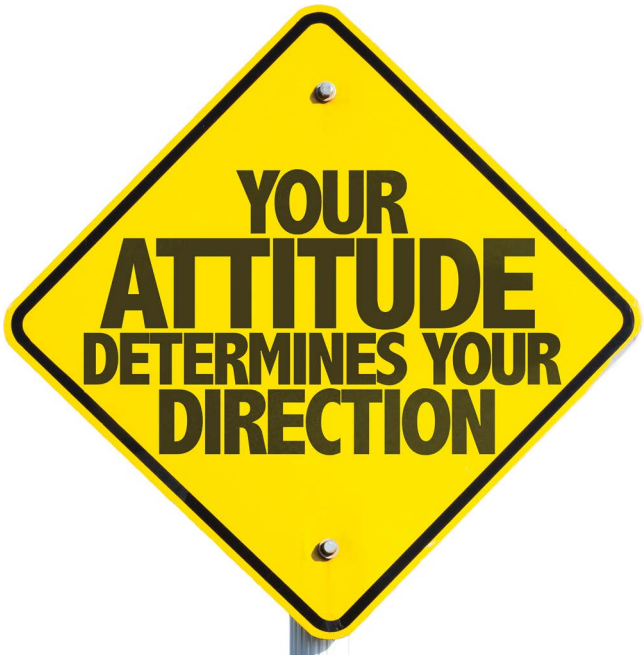


FIGURE 8.30 Your attitude is important

A technician with a good attitude has the following traits:

- **Is proactive, not reactive:** A good technician actively looks for a solution rather than waiting for someone to instruct them.
- **Projects confidence:** A technician who lacks confidence is easily spotted by end users. A confident technician isn't arrogant but instead is secure in the knowledge that a problem can be solved.
- **Seeks solutions instead of providing excuses:** A positive person does not continually apologize or talk in a subservient tone. For example, a positive technician explains issues such as late deliveries in a professional, positive manner.
- **Accepts responsibility for actions taken:** If you forget something or take a misstep, you should apologize and explain to the customer what happened. Truth goes a long way with customers. A positive technician does not constantly shift blame to other departments or technicians. Even if the other department or technician is responsible, a person with a positive attitude handles the customer and then talks to the other department or technician about the problem.
- **Deals with priority changes professionally:** In the IT field, computer and network problems may require tasks to be reprioritized weekly, daily, and even hourly. These are normal occurrences, and a person with a positive attitude understands this.
- **Cooperates and works well with others:** A positive attitude is contagious, and others like being around it.
- **Maintains professionalism even when working with a coworker who is unethical, unprofessional, or uncooperative:** A technician with a good attitude does not let someone else's poor attitude be a negative influence.

> **Embraces problems as challenges to learn and develop skills:** Sometimes, after joining the IT field, a technician becomes complacent and does not seek new skills. The IT field requires that you constantly improve and refine your skills. See a tough problem as a challenge, not a burden. With such an attitude, problems will not frustrate you but will serve as catalysts for advancement and make you a better technician.

You should exhibit all these traits consistently to establish a positive mental attitude and make it part of your daily habits.

Chapter Summary

> A video card uses a PCIe slot and may require additional power.
> Video memory can be separate from motherboard RAM, can be shared system memory, or can be a combination of both.
> When a computer shows a blank screen, check the power source, the display cable, the power cable, and the surge protector. Try rebooting and using the *Safe Mode* or *Enable low resolution video* boot option.
> If an artifact appears on a display, check for heat problems.
> If an LCD or plasma display has burn-in, try turning off the display for a few hours. Create an all-white image in a graphics program and use it as the screen saver. Turn the display brightness to low and leave the monitor on for a few hours.
> If geometric distortion occurs or if the screen is not centered correctly, check video cables or reset the display to the factory default settings.
> If the display image is dim or blank, try adjusting the brightness controls and contrast. Reset to the factory defaults. Replace the inverter.
> If the display flickers, check the video cable or refresh rate. Check for external radio or other interference sources.
> Projectors come with a variety of ports, including VGA, DVI, HDMI, composite, and component/RGB.
> Check power, input source, and computer output source if nothing outputs to a projector. The bulb may be burnt out.
> A motherboard normally has a small speaker used for POST codes when sound does not work properly.
> If a sound card is installed, disable the motherboard sound ports.
> The higher the sampling rate, the better the audio quality.
> For sound issues, check muting, volume controls, cables, and device conflicts.
> Install ODDs using the same rules of configuration as for SATA drives.
> Use the appropriate media for the type of drive installed.
> Optical drives and discs have region codes that must match.
> For stuck optical discs, use the *Eject* option from Windows Explorer/File Explorer or the emergency eject hole.
> Keep the laser lens clean.
> Wipe dirty discs in an inward-to-outward (not circular) motion.
> Scanners commonly connect using USB, an RJ45 network port, or through a wireless network.
> Do not spray cleaner directly on scanner glass but do keep the glass clean.
> A webcam can be integrated into a display or mobile device, or it can be an external unit that is used for conference calls or for recording video.

> When installing and configuring peripheral devices, always follow manufacturers' directions. Software is commonly provided to configure device options.
> A technician should have a positive attitude and project confidence, be proactive, and maintain professionalism when working with others.

A+ CERTIFICATION EXAM TIPS

- ✓ Be able to install and configure a sound, a video card, and a capture card.
- ✓ Be able to select and install an optical drive and a flatbed scanner.
- ✓ Recognize symptoms and what to do when the following video problems occur: cabling issues, fuzzy images, burn-in, dead pixels, flashing screen, incorrect color, audio issues (if the display has this capability), and a dim image.
- ✓ Note that projector troubleshooting has similar issues that require additional troubleshooting—like dim image, cabling issues, audio issues, and fuzzy images—but can also have problems like incorrect data source, burnt-out bulb, and intermittent shutdown.
- ✓ Recognize that an optical drive can make grinding or clicking noises if the disc is inserted incorrectly.
- ✓ Maintaining a positive attitude and projecting confidence are the professionalism and communication skills that are part of the 220-1202 exam.

Key Terms

ADF scanner, attitude, audio issue, blank screen, burnt-out bulb, clicking sound, color gamut, component/RGB video, dead pixel, digitizer, dim image, DirectX, discrete GPU, display burn-in, distorted image, `dxdiag`, flashing screen, flatbed scanner, frequency response range, fuzzy image, grinding noise, iGPU, incorrect color, incorrect data source, integrated graphics card, intermittent projector shutdown, inverter, LCD, LED, lumens, mini-LED, OLED, optical drive, physical cabling issue, pixel density, pixel pitch, power rating, refresh rate, region code, screen resolution, shared system memory, sizing issue, sound card, touch screen, video capture card, video card, webcam

Review Questions

Consider the following optical drive specifications as you answer Questions 1–7:

- SATA interface half-height internal BD-ROM
- Maximum 4x BD-ROM/BD-RE SL and 4x BD-ROM/BD-R/BD-RE DL CAV reading
- Maximum 8x DVD-ROM/+R/+RW/+RDL/-R/-RW/-RW DL CAV reading
- Maximum 32x CD-ROM/R/RW CAV reading
- Random access times: BD, 250 ms; DVD, 160 ms; CD, 150 ms
- Buffer size 2 MB
- System requirements for HD Blu-ray playback: 3.0 GHz, 1 GB+ of RAM, Windows 7 or higher, HDCP capable display, or TV for digital output.

1. Which SATA version is being used?

   [1 | 2 | 3 | Cannot be determined from the information given]

2. Can Blu-ray discs be created on this unit? How can you tell?

   _____

3. Pretend you are adding this device to a computer. What is the maximum number of devices (if any) that can be on the same cable that connects this drive to the motherboard?

   [None | 1 | 2 | Cannot be determined from the information given]

   _____

4. What would the computer have to have in order to install this device?

   _____

5. If the non-used SATA motherboard ports are disabled by default how would a technician enable them before installing this device?

   _____

6. Can a DVD±RW disc be read in this drive? How can you tell?

   _____

7. What does BD-RE DL mean?

   _____

   _____

8. A technician for a computer store is examining a computer that a client has just built and brought into the store. The AMD-based system will not output video even though the system has an HDMI port and a new HDMI cable attaches to a new display that works on another system and is powered. What is a likely problem?

   a. The cable is bad.

   b. The monitor is bad.

   c. The system RAM needs to be inserted properly.

   d. The system needs a video adapter.

9. Select the non-sound port.

   [RJ45 | S/PDIF | TOSLINK | RCA | 1/8-inch TRS]

10. Which optical media has the highest capacity? [DVD | CD | BD]

11. Which drive would have two lasers?

    a. A drive that can handle an 8.5 GB single-sided dual-layer disc

    b. A drive that can handle a double-sided single-layer disc

    c. A drive that can handle a 25 GB dual-layer disc

    d. A drive that can handle either a DVD or a Blu-ray disc

12. A PCIe sound card is being installed. Which two steps are most likely going to be done by the technician? (Choose two.)
    - **a.** Upgrade the power supply.
    - **b.** Install a driver.
    - **c.** Flash the BIOS/UEFI.
    - **d.** Disable the integrated ports in BIOS/UEFI.
    - **e.** Configure jumpers on the adapter.
    - **f.** Delete the integrated port drivers.
13. Which utility is best used to troubleshoot sound issues?

    [Disk Management | DirectX | BIOS/UEFI diagnostics | Device Manager]
14. A projector is not outputting sound. What are three likely issues? (Choose three.)
    - **a.** burnt-out bulb
    - **b.** mute button
    - **c.** faulty projector filter
    - **d.** projector volume setting
    - **e.** projector fan
    - **f.** projector battery low
    - **g.** computer volume setting
15. A user has attempted a scanner installation to the computer's front USB ports because all the back ports were taken. However, the scanner will not function. What should the technician try next?
    - **a.** Replace the scanner.
    - **b.** Replace the USB port.
    - **c.** Reattach the USB cable that leads from the front panel to the motherboard.
    - **d.** Add a version 2.0 or higher USB hub to a back USB port.
16. [T | F] A technician can clean a scanner using paper towels.
17. [T | F] Part of the installation process for a tablet is to calibrate the camera.
18. A user has heard about dead pixels and has brought in a recently purchased display, suspecting that the display has this issue. What should the technician do?
    - **a.** Replace the display.
    - **b.** Connect the display to a computer and use the burn-in process to check the display for this problem.
    - **c.** Test the display and explain that dead pixels are common and as long as there are not too many of them, they will not interfere with the output.
    - **d.** Tell the user to update the video drive and the BIOS/UEFI version.
19. An administrative assistant who commonly uses a specific meeting room complains that the projector is shutting down after five minutes each time it is used. What is a likely issue?

    [bulb | power supply | input source | filter]

20. Which scenario is one that most shows a positive attitude?
    a. A technician returns a borrowed disc to a team member after having the disc more than six months.
    b. A technician leaves documentation for a newly installed optical drive with the customer, even though the customer treated the technician poorly during the installation.
    c. A technician eagerly helps reorganize a wiring closet for the company.
    d. A technician smiles when an angry customer is taking out her computer problems on the technician.

Exercises

Exercise 8.1 Video and Multimedia Device Research

Objective: To be able to use the internet to locate device drivers and technical specifications

Parts: A computer that has internet access

Procedure: Using the internet, find the cost, latest device driver, and most important technical specification for each of the devices listed in Table 8.9.

TABLE 8.9 Multimedia device information

Device type	Cost	Device driver version	Most important technical specification
Flatbed scanner	_____	_____	_____
Barcode reader	_____	_____	_____
Video card	_____	_____	_____
Projector	_____	_____	_____
Digitizer	_____	_____	_____
Webcam	_____	_____	_____
Sound card	_____	_____	_____
Speakers	_____	_____	_____

Exercise 8.2 Which One Will You Buy?

Objective: To be able to use the internet to locate multimedia devices for a specific purpose

Parts: A computer that has internet access

Procedure: Using the internet, find a device to meet the user specifications.

1. A 10-person conference room has an oval table. A computer is in the corner. The company would like to add a projector and a projection screen to the room. Do the following:
   - List three criteria you looked for in the projector.
   - List at least one projector you recommend.

   _____

   _____

2. A 25-person computer training room needs a scanner. The people who use the room scan forms completed by trainees. Each person completes a three-page form. Because of the nature of the information, the form cannot be put onto a web page.
   - List three criteria you looked for in the scanner.
   - List at least one scanner you recommend to the company.

   _____

   _____

3. A person owns a home business creating videos for events such as weddings, receptions, showers, and so on and providing a digital copy of each edited video. Previously, the owner provided the digital copy on an external drive, but now the owner wants to offer optical media as well. Even though folders are backed up to a remote site, what type of optical drive and media supported by the drive would you recommend for this home business owner?

   List the type of optical drive you recommend and give at least two reasons for why you chose this type.
   - Would you recommend an internal or external drive? Describe why you chose this type.
   - List at least one drive you would recommend for this desktop computer. Include the part number and website where you found the drive.

   _____

   _____

Activities

Internet Discovery

Objective: To obtain specific information on the internet regarding a computer or its associated parts

Parts: Computer with access to the internet

Questions: Use the internet to answer the following questions.

1. Find a website that sells external optical drives. List the cost of one drive and the website URL.

   _____

2. Find three recommended replacement PCIe 3.0 x16 video cards with a minimum of 4 GB of video RAM for a gamer who can spend a maximum of $300. List the three models and the website URL where you found each one.

   _____

   _____

   _____

3. Find the driver version for a Sound BlasterX AE-7 PCIe adapter that is going in a Windows 11 computer. Document the driver download filename and URL where you found this information.

4. A business is using the NEC NP-UM352W projector. Whenever they use the projector, the picture suddenly becomes dark. List the recommended steps and the URL where you found this information.

5. The president of a company has a 43-inch Samsung Class Crystal UHD DU7200 mounted in the office. Does this device support outputting to a sound bar? Write the answer with an explanation of how you know this based on the specifications and the URL where you find the answer.

6. A customer has a Plextor PX-891SAF CD-RW, DVD+/-RW drive. How much buffer memory does the drive contain, and which interface(s) does it support? Write the answers and website URL where you found the information.

Soft Skills

Objective: To enhance and fine-tune a technician's ability to listen, communicate in both written and oral forms, and support people who use computers in a professional manner

Activities:

1. List some tips for determining whether a computer has an optical drive installed, as if you were stepping through it over the phone with a customer who is not a technician. Using your instructions, practice with a classmate.

2. With the class divided into groups of five, each group makes a list of three categories that relate to multimedia devices. The five groups share their lists and determine which group works on which category. In 30 minutes, each team comes up with five answers with corresponding questions for their category. The answers are rated from 100 to 500, with 100 being the easiest. The teams play *Jeopardy!*, with the rule that each team cannot choose its own category.

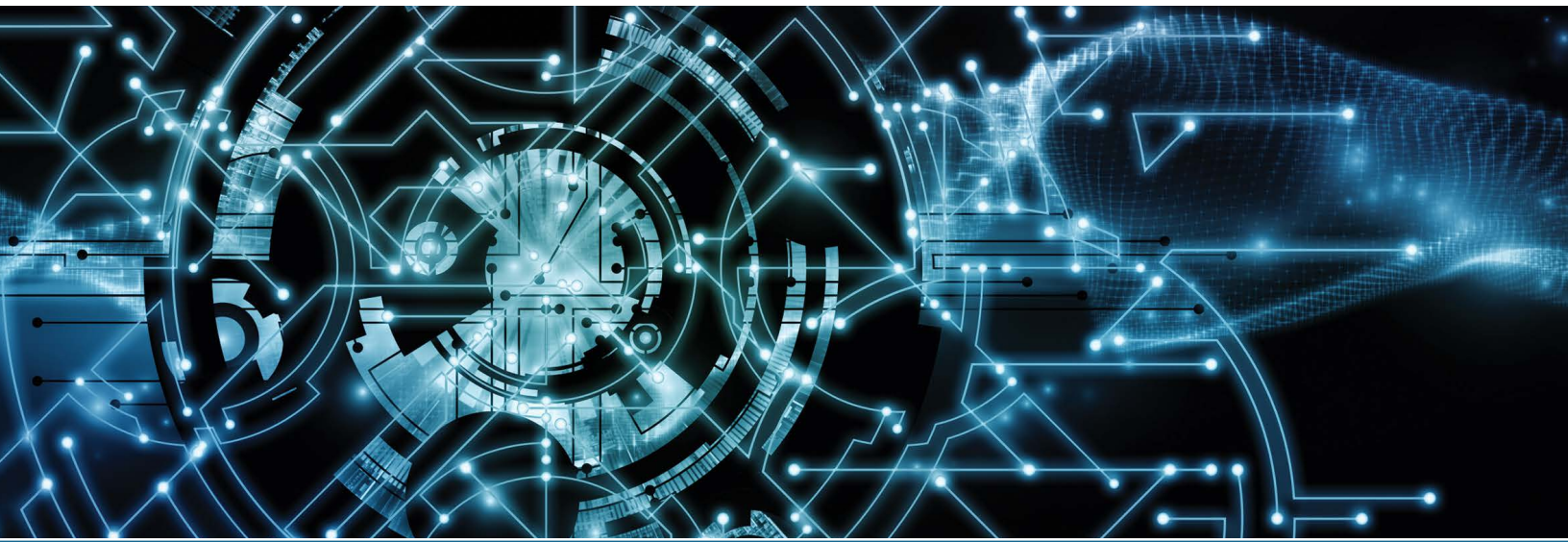
Critical Thinking Skills

Objective: To analyze and evaluate information and apply information to new or different situations

Activities:

1. For this activity, you need an advertisement for a sound card, including the technical specifications. Make a list of all terms used in this ad that you do not know. Using books, the internet, or other resources, research these terms and define them.
2. Form teams of two and obtain several multimedia devices. The devices are numbered. Each team selects a number and installs, configures, and tests the associated device. Each team documents its installation and shares its experience (including lessons learned) with the rest of the class.

9 Printers/Multifunction Devices



In this chapter you will learn:

- How each type of printer operates
- The steps required to install a printer or multifunction device
- Preventive printer maintenance
- How to control printers/multifunction devices from Windows and make printer adjustments
- How to solve common printer/multifunction device problems
- Techniques for ethical and professional behavior

CompTIA Exam Objectives:

- ✓ 1201-2.3 Summarize services provided by networked hosts.
- ✓ 1201-3.7 Given a scenario, deploy and configure multifunction devices/printers and settings.
- ✓ 1201-3.8 Given a scenario, perform appropriate printer maintenance.
- ✓ 1201-5.6 Given a scenario, troubleshoot printer issues.
- ✓ 1202-4.7 Given a scenario, use proper communication techniques and professionalism.

Printer/Multifunction Device Overview

Printers are commonly used output devices and can be a source of frustration for users. Printers frequently have additional functions, such as scanning, copying, and faxing. A printer that can do other things is called a **multifunction device**, or all-in-one device. The multifunction device shown in Figure 9.1 has an automatic document feeder (**ADF**) on top, which is used to feed papers to be copied, scanned, or faxed. We will be looking at how to install and troubleshoot these devices in this chapter.

FIGURE 9.1 Multifunction device

TECH TIP

Dealing with sensitive printed material

If any printouts are on a printer, ask the user to remove them and put them away. Demonstrate professionalism any time you are exposed to corporate or personal information that might be found on printers or desks or within documents.

Categories of Printers

Printers can be categorized according to how they put an image on paper. There are five main categories of printers: impact, inkjet, laser, thermal, and 3-D. There are other types, but these five account for the majority of printers used in businesses and homes. Computer users normally choose a printer based on the type of printing they need to do. Table 9.1 describes the five major printer categories.

TABLE 9.1 Printer categories

Type of printer	Description
Impact printer	Also known as a dot matrix printer, good for printing multiple copies of text but has limited graphics capabilities. Uses ribbons. It is the only printer that can do multiple-part forms using impact printer paper/forms and supports the 132-column paper needed in some industries.
Inkjet printer	Much quieter and produces higher-quality graphics than an impact printer. Uses an ink cartridge that costs $10 to $60 and can print a varying number of pages, depending on the manufacturer, the size of the cartridge, what is printed, and print quality settings. Inkjet printers are best for color printing.
Laser printer	Produces the highest-quality output at the fastest rate. Uses a toner cartridges that can cost $20 to $350. Common in the corporate network environment, where users share peripherals and require fast printing, often in bulk. Used for graphic design and computer-generated art where high-quality printing is a must. Some can produce color but at a much higher cost. Some have stapling capabilities.
Thermal printer	Uses special thermal paper that is sensitive to heat. An image is created where the heat is applied. Commonly used as ticket printers or receipt printers in retail outlets and gas stations.
3-D printer	Used to create 3-D objects using various types of materials, including plastics, **resin**, filament, thermoplastics, clay, alloys, rubber, stainless steel, and metal alloys.

Impact Printers

Impact printers (see Figure 9.2) are also called dot matrix printers because of the way they create an image on paper. Such a printer has an **impact printhead** that holds tiny wires called print wires. Figure 9.3 shows an OKI Data Americas, Inc., printhead. The print wires are shown on the front of the printhead. The print wires can get out of alignment and produce malformed characters.

FIGURE 9.2 Impact printer

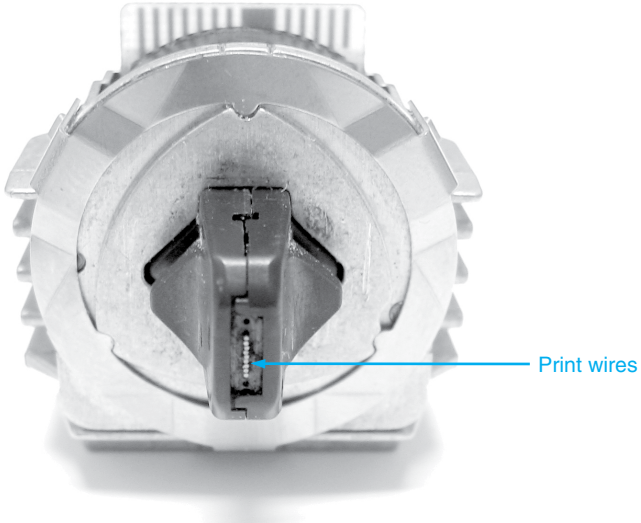


FIGURE 9.3 Impact printer head

The wires individually strike a **print ribbon** hard enough to create a dot on the paper. The dots collectively form letters or images. The speed at which the printhead can place characters on a page is its characters per second (cps) rating. The number of print wires in the printhead determines the quality of printing: The more print wires, the better the print quality. The most common numbers of print wires are 9, 18, and 24. The 24-pin impact printers can print near letter quality (NLQ) output.

When current flows to the print wire, a magnetic field causes a wire to move away from the printhead and out a tiny hole. The print wire impacts a ribbon, creating a dot on the paper. The act of the print wire coming out of the printhead is called *pin firing*. The impact of the printer physically striking the ribbon, which in turn touches the paper, causes impact printers to be noisy. Figure 9.4 shows an impact printer printhead. To show the individual print wires, the casing that covers the print wires has been removed from the illustration.

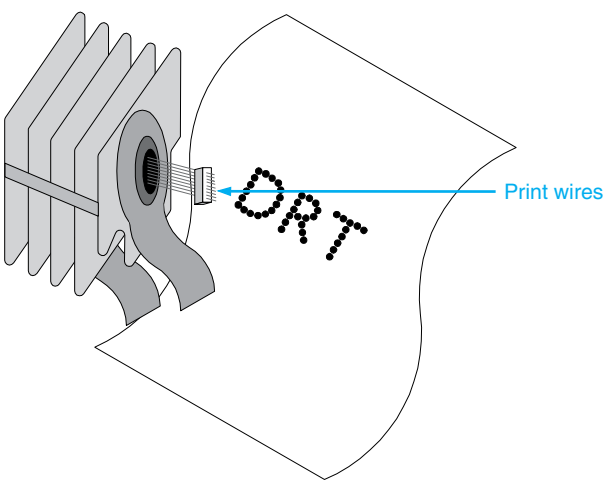


FIGURE 9.4 Impact printhead operation

TECH TIP

Printing in one direction is not a problem

Most impact printers print bidirectionally. When the printhead gets too hot, the printer prints only in the left-to-right direction. This is normal.

Because the print wire impacts the ribbon, one of the most common points of failure with impact printers is the printhead. It can be expensive to replace printheads frequently in a high-usage situation; however, refurbished printheads are available at a reduced price.

Impact printers are the workhorses of printers. One advantage of an impact printer is that it can print multiple-part forms and wide forms. Special **multipart paper** can be purchased so duplicates are made each time a print job is sent. Laser and inkjet printers cannot produce multiple-part forms; they can only make multiple copies of the same document.

TECH TIP

Don't stack

Don't stack things on top of a printer, especially an impact printer. Keep a printer in a cool environment to avoid overheating.

Inkjet Printers

Inkjet printers are much quieter than impact printers and are used to print black-and-white, gray-scale, and color output. An inkjet printer also has an **inkjet printhead** that may be integrated into the ink cartridge. The cartridge has many tiny nozzles that squirt ink onto the paper. Each nozzle is smaller than a strand of human hair. There are up to 6,000 nozzles, for better quality than is available with the 9-, 18-, or 24-pin configuration of an impact printer. Figure 9.5 shows an **ink cartridge**. Notice the three rows of nozzles on the cartridge on the left.

FIGURE 9.5 Inkjet print cartridge

Inkjet printers, also called bubble jet printers, use thermal (heat) technology to place the ink on the paper. Each print nozzle attaches to a small ink chamber that attaches to a larger ink reservoir. A small amount of ink inside the chamber heats to a boiling temperature. Once the ink boils, a vapor bubble forms. As the bubble gets hotter, it expands and goes out through the print cartridge's nozzle onto the paper.

An alternative for producing the ink dots is to use piezo-electric technology, which uses pressure, rather than heat, to eject the ink onto the paper. Some companies use this technology to obtain high resolutions. DPI is the number of dots per inch a printer outputs. The higher the DPI, the better the quality of inkjet or laser printer output. Figure 9.6 shows the basic principle of how an inkjet printer works. Table 9.2 lists the major parts of an inkjet printer.

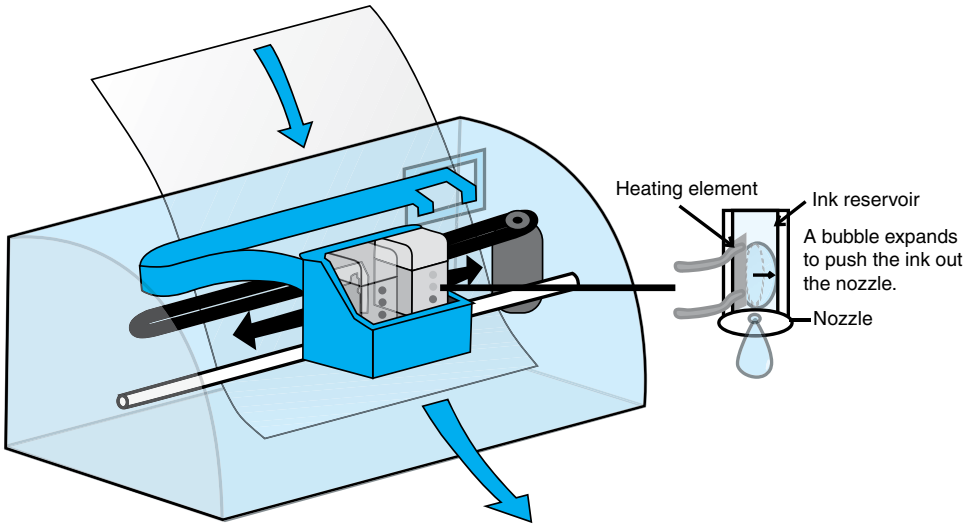


FIGURE 9.6 How an inkjet printer works

TABLE 9.2 Inkjet parts

Part	Description
Printhead	Contains nozzles used to dispense ink
Printhead assembly	Holds the printhead and possibly ink cartridge(s)
Ink cartridge	Also known as a print cartridge or simply as a cartridge; may be one color or may have sections for separate colors and may include the printhead
Stepper motor	Used to move the printhead/ink cartridge from one side of the printer and back as well as move the printhead assembly (see Figure 9.7)
Carriage belt	Connects to the stepper motor and printhead assembly to move the printhead and ink cartridge from one side of the printer to the other side (see Figure 9.7)
Power supply	Converts wall outlet AC to DC for inside the printer
Carriage	The part that moves from one side of the printer and back; includes the belt, stabilizer bar, and printhead assembly, as well as the printhead that may be included with the ink cartridge(s) (see Figure 9.7)
Paper tray and/or paper **feeder**	Holds paper (see Figure 9.7)
Roller	Moves paper through the printer
Duplexing assembly	Supports two-sided printing (see Figure 9.16, later in the chapter)

Most inkjet printers have different printing modes. The draft mode uses the least amount of ink, and the NLQ mode uses the most ink. The quality produced by an inkjet printer is equal to or sometimes higher than that of a laser printer, and inkjet printers print in color, whereas most laser printers print only in monochrome (black and white).

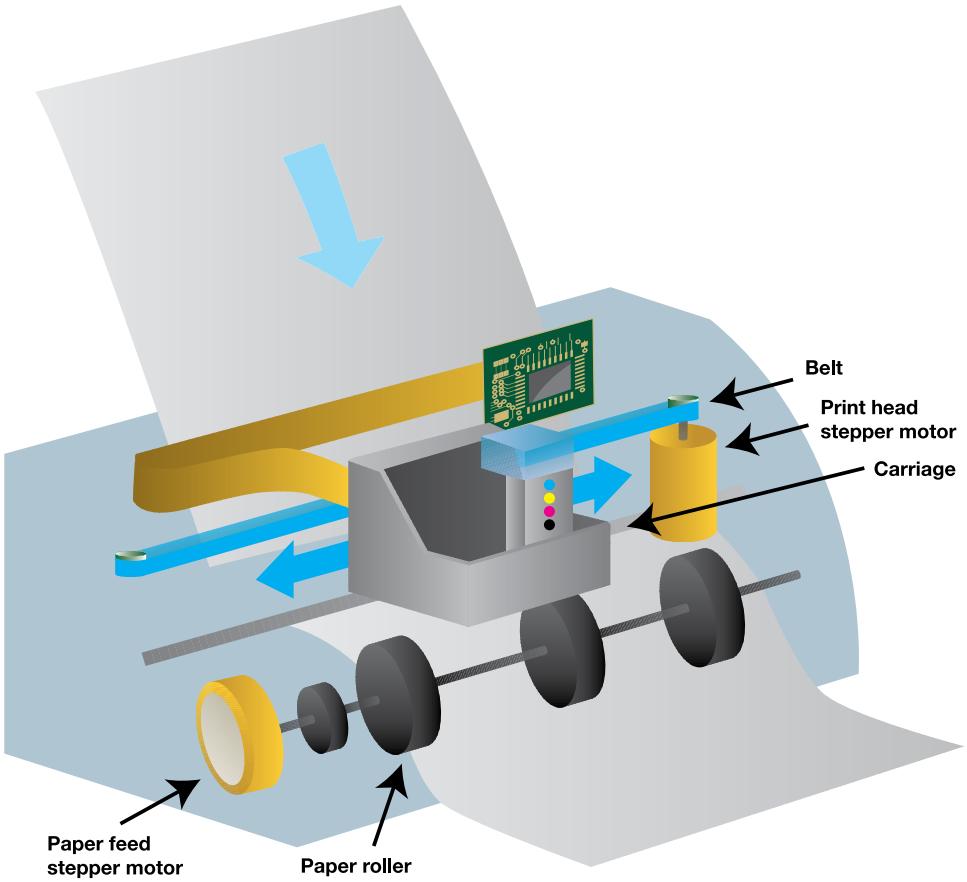


FIGURE 9.7 Major inkjet printer parts

TECH TIP

Be aware of optimized DPI

Many inkjet printers now show their DPI as *optimized* DPI. Optimized DPI describes not how many drops of liquid are in an inch but how many are in a specific grid.

Color inkjet printers usually have a black cartridge for text printing and a separate color cartridge or separate cartridges for non-black ink. Buying an inkjet printer that uses a single cartridge for all colors means a lower-priced initial printer purchase but is more expensive in the long run. Models do exist that have separate cartridges for black ink and the other colors.

A drawback to using an inkjet printer is that sometimes the ink smears. Ink manufacturers vary greatly in how they respond to this problem. If the paper gets wet, some inkjet output becomes messy. The ink also smears if you touch the printed page before the ink dries. The ink can also soak into and bleed down the paper. Using good-quality paper and ink in the ink cartridge helps with this particular problem. See the section "Paper," later in this chapter, for more information on choosing the correct paper for different printers.

There are some alternatives to inkjet technology. Table 9.3 outlines five of them.

TABLE 9.3 Other printer technologies

Type of printer	Description
Solid ink printer	Sometimes called a phase change or hot melt printer; uses colored wax sticks to create vivid color output. This type of printer can print more colors, is faster, has fewer mechanical parts, and is cheaper than color laser printers but is more expensive than normal inkjet printers.
Dye sublimation printer	Also known as a dye diffusion thermal transfer printer; uses four film ribbons that contain color dyes. The quality is high, but the printers are expensive.
Thermal wax transfer printer	Uses wax-based inks like a solid ink printer but prints at lower resolutions.
Large-format inkjet printer	A wide printer to print large-scale media such as CAD drawings, posters, and artwork.
3-D	Used to create 3-D objects out of various types of materials. An image is scanned into the computer, drawn, or downloaded from the internet. Software slices the images into thousands of layers. The printer creates each layer until the object is formed, as shown in Figure 9.8.

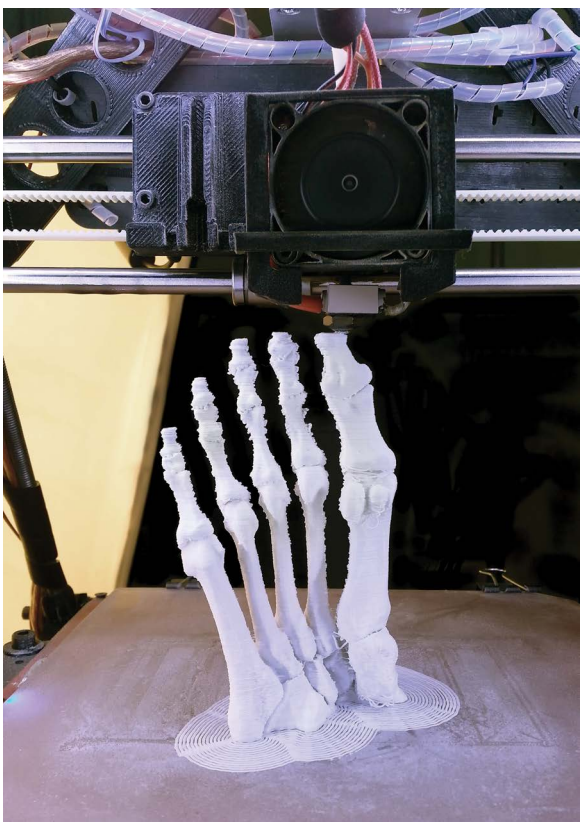


FIGURE 9.8 3-D printing

Laser Printers

Black-and-white laser printers have lower cost per page than inkjet printers, making them a good investment for general printing. A laser printer uses a process similar to a copy machine's electrophotographic process. Before exploring how a laser printer works, let's identify the major parts inside a printer to better understand how it works. Figure 9.9 shows a side view of a laser printer.

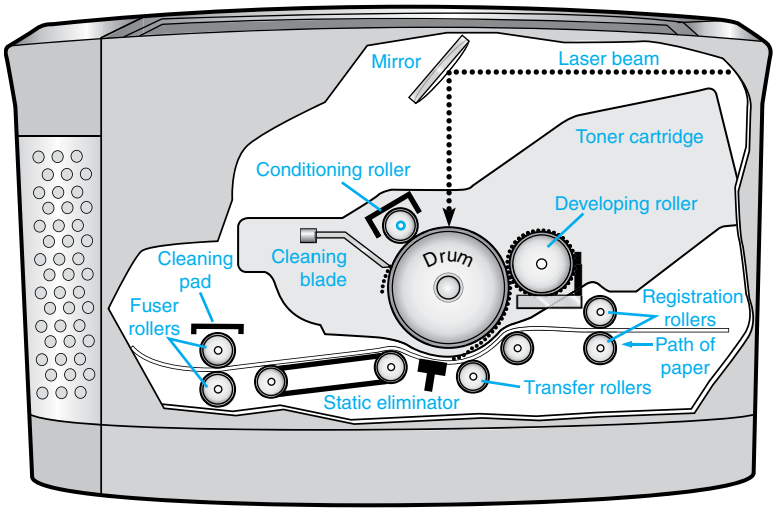


FIGURE 9.9 Inside a laser printer

TECH TIP

Knowing the dangers inside laser printers

Be very careful when working inside a laser printer. There are high voltages and high temperatures in various parts. Turn off the printer and let it cool down before servicing it. Remove power from the printer before working on it, when possible.

The computer sends 1s and 0s to the printer. The data is converted into dots. and sent through an array of LEDs or through a laser beam. The light beam strikes the photosensitive imaging drum located inside the toner cartridge (see Figure 9.10). Laser toner particles are attracted to the drum. The paper feeds through, and the toner transfers to the paper. The toner is then fused or melted onto the paper. Table 9.4 summarizes the seven-step laser printer imaging process.

FIGURE 9.10 Laser imaging drum

TABLE 9.4 Laser printer imaging process

Step	Description
Processing	This step involves getting the data ready to print. The laser printer converts the data from the printer language into a bitmap image. The laser printed page is made up of very closely spaced dots.
Charging	This step involves getting the drum ready for use. Before any information goes onto the drum, the entire drum must have the same voltage level. The primary (main) corona or conditioning roller is used to apply a uniform electrical charge.
Exposing	A laser creates a charge-neutralized pattern on the drum's surface. By selectively exposing the drum to light, the laser neutralizes the electrostatic charge in specific areas, forming a latent image (invisible electrostatic pattern). The image on the drum is nothing more than dots of electrical charges and is invisible at this point.
Developing	This step involves getting toner on the drum (developing the image). A developing cylinder/roller inside the toner cartridge contains a magnet that runs the length of the cylinder. When the cylinder rotates, toner (with iron particles) is attracted to the cylinder. The magnetized toner particles are attracted to the places on the drum where the light beam strikes. The image is now black on the drum surface.
Transferring	The image is transferred to paper. A transfer belt (roller, corona, or pad) is located at the bottom of the printer and places a positive charge on the back of the paper. The positive charge attracts the negatively charged toner particles from the drum. The particles leave the drum and go onto the paper. At this point, the image is on the paper, but the particles are held only by their magnetic charge.
Fusing	The **fuser assembly** melts the toner onto the paper. Heat and pressure make the image on the paper permanent. The top roller applies intense heat to the toner and paper that literally squeezes and melts the toner into the paper fibers. Figure 9.11 shows an example of a fuser assembly and the motor that is used with it.
Cleaning	A wiper blade or brush clears the photosensitive drum of any excess toner. Then a charge roller neutralizes any charges left on the drum so the next printed page begins with a clean drum.

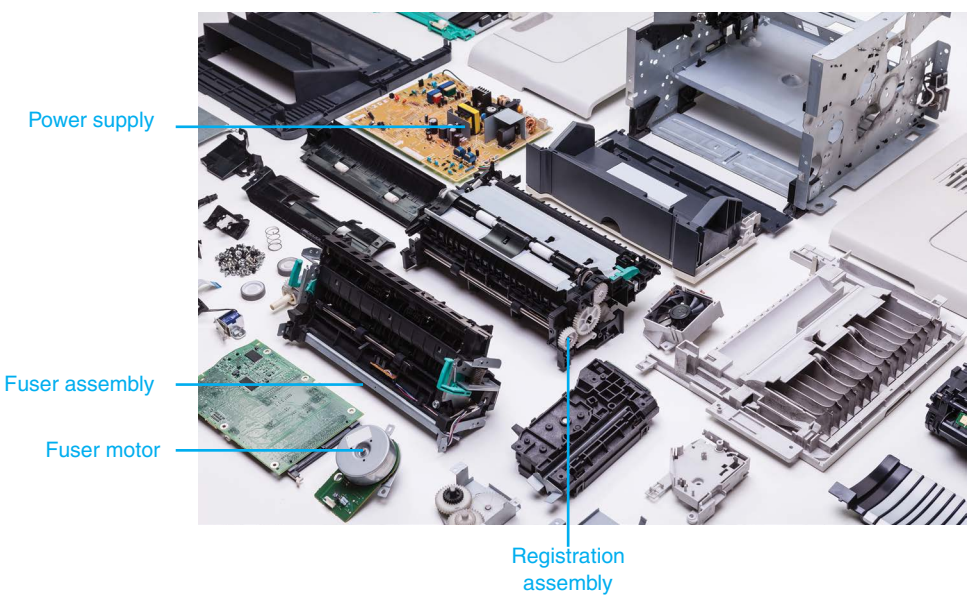


FIGURE 9.11 Laser printer parts

TECH TIP

Laser printers *do* make weird noises

A laser printer frequently makes an unusual noise that is a result of the fusing rollers turning when the printer is not in use. If the rollers didn't turn like this, they would have an indentation on one side. Users not familiar with laser printers sometimes complain about this noise, but it is a normal function of a laser printer.

To help with this flood of data about laser printers, Table 9.5 lists the major parts of a laser printer and briefly describes the purpose of each one.

TABLE 9.5 Laser printer parts

Part	Purpose
AC power supply	Acts as the main power supply for the printer
Cleaning blade	Wipes away excess toner from the drum before printing the next page
Cleaning pad	Applies oil to the fusing roller to prevent sticking; also removes excess toner during the fusing stage
Density control blade	Controls the amount of toner allowed on the drum (usually user adjustable)
Drum (photo-sensitive)	Also known as imaging drum; accepts light beams (data) from LEDs or a laser; can be permanently damaged if exposed to light; humidity can adversely affect it
Duplexing assembly	Supports two-sided printing
Fuser (fusing) assembly	Holds the fusing roller, conditioning pad, pressure roller, and heating unit
Fusing rollers	Applies pressure and heat to fuse the toner into the paper
Toner	Powder made of plastic resin particles and organic compounds bonded to iron oxide
Toner cartridge (EP cartridge)	Holds the conditioning roller, cleaning blade, drum, developing cylinder, and toner; always remove the toner cartridge before shipping a laser printer

TECH TIP

A word about spilled toner

Toner melts when warmed; small toner spills outside a printer can be wiped using a cold, damp cloth. Toner spills inside a printer require a special type of vacuum with special bags. Toner on clothing can normally be removed by washing in cold water. Do not put the clothing in a dryer if the toner has not yet been removed, or the toner will melt into the clothing and become impossible to remove.

Thermal Printers

Thermal printers are used in a lot of retail establishments and at kiosks, gas pumps, trade shows, and basically anywhere someone needs a little printer to print a small document, such as a receipt. IT staff commonly have to service thermal printers. Thermal printers are also known as point of sale (POS), or cash register, printers.

A thermal printer uses **special thermal paper** that is sensitive to heat. A printhead has closely spaced **heating elements** that appear as closely spaced dots on the heat-sensitive paper. A **feed assembly** is used to move the thermal paper through the printer. Figure 9.12 shows examples of thermal printers. Figure 9.13 shows how a thermal printer works.

FIGURE 9.12 Thermal printers

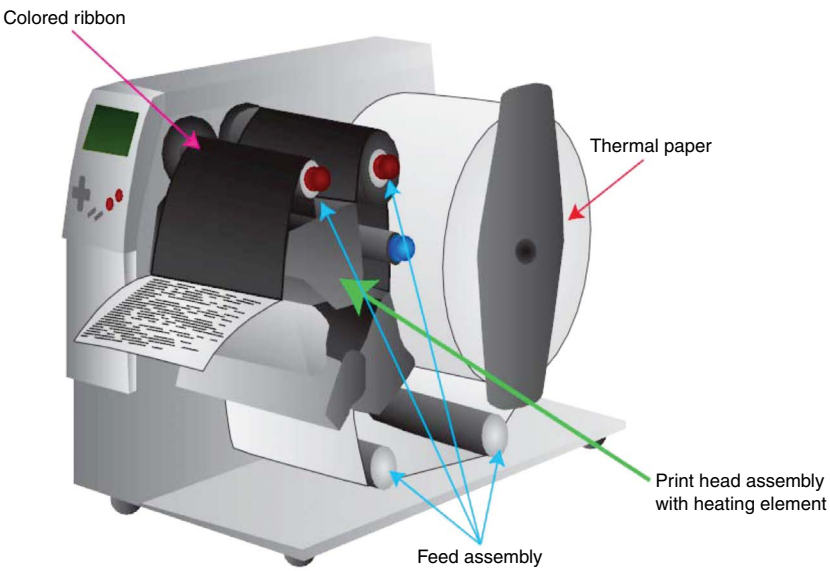


FIGURE 9.13 Inside a thermal printer

A technician must be sure to warn the user about the **high sensitivity of thermal paper** and to store the paper in a cool location. Most thermal printing situations—such as parking receipts and bar codes—require high-sensitivity thermal paper that does not last long. Other situations—such as certain sales receipts, warehouse labeling, and supermarket weigh scale labels—require low-sensitivity thermal paper that is not as affected by high temperatures or exposure to the sun.

The thermal printhead is one of the most important parts of a thermal printer. The printhead can be damaged in several ways:

> Residue or material buildup can cause uneven printing or missing dots
> Opening the print mechanism while printing
> Poor-quality thermal paper
> A dirty environment

- Other objects (stuck labels, staples, paper clip, and debris)
- ESD—even very little voltage—can damage the printhead. Use self-grounding or an anti-static wrist strap when handling the printhead.
- Excessive moisture, such as in high-humidity environments

Paper

The type of paper used in a printer can affect its performance and cause problems. Because inkjet printers spray ink onto the paper, the quality of paper determines how well the ink adheres. If the paper absorbs too much of the ink, the printout appears faded. For a laser printer, how well the paper heats and absorbs the toner affects the printed output. Paper is a big factor in the quality of the printouts produced and how long the printed output lasts.

Recycled paper may cause printer jams, but some paper manufacturers show a jam-free percentage. Another factor in the printed output is the brightness rating, which is a measurement of how much light the paper reflects. The higher the number, the more white the paper appears and the more crisp the printed output appears.

TECH TIP

Paper and pounds

Paper is rated in pounds (abbreviated lb) and shown as 20 lb or 20# (a good weight for standard use). A higher number indicates heavier, thicker paper.

The highest-quality paper available does not work well if the environment is too humid. Humidity causes paper to stick together and reduces the paper's strength, which causes feed problems. Paper affected by humidity may be noticeably lumpy. If you detect that paper is damaged, recycle it or make it into scrap paper. For best printing results, store paper in a non-humid storage area and fan the paper before you insert it into the printer's bin.

A multifunction device or printer might have two or even three paper feeds: from the rear paper tray, from a paper tray accessed from the bottom front of the unit, and from the top, which is commonly used for copying or scanning. Some impact printers allow you to remove the normal paper feeder and attach a **tractor feed** option that allows continuous-feed paper to be fed through the printer. Figure 9.14 shows how the paper with holes on both sides feeds through an impact printer. Figure 9.15 show the rear of an impact printer with the tractor feed option removed. Notice that the paper guide covers are open. Once you thread the paper into the printer and over the guide, you press the cover down to keep the paper in place. Both impact and inkjet printers have special feeders or a slide bar to feed envelopes or unusual-sized paper through. Laser printers sometimes ship with additional trays and must be configured for such options.

Another option is a **duplexing assembly**, which enables two-sided printing. You may have seen and heard a duplexing assembly in action on a copier. A duplexing assembly is more commonly purchased for a laser printer than for any other printer types, but specific inkjet printers can also have this optional part. The duplexer is integrated into the printer or attached to the bottom or rear of the printer and selected through the *Print* menu of any application. Figure 9.16 shows a duplexing assembly.

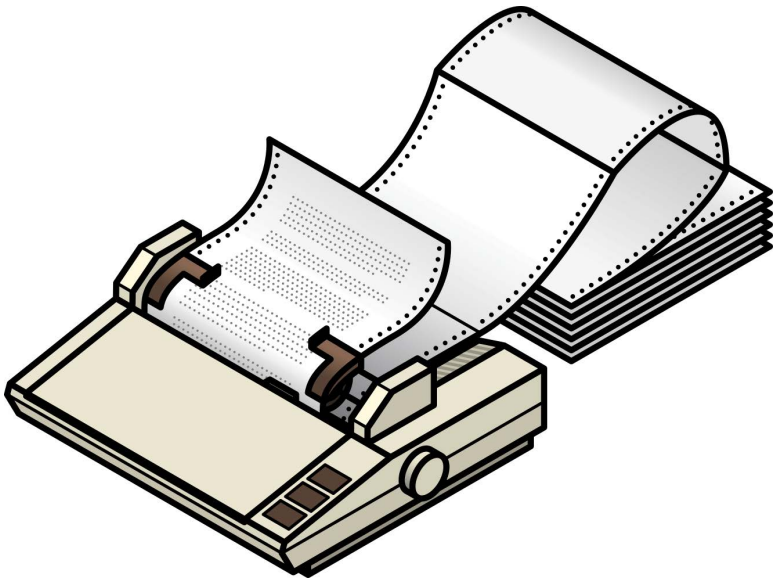


FIGURE 9.14 Tractor-fed paper

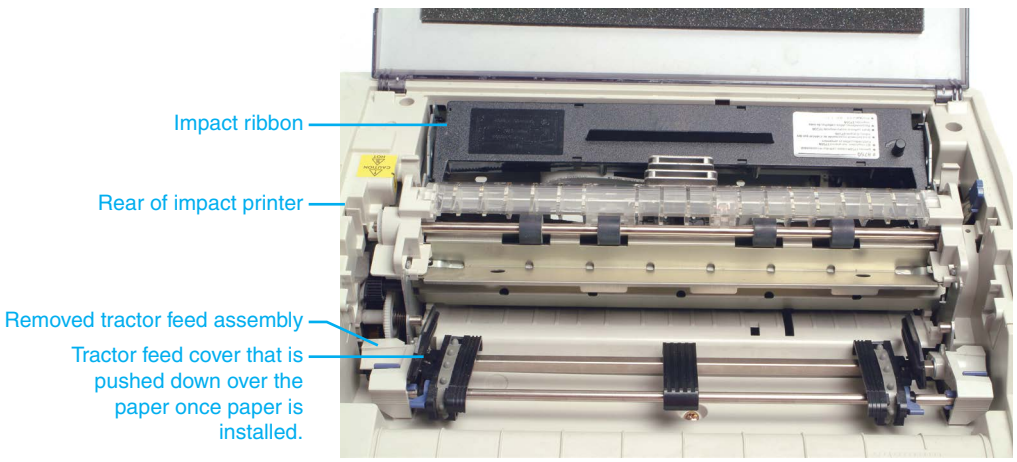


FIGURE 9.15 Impact printer with tractor feed option

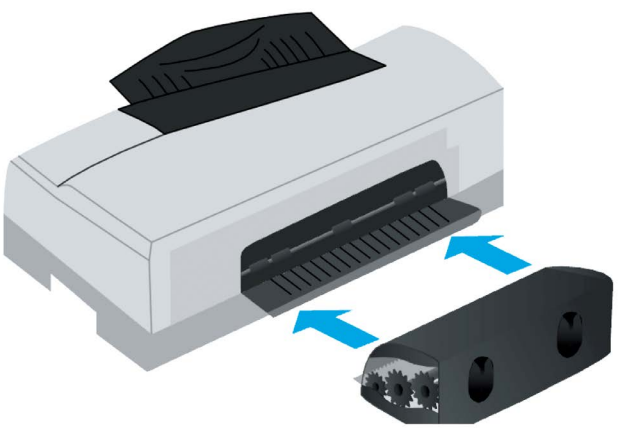


FIGURE 9.16 Duplexing assembly

TECH TIP

How to control printer trays and manual feed options

In Windows, the *General* tab of the *Printer properties* window is commonly used to view the current paper settings. Click the *Preferences* button to configure where you want the printer to look for paper to be used (see Figure 9.17).

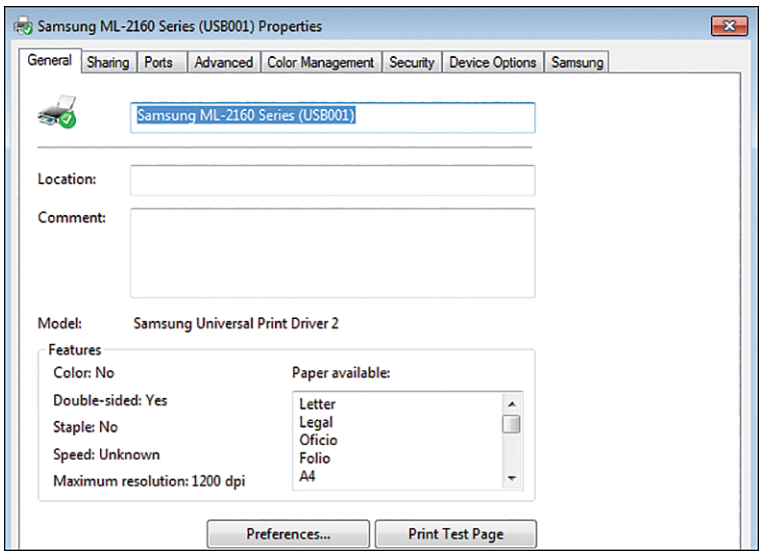


FIGURE 9.17 Paper options for a printer

Most printers allow you to set a default order in which the printer looks for paper. You can typically configure this through either manufacturer-provided software or the *Printer properties* window. As shown in Figure 9.18, many printers have both *Properties* and *Printer properties* options. Figure 9.19 shows the difference between the windows these options bring up. You will most likely want to use the *Printer properties* option.

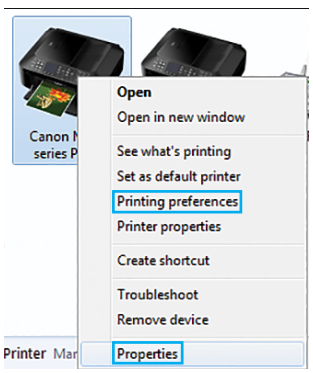


FIGURE 9.18 Right-click menu options for a printer

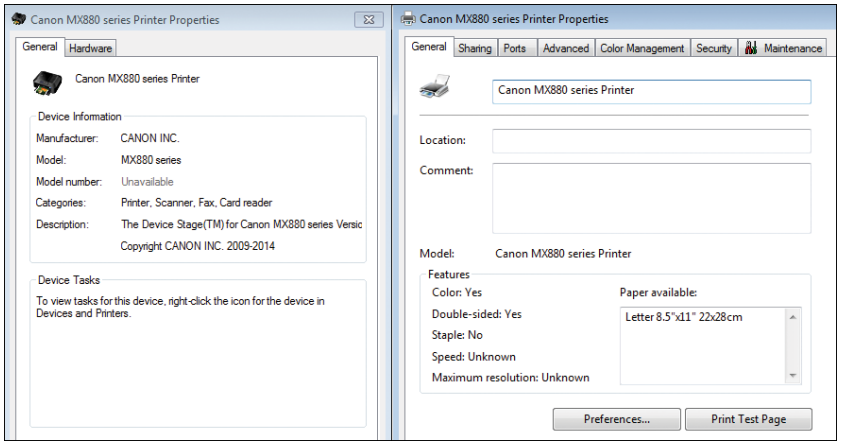


FIGURE 9.19 Properties window (left) and Printer properties window (right)

Virtual Printing

Printing of any type takes information formatted in a specific application (web browser, word processor, spreadsheet, photo viewer, and so on) and puts it into a format the printer understands. **Virtual printing** means printing to somewhere other than the directly connected printer and commonly to a specific file type so the file can be viewed, saved, or even emailed instead of printed or eventually sent to a printer. Four common virtual printing techniques are outlined in Table 9.6.

TABLE 9.6 Virtual printing options

Virtual printing type	Description
Print to file	Saves a print job as a .prn file to be printed later. Not all printers support this. *File* > *Print* > select *Print to File* checkbox > *OK*.
Print to PDF	Saves a print job as a Portable Document Format (.pdf) file (see Figure 9.20) that can be sent or printed to any printer later. If it is not shown, search for the *Advanced Printer Setup* Control Panel link > *The Printer That I Want Isn't Listed* link > *Add a Local Printer or Network Printer with Manual Settings* radio button > *Next* > from the *Use an Existing Port* drop-down menu, select *File: (Print to File)* > *Next*. From any application, select *File* > *Print* > select *Microsoft Print to PDF* > *OK*.
Print to XPS	Saves a file as a Microsoft XPS file that allows a document to be printed on any printer but not modified. From any application, *File* > *Print* > select *Microsoft XPS Document Writer* > *Properties* > *XPS Documents* tab > ensure the *Automatically Open XPS Documents Using the XPS Viewer* checkbox is enabled.
Print to image	Saves a file to an image file. When documents cannot print to PDF due to a poor download or damaged content, print to image is a great option. Some software allows you to save as a JPEG, TIFF, or PNG.

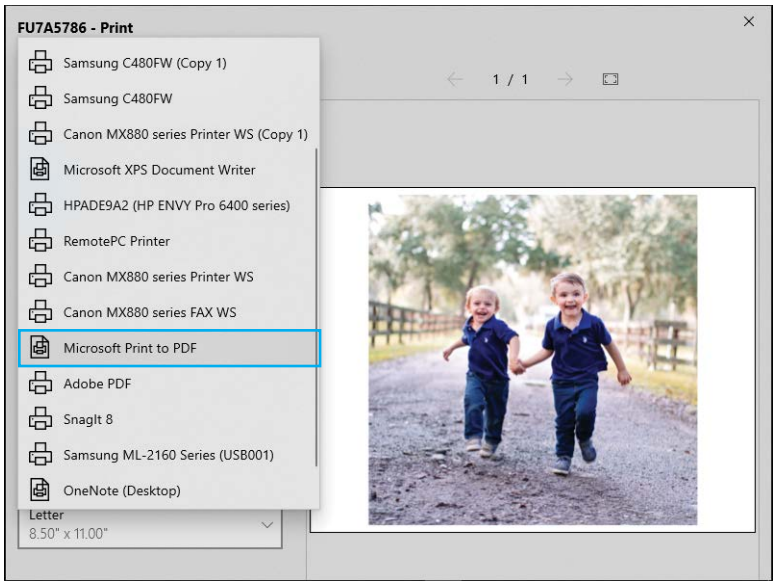


FIGURE 9.20 Microsoft Print to PDF option

Refilling Cartridges, Re-inking Ribbons, and Recycling Cartridges

Controversy exists about re-inking impact printer ribbons, refilling inkjet cartridges, and buying remanufactured laser cartridges. Even if a company or an individual user decides not to purchase remanufactured products, some send empty cartridges to companies that do the remanufacturing or take them to a local office supply company for credit. Refilling ink cartridges significantly lowers printing costs.

If you refill ink cartridges, you should add new ink before the old cartridge runs completely dry. Also, be sure the refill ink emulates the manufacturer's ink. Some ink refill companies use inferior ink that, over time, has a corrosive effect on the cartridge housing. A leaky cartridge or one that bursts, causing ink to get into the printer, is trouble.

Some ink refill companies have exchange systems. The old ink cartridges are placed into a sealed plastic bag and returned to the company, where they are remanufactured. In return, the company ships a remanufactured cartridge filled with ink. If the empty ink cartridge sent to the company does not meet the company's standards criteria, the cartridge is not used.

Some manufacturers offer a continuous ink system (CIS) that does not require changing out ink cartridges so often. Other companies sell a product that modifies a printer to use a CIS. Figure 9.21 shows a CIS.

When it comes to laser cartridge remanufacturing, the most important components are the drum and the wiper blade that cleans the drum. Many laser cartridge remanufacturers use the same parts over and over again. A quality refill company will disassemble the cartridge and inspect each part. When the drum and wiper blade are worn, they are replaced with new parts. Some states have disposal requirements for inkjet and laser printer cartridges.

TECH TIP

Beware of toner cartridges

Toner powder is harmful if inhaled. Wear a mask when refilling. Also, wear disposable gloves when replacing or refilling a toner cartridge to prevent toner from entering your skin pores.

FIGURE 9.21 Refilling a CIS

Re-inking an impact printer ribbon is not a good idea. It can cause a mess, and the ink is sometimes an inferior quality that causes deterioration of the printhead over time.

Upgrading Printers

Printers can be upgraded in many ways, and the options available are vendor and printer dependent. The most common upgrades include memory and tray/paper feed options. DIMMs and SO-DIMMs are popular memory options, but some printers have proprietary memory modules. Printer memory is important so that the documents can be sent and stored away from the computer that requested the print job. This frees up the computer's memory and hard drive space to do other tasks.

Paper storage trays and feeders are another common upgrade. Special paper feed options can be purchased that are mounted onto a printer for rolls or different sizes of paper. With the increased popularity of digital photography, these printer options are quite popular.

Printer Maintenance

Maintenance is important for all types of electronics, but printers have maintenance and preventive maintenance requirements that are a bit different than those of other devices. For some printers, preventive maintenance kits are available for purchase. Quality printer replacement parts and preventive maintenance kits are important to a technician. Let's examine the maintenance procedures associated with each printer type.

Impact Printer Maintenance

A technician may be required to do the following maintenance on an impact printer:

- Replace the ribbon (see Figure 9.22).
- Replace the printhead.
- Replace the paper.
- Clear and clean the paper path.

FIGURE 9.22 Impact printer ribbon

You know it is time to **replace the ribbon** when the print output is consistently light. Generic ribbon replacement instructions are to pull straight up on the ribbon to lift it out of the printer. Insert the new ribbon into the grooves in the frame and push downward until it clicks into place.

The time to **replace the printhead** is when the output shows one or more white horizontal lines. When replacing the printer printhead, always follow the manufacturer's instructions. Generic steps to install an impact printer printhead are as follows:

Step 1. Power off the printer and allow the printhead to cool.

Step 2. Press the release lever or button that allows the printhead to be removed.

Step 3. Insert the replacement printhead.

Step 4. Power on the printer and send a sample print job to ensure that the printhead is firing all pins.

To **replace the paper**, simply insert the paper inside the paper tray. If continuous paper or forms are installed, you may be required to clear and clean the paper path. Ensure that the paper aligns properly and evenly to the pins in the continuous (tractor-fed) paper. A sample form may have to be printed to ensure that data is placed in the appropriate form fields.

Impact printers usually require cleaning more often than any other type of printer because they are frequently used for continuously fed paper or multiform paper and are often installed in industrial environments. Paper bits, dust, and dirt cause an insulating layer of heat to form on the printer components, which causes them to fail. It is important to vacuum impact printers more often than other printers as a preventive maintenance task.

Inkjet Printer Maintenance

On inkjet printers, a technician may need to do the following maintenance:

> Replace the cartridge (see Figure 9.23).
> Calibrate colors and printhead alignment.
> Clear paper jams.
> Clean the printhead.
> Replace the printhead.
> Replace or maintain a roller.
> Replace or maintain the feeder.

FIGURE 9.23 Inkjet ink cartridge assembly

You know it is time to **replace an ink cartridge** when the print output is consistently light, a particular color does not print, or a message appears. The generic steps to install an ink cartridge are as follows, but always refer to the manufacturer's directions:

Step 1. Ensure that the printer is powered on.

Step 2. Open the printer cover or door to gain access to the print cartridge assembly. Most printers automatically move the assembly to a place where access is easiest. Give the printer time to complete this process.

Step 3. Release the old print cartridge. There might be a release lever to access the cartridge. Some cartridges require pressing down to eject or simply pulling out, pulling out and then up, or lifting up.

Step 4. Remove the protective tape from the new cartridge. Be careful not to touch any ink nozzles and/or the copper contacts on the cartridge.

Step 5. Insert the new cartridge, reversing the removal procedure.

Step 6. Replace the printer cover or access door.

Step 7. Print a test page.

On most inkjet printers, you have to **calibrate** in order to do a printhead alignment process and adjust colors to ensure quality output. Many inkjet printers come with their own optional software that can be installed to perform this process. Each inkjet printer has a different calibration process, but the generic steps are as follows:

Step 1. Locate the printer in the appropriate Windows Control Panel.

Step 2. Right-click the printer and select *Properties* or *Printer properties*.

Step 3. Locate the calibration function, which is commonly found on a *Tools*, *Maintenance*, or *Advanced* tab.

Step 4. Perform the calibration, which normally involves printing a page and then selecting specific values through another menu. Figure 9.24 shows an example of the calibration or printhead alignment page that is printed as part of the calibration process.

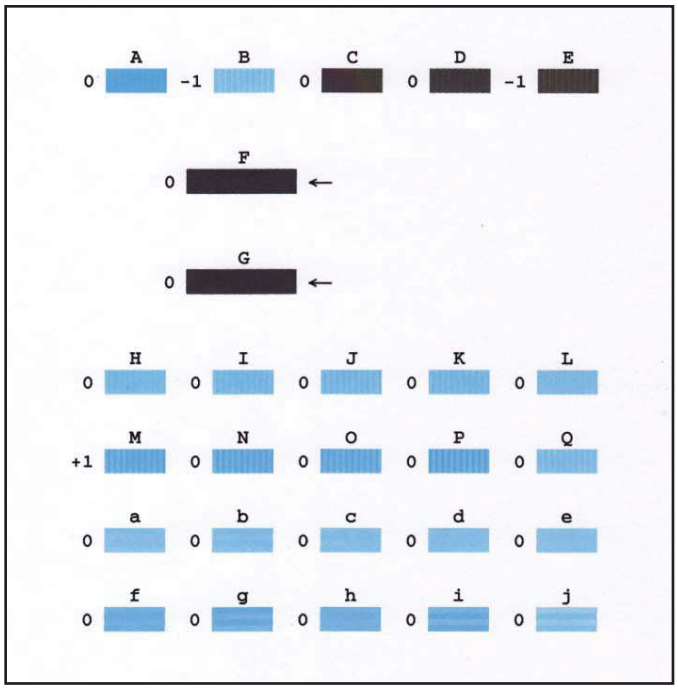


FIGURE 9.24 Sample inkjet printhead/calibration output page

Every printer needs a method to feed paper through, and on an inkjet printer, that involves a paper tray and paper feeder as well as rollers that move the paper along the paper path. Part of maintenance should be inspecting this paper path for debris, especially paper clips, staples, and labels. Then visually inspect all paper path components for wear.

Inkjet printers sometimes have issues with the inkjet rollers. You should clean them using a lint-free cloth or foam swab after you have turned off the printer and removed the paper tray so you can get to the rollers. Use denatured alcohol or a mixture of distilled water and alcohol on the roller. Use a lint-free cloth or dry swab to dry the roller. Sometimes rollers get slick from use and may need to be conditioned or replaced. There are rubber rejuvenator products that can be used to recondition a roller so it grips the paper and sends it through the paper delivery system.

Inkjet printers require little preventive maintenance. Keep the interior and exterior clean of dust and particles. Use a soft brush or nonmetallic vacuum nozzle to remove dust. Do not use any type of lubricants on the print cartridge bar. Use the printer's software or maintenance procedure for aligning the print cartridge each time it is replaced.

Some printers have a "clean" maintenance procedure that can be done through the software that ships with the printer. Some of these processes do not **clean the printhead** well enough, and the printhead may clog with use. In such a case, remove the printhead and clean it with a lint-free cloth or with a dampened cotton swab. Allow the cartridge to dry thoroughly before reinstalling it.

Laser Printer Maintenance

Technicians commonly do maintenance on a laser printer, such as the following:

> Replace the toner cartridge.
> Apply a maintenance kit.
> Perform calibration.
> Clear paper jams.
> Clean the printer.

To **replace the toner cartridge** on a laser printer, refer to the manufacturer's instructions. These are the generic steps:

Step 1. Power off the printer.

Step 2. Access the toner cartridge. This may involve lifting the top cover or opening an access door.

Step 3. Remove the old cartridge by lifting up or sliding forward and then lifting up (see Figure 9.25). If this model has a release tab, press it.

Step 4. If the original covering and bag are available, attach the covering and insert the cartridge inside the bag. Recycle if possible.

Step 5. Remove the new cartridge from the box. Avoid doing this in sunlight. Avoid touching the cartridge drum. Many cartridges have a plastic strip that must be pulled out and thrown away. Remove the protective drum covering.

Step 6. Install the new cartridge and ensure that it snaps securely in place.

Step 7. Close the top cover or access door.

Step 8. Print a test page to ensure that the printer works well.

FIGURE 9.25 Replacing a laser printer cartridge

A **laser printer maintenance kit** is available for some models. The contents of the kit are vendor specific and might include any of the following: separation pad, pickup roller, transfer roller, charge roller, and fuser assembly. Follow the manufacturer's directions for installing a maintenance kit. The separation pad and pickup rollers commonly require removal of an e-clip that holds rollers tightly on a bar. An e-clip looks like the letter C or letter E, as shown in Figure 9.26.

FIGURE 9.26 E-clip

There is a specific tool for removing e-clips, but needle-nose pliers and a small flat-tip screwdriver can work, too. Hold the closed side of the e-clip tightly with the pliers and use the tip of the screwdriver to gently pry the e-clip off the bar.

A common process done at the end of applying a maintenance kit is to reset the **maintenance counter**. This counter is used to count the number of pages until the next time the message to apply the maintenance kit appears again. Usually this counter is reset through the laser printer menu, but some printers require you to press a special button sequence.

TECH TIP

Allow a laser printer to cool

Before working on a laser printer, allow the printer to cool down. Look for warnings where hot components are located.

A laser printer may have software options for cleaning and calibration. The cleaning mode cleans the paper path so that no random specks appear on the output. When you **calibrate** a laser printer, you adjust for print density or how dark the print appears on the page. Cleaning mode and calibration are commonly accessed through the printer menu or from manufacturer-specific software on a PC.

Laser printers do require some periodic maintenance. The list that follows can help:

> Be careful about using compressed air to **clean a laser printer** that has loose toner in it. The compressed air could push the toner into hard-to-reach places or into parts that heat up, causing the parts to fail. Be sure to vacuum laser printer toner before using compressed air inside a laser printer.

> If a transfer corona is used, clean it when replacing the toner cartridge. Some printers include a small cleaning brush for this purpose. Some toner cartridges include a cotton swab. The transfer corona wire is normally in the bottom of the printer, protected by monofilament wires. Be extremely careful not to break the wires or the transfer corona.

TECH TIP

Laser printer preventive maintenance is important

If any toner appears inside a laser printer, do *not* use a normal vacuum cleaner to get it out. Toner particles can seep through the vacuum cleaner bag and into the vacuum's motor, where the particles melt. Also, the toner can become electrically charged and ignite a fire. Special high-efficiency particulate air (HEPA) vacuum bags are available for some computer and/or laser printer vacuum cleaners.

> The fuser cleaning pad, which sits above the top fusing roller, is normally replaced at the same time as the toner cartridge. However, the cleaning pad sometimes becomes dirty before it is time to replace the cartridge. To clean, remove the pad and hold it over a trash can. Use the shaft of a small flat-tipped screwdriver to rub along the felt pad. Reinstall the cleaning pad and wipe the screwdriver with a cloth.

> The fusing roller sometimes has particles cling to it. When the assembly cools, gently scrape the particles from the roller. A small amount of isopropyl alcohol on a soft, lint-free cloth or foam swab or an alcohol pad can help with stubborn spots.

Thermal Printer Maintenance

Maintenance done on a thermal printer commonly involves doing the following tasks:

- Replace the thermal paper.
- Clean the printhead/heating element.
- Remove debris.
- Check the feed assembly.

If a company uses thermal printers, you might be required to **replace the paper**. Look back at Figure 9.13 to see how the paper is threaded through the rollers. Commonly, there are arrows that show you the path or a picture. Ensure that the proper size and type of thermal paper is being used.

You also need to **clean the heating element**. The heating element is part of the printhead, and you can use a thermal printer cleaning pen that contains isopropyl alcohol and a beveled (slanted) edge to reach the heating element. Isopropyl alcohol or premoistened thermal cleaning swabs can be used on both the printhead and the rollers. **Remove debris** inside the printer and use compressed air if needed. It is recommended that with some thermal printers, you use a cleaning card, cleaning file, cleaning pen, or cleaning swabs. Remember to always use proper ESD procedures and to allow the thermal printer to cool before performing preventive maintenance.

Remember that the feed assembly is part of the paper path, and it must be checked and maintained. Turn off the printer and then clean the rollers with a lint-free cloth or foam swab with denatured alcohol or a mixture of distilled water and alcohol. Allow a roller to dry before putting it back in service.

Printer Maintenance Conclusion

Printers are critical to some users. Keeping a printer well maintained and recommending a maintenance routine is part of the job for many technicians. If any type of printer must be sent out for repair, for warranty work, or for some other reason, make sure to remove the toner cartridge, platen knobs, and power cords before packing the printer in a box (or remind the user to do so). Check with the receiving company to see if you should send the toner cartridge separately.

TECH TIP

What if you just performed maintenance on a printer, and now the printing looks bad?

After performing preventive maintenance on a printer, the pages may appear smudged or slightly dirty. Run a few print jobs through the printer to allow the dust to settle (so to speak). Never perform any maintenance on any computer part or peripheral without testing the results.

Printer Installation Overview

A printer is one of the easiest devices to install. Refer to the printer documentation for exact installation and configuration specifics (see Figure 9.27). As with any device, you want to do your homework first by deciding on the **setup location**. Ensure that the location is free from debris and nothing blocks device vents. Then determine if the printer is going to be wired or wireless. If wired, determine if the printer will connect through a USB port or through the wired network. Ensure that you have the proper cable on hand. If the printer is wireless, determine if it will connect via Bluetooth or the Wi-Fi network. Table 9.7 describes some tips for the various connectivity types.

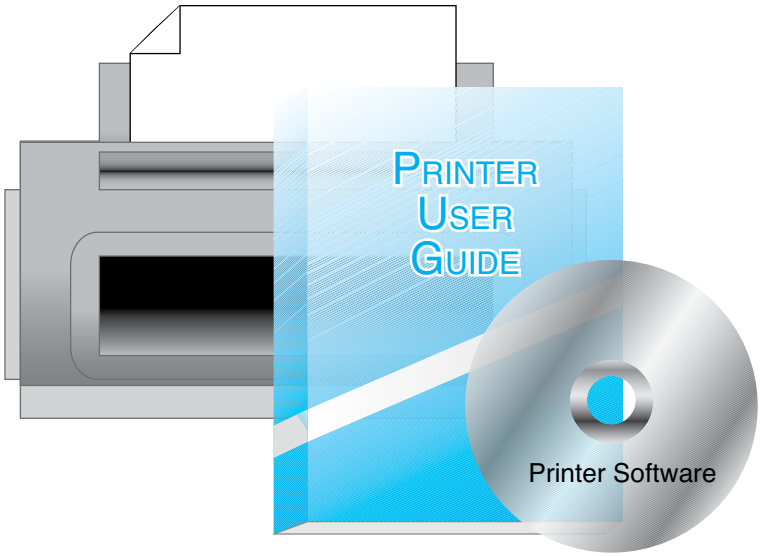


FIGURE 9.27 Printer installation, using software and a manual

TABLE 9.7 Printer device connectivity types

Connectivity type	Notes
USB	If software was installed before attaching the cable, Windows should detect it and automatically start the installation process.
Wired network	To set up a printer on a wired network, use the *Devices >Add a printer or scanner* link. A prompt asks whether the printer is local or networked. A local printer is directly attached to the computer. A networked printer attaches to another computer or directly to the network.
Wireless network	Requires a few details about the wireless network, such as the wireless network name (SSID) and password.
Bluetooth	Bluetooth must be enabled on the computer and on the printer to make it discoverable.

Properly **unbox a printer**, making sure the shipping container is not damaged and documenting if it is. You should also ensure that there are no damaged parts; if there are, you need to document the problem and return the printer. Usually there is a quick start guide that has pictures to tell you what to do, such as remove all tape that holds down the covers, install any print cartridge(s), adjust paper guides to the proper size, insert paper, and, if it is not already attached, attach the power cord to the printer and plug the other end into a wall outlet.

Remember that with Windows, if a printer is not discovered, you can use the *Add a printer or scanner* link found in the *Printers & scanners* Settings option. If the printer does not appear, you can select the link *The printer that I want isn't listed* > *Add a local printer or network printer with manual settings* link > *Next* > *Use an existing port* > select the appropriate port > select the manufacturer and printer model from the list or click the *Have Disk* button to browse to the downloaded file.

If you are unable to install a printer using the manufacturer's instructions, try the following steps:

Step 1. Check the cabling and power.

Step 2. Reread the manufacturer's directions and ensure that they have been followed.

Step 3. Delete the print driver and try the installation again, following the manufacturer's instructions.

Step 4. Download a different print driver and try the installation again.

Step 5. Research the error on the printer manufacturer's website. In some cases, it may be necessary to back up the registry, modify the registry, and restart the print spooler in order to repair this issue.

Be sure to test all functionality. Have the user print from an application. Be sure the printer is the default, if applicable. (This is covered later in the chapter.) Be sure to test the ADF capability, if installed.

Installing Multifunction Devices

A multifunction device (sometimes called an all-in-one printer) connects with a cable or wirelessly the same way as a printer, but it supports printing, scanning, copying, and sometimes faxing. You have to remove protective materials from the scanner glass before using.

Installing a multifunction device is different from installing a printer in that you have more configuration to do. In addition to doing a printer and scanner calibration, you may have to connect the device using a phone cable between the RJ11 port on the device and a phone jack on the wall and configure/test the fax function. Be sure to test all functions.

USB Printer Installation

The following steps explain how to install a printer that attaches to a USB port:

Step 1. Take the printer out of its box and remove the shipping materials. The main reason new printers do not work properly is failure to properly remove all the shipping safeguards. Set it in an appropriate area.

Step 2. Connect the power cord from the printer to a wall outlet, surge protector, or UPS outlet.

Step 3. Load paper and the ribbon, ink, and cartridge into the printer, according to the manufacturer's instructions.

Step 4. Turn on the printer and verify that the power light is on.

Step 5. Install the print driver by following the manufacturer's instructions for the particular operating system being used.

Step 6. Attach the USB cable to the printer and to the computer, as shown in Figure 9.28. Note that this cable might not be provided with the printer.

Step 7. Configure options and default settings.

Step 8. Verify that the operating system recognizes the printer. Perform a test print to verify communication between the computer and the printer. Perform the calibration/printhead alignment procedure.

Step 9. Train the user on printer operation and leave all printer documentation with the customer.

TECH TIP

Educating the user on printer functionality and print cartridges

As part of the installation process, ask the user to print something and show them any unique features. Inform the user that the cartridge that comes with the printer does not last long and to order a new one as soon as possible.

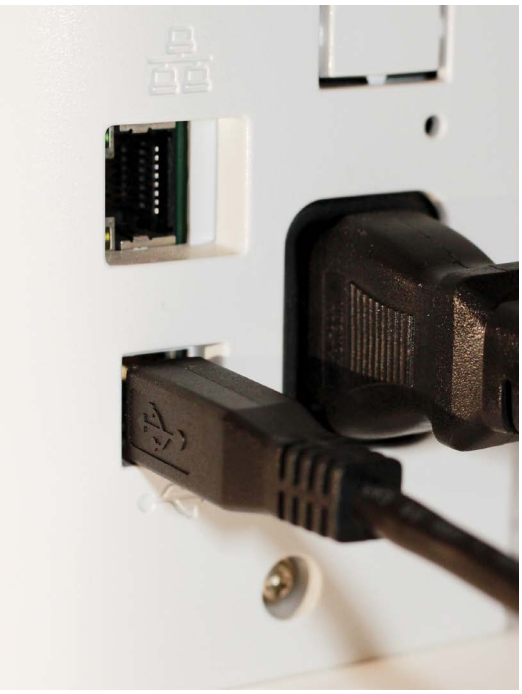


FIGURE 9.28 USB connection to the back of a printer

Printers in the Windows Environment

The operating system plays a big part in controlling a printer. When working in a Windows environment, there are three essential areas for a technician to know (besides knowing how to print): (1) configuration utilities, (2) managing the print driver, and (3) printer settings. Sometimes these areas overlap.

To print in Windows, use one of the following methods:

> Open the file in the appropriate application. Click the *File* menu item and click the *Print* option.
> Drag the file to print to the printer's icon in the *Printers* folder.
> Create a shortcut icon on the desktop for a specific printer and drag the file to that icon.
> Right-click the filename and select the *Print* option.
> Open the file in the appropriate application and press Ctrl+P to bring up the *Print* window.
> Open the file in the appropriate application and click the printer icon located under the menu bar.

TECH TIP

Using the printer icon in the notification area

When a print job occurs, Windows normally shows an icon of a printer in the notification area (the right side of the taskbar). When the print job is still accessible, you can double-click the printer icon, click the document, and pause or cancel the print job by using the *Documents* menu option.

You can use the Windows *Printers & scanners* Settings link to add a printer, remove a printer, temporarily halt a print job (that is, pause the printer), and define or change printer settings, such as resolution, paper type, and paper orientation. Note that you can also use the *Devices and Printers* Control Panel to add a printer. After the wizard starts, you must select whether the printer is a local

printer (used by only one computer) or a network printer. If the local printer option is selected, you have to install a print driver. (Device sharing and networking printers are covered later in this chapter.) For best performance, always use the latest driver from the printer manufacturer for the operating system installed.

A **default printer** is a printer that applications use without any configuration changes. Even if you reply *No* to this prompt, you can change a printer to the default printer at a later date. Using the *Settings* > *Devices* > *Printers & scanners* link allows you to select a specific printer icon > *Manage* and gives you access to the *Printer properties* link. In this window, several tabs are available, depending on the printer model. Common tabs include *General*, *Sharing*, *Ports*, and *Advanced*. Figure 9.29 shows an example of this window. Notice that the *General* tab has a *Print Test Page* button that can be used to test connectivity between the computer and the printer, and the test can be used to ensure that the print driver is working.

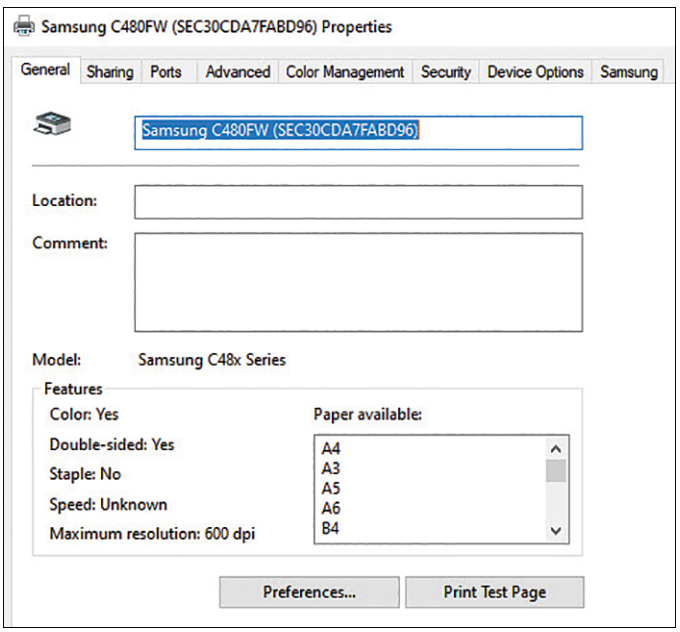


FIGURE 9.29 Printer properties window

TECH TIP

Setting a printer as the default printer

Click on the printer > *Manage* > *Set as default*. The default printer has a check mark next to the printer icon.

A specific printer's *Printer properties* window contains useful tools and settings. Table 9.8 lists the common tabs and their general purposes.

TABLE 9.8 Printer Properties window tabs

Tab	Description
General	Displays the printer name and has a button for printing a test page
Sharing	Shares the printer over a network
Ports	Sets the LPT port number or displays the current port

Tab	Description
Advanced	Allows setting of resolution, graphics intensity (darkness), graphics mode, spooling (transmission delay), and defaults
Maintenance	Printer type dependent; contains links to various maintenance functions, including cleaning, calibration, printhead alignment, nozzle check, roller cleaning, and quiet mode
Fonts	Displays and installs printer fonts
Device Options	Adjusts print density and quality, displays the amount of RAM installed in the printer, and adjusts printer memory tracking

TECH TIP

***Print Test Page* button on the Printer properties window *General* tab**

The *General* tab is normally where you find a button that forces communication between the PC and the printer to be tested with a test page printed output.

TECH TIP

I want my print job now!

If multiple print jobs are in the printer queue, some printers allow you to reorder them by right-clicking on a document and selecting *Properties*. On the *General* tab, change the priority. Commonly, a lower number, such as 1, indicates a higher priority.

How an application outputs to a printer is determined by the operating system used. A **print driver**, or printer driver, is a piece of software specifically written for a particular printer for a specific operating system. If you upgrade the operating system or move the printer to a different computer, a different print driver is required. The print driver enables the printer's specific features and allows an application to communicate with the printer via the operating system. Windows applications use one print driver per printer. If you have two printers attached, two print drivers have to be installed.

TECH TIP

Using the latest print driver

For best results and performance, use the manufacturer-provided driver that is designed for the operating system being used.

The print driver and software from the printer manufacturer provide customizable configuration settings for a particular operating system. These settings can be accessed by right-clicking on the printer within the *Printers & scanners* Settings link, selecting the printer > *Manage* and selecting *Printing Preferences*. Commonly used configuration settings include the following:

> **Orientation (see Figure 9.30):** The **orientation** is the vertical or horizontal presentation of the document. Portrait orientation is taller than it is wide, and landscape is wider than it is tall.

> **Duplex (see Figure 9.30):** **Duplex** is also known as double-sided printing. Note that the printer featured in Figure 9.30 does not have a duplexer assembly, so printing on two sides would require turning the paper over and sending it back through the printer.

> **Collate:** The collation setting affects the order in which the pages are printed when multiple copies of a multipage document are being made. For example, if you want to make three copies of a 10-page document, with collation enabled, you would get the first copy of the 10-page document, then the second copy, and finally the third copy. Without collation enabled, you would get three copies of the first page, three copies of the second page, and so on.

> **Quality (see Figure 9.31):** The **quality** setting controls the resolution (DPI for example) and amount of ink/toner used.

> **Tray settings:** The **tray settings**, which may be under the *Paper/Quality* or *Paper* tab, include different paper sizes, percentage output, tray switching, and tray priorities.

> **Paper source:** This setting controls where the printer pulls the paper. The printer may have an Auto Select or Automatically Select function and use paper from the appropriate source based on the paper size chosen within the document. Otherwise, you can select a specific tray that is to be used by default.

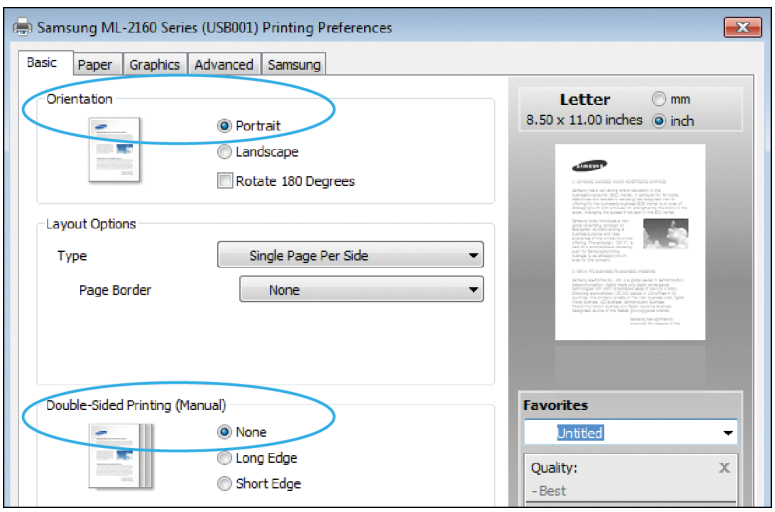


FIGURE 9.30 Printer orientation and duplex settings

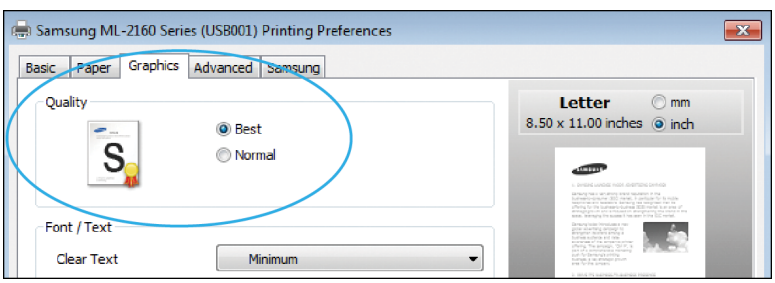


FIGURE 9.31 Printer print quality option

Each printer has its own Page Description Language (**PDL**) that is a translator between the computer and the printer. The PDL handles the overall page look and has commands that treat the entire document as a single graphic. The two most popular page description languages are Adobe Systems Inc.'s **PostScript** and Hewlett-Packard's Printer Control Language (**PCL**). Both are used by printer manufacturers. PCL uses the printer hardware to do the translation, which speeds up the printing process no matter which operating system you are using. The drawback to using a PCL printer is that when you print the document on a different PCL printer, the quality may not be

the same. In contrast, PostScript provides higher-quality output even if printed on two PostScript printers. Note that when *Auto* is selected for the printer language, the printer switches to the most appropriate printer language, depending on the type of information in the document.

TECH TIP

Which driver should I use, PostScript or PCL?

Some manufacturers may provide both a PCL driver and a PostScript driver. If the user does mostly word processing or spreadsheets, then use the PCL driver. If they print graphics and need higher-quality output, then the PostScript driver will serve them better.

A printer accepts as much data as possible from a computer, processes that data, outputs it, communicates to the computer the need for more data, accepts more data, and repeats the process. With Windows, a print spooler is used. A **print spooler**, or print manager, is a software program that intercepts an application's request to print. Instead of going directly to the printer, the data goes on the hard drive. A print spooler allows multiple print jobs to be queued on the hard drive so that other work can be performed while the printer prints. A printer may come with its own print manager that replaces the Windows print spooler.

If you select *Printer properties* for a particular printer, you can control the print spooler from the *Advanced* tab, as shown in Figure 9.32.

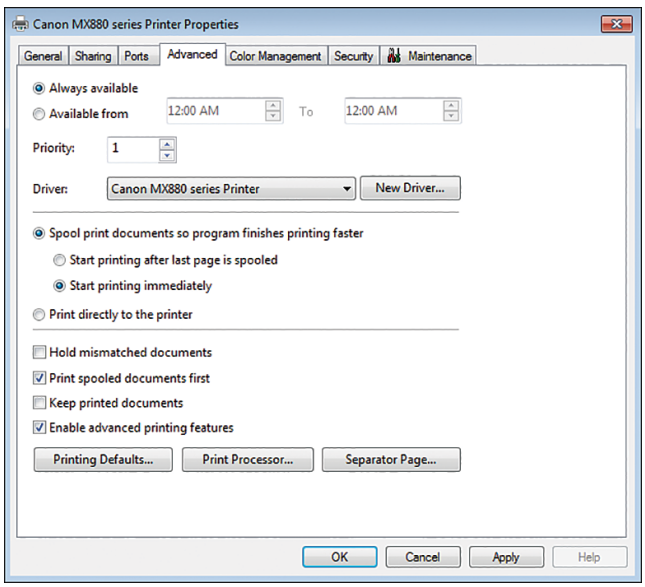


FIGURE 9.32 Spooling settings

A print spooler runs as a service in Windows and relies on another service, called the Remote Procedure Call (RPC) service, and, optionally, the HTTP service in order to operate. To verify whether the services are running, type `services.msc` at a command prompt or in the search textbox to ensure that the services are running. Note that if a printer is shared for use by other computers, spooling must be enabled.

TECH TIP

When not to use spooling

If you have less than 300 MB of hard drive space, turn off spooling because the system needs the free drive space to operate. Remove files from the hard drive and clean up if possible or add more storage so spooling can be re-enabled.

Printer Sharing

Many home users and almost all businesses use printing device sharing (that is, printers that can be used by more than one computer). Printers can be shared using the following methods:

- Connect a printer to a USB port on a computer that is connected to the wired or wireless network and share the printer.
- Connect a printer with a wired or wireless NIC directly on the network. The network Server Message Block (**SMB**) protocol is used to send a print job directly to a network printer (or other network devices). Some printers can be upgraded to have a wired or wireless network port added to them. Figure 9.33 shows a module that can be inserted into a printer so that the Ethernet port connects the printer to a wired network.
- Set up a computer or device that is designated as a print server. Connect the printer to the print server. Connect the print server to the network.
- Use public/shared devices.

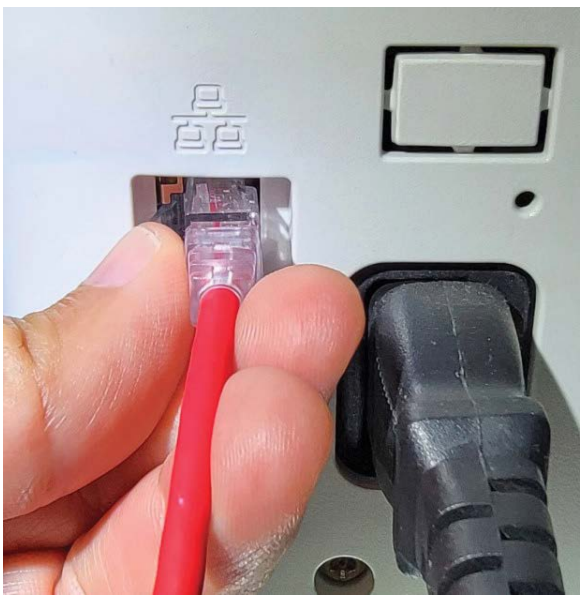


FIGURE 9.33 Printer with a wired network port

A networked printer can reduce costs. Laser printers can be expensive—especially ones that produce high-speed, high-volume, high-quality color output. Buying one printer and allowing users to access it from their individual desktops, laptops, and mobile devices can be cost-effective. It also reduces the amount of office or home space needed. Network printing is a viable alternative to using a computer's USB port. Wired printers can connect to a computer and then be shared or can connect to a wired network so that everyone on the network can use the printer.

Sharing Through Windows

To share a workstation-connected printer across the network, follow these steps:

Step 1. Enable *File and Print Sharing* by selecting the *Network and Sharing Center* Control Panel > *Change advanced sharing settings* > expand the current network profile > *Turn On file and printer sharing* > *Save changes* (see Figure 9.34). You can also use the *Advanced sharing settings* Windows Settings option to turn on file and printer sharing, as shown in Figure 9.35.

Step 2. To share a directly connected printer so others can access it, right-click the printer to be shared > *Properties* (or possibly *Printer properties*) > *Sharing* tab > enable (select) the *Share this printer* option so it is checked > in the *Share name* textbox, type a name for the printer > *OK* (see Figure 9.36).

Notice in Figure 9.36 that you can install additional drivers for other Windows operating systems so that when other computers access this shared printer, they do not have to download and install the driver for this printer. Note that the shared printer must stay powered on, as must the computer to which it attaches, in order for print jobs sent from other devices to be processed.

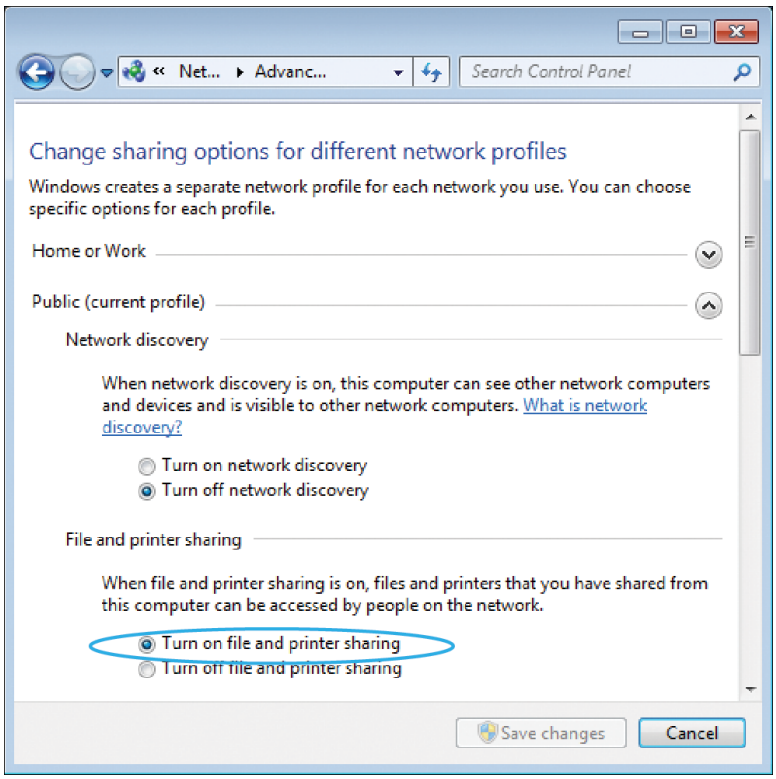


FIGURE 9.34 Enable print sharing using a control panel

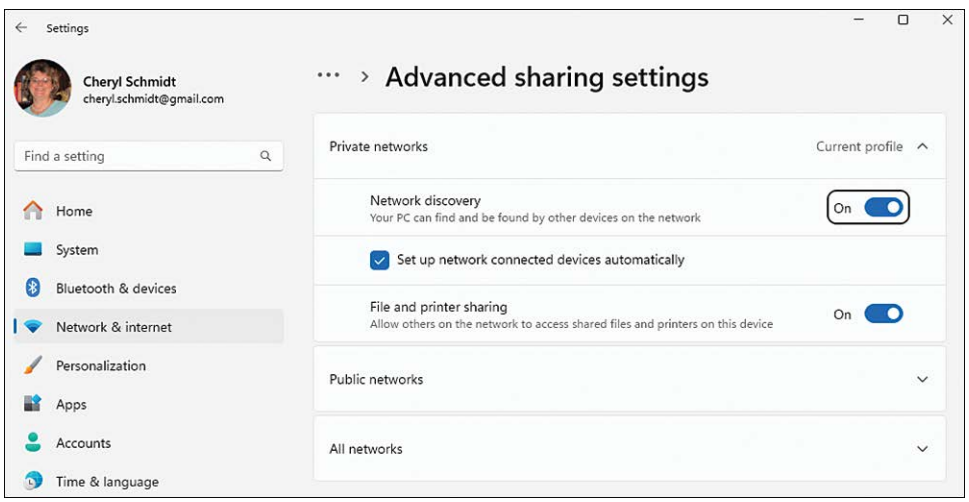


FIGURE 9.35 Enable print sharing using Windows Settings

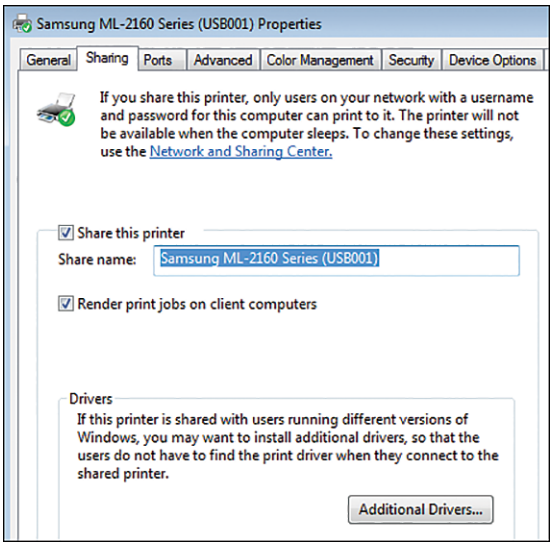


FIGURE 9.36 Printer Sharing tab

Wireless Printers

A PC can use different methods to connect wirelessly to a printer:

- The printer can have an 802.11 wireless NIC installed, or the NIC can attach to a USB port.
- The printer can have integrated Bluetooth capabilities or a Bluetooth adapter attached via a USB port.
- The wireless printer can communicate directly with another wireless device.
- The print server to which the printer connects can have wireless capabilities, and wireless PCs and devices can connect to the printer through the print server (as discussed in the next section).

Printers with wireless capabilities are common. Refer to Chapters 13, "Networking," and 14, "Introduction to Operating Systems," for more information on wireless networking theory and issues related to installing wireless devices.

An 802.11 wireless network has an 802.11 access point or combination access point and router that coordinates communication between all devices on the wireless network, including the wireless printer, as shown in Figure 9.37.

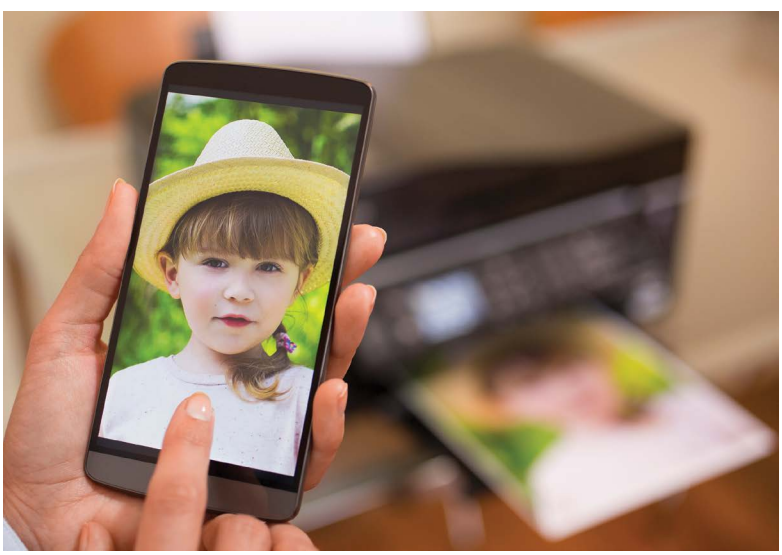


FIGURE 9.37 Wireless printing

TECH TIP

Doing your wireless homework

When installing an 802.11 wireless network printer, obtain the SSID and security information before starting the installation.

There are different types of 802.11 networks (a, b, g, n, ac, and ax). Each type has its own frequency and rules of operation. The wireless NICs in all the devices on a wireless network must be of compatible types. (See Chapter 13 for more information on wireless types and obtaining a network IP address.)

The steps for installing a wireless printer are similar to the steps for installing a wired network printer once the printer is attached to the wireless network. Before installing a wireless printer, you need to ensure that a functional wireless network is in the area. You need to know the SSID and any security settings configured on the wireless network. Normally, you can configure wireless printers using one of the following methods:

> Install software that comes with the printer *before* connecting the printer. Then use the software to enter the wireless network SSID and optional security parameters.
> Use the controls on the front panel of the printer to configure the wireless settings.
> Use a USB connection to the printer until the wireless network configuration options are entered.

Some Bluetooth printers are configured by first connecting them via USB and then configuring the Bluetooth option. To install a Bluetooth printer, follow the manufacturer's directions. These are the generic steps:

Step 1. Install the print driver for the operating system version being used.

Step 2. Ensure that Bluetooth is enabled on the computer or mobile device.

Step 3. Ensure that Bluetooth is enabled on the printer (usually through a front panel control). Note that you may have to set the visibility option to *Visible to All*.

Step 4. If in Windows, use the *Settings* > *Devices* > *Bluetooth & other devices* link to access the *Add Bluetooth or other devices* link. On a device, something may have to be tapped or pushed in order to start pairing with the Bluetooth printer.

Step 5. Ensure that the two devices pair properly and that the print function works.

Print Server

A **print server** connects to a network and allows any computer that is also connected to a network to print to it if the networks are the same or connected to one another. Some print servers can handle both wired and wireless connections. In such a case, the print server attaches to a network switch, and a network wireless router or wireless access point attaches to the same switch. Any PCs (wired or wireless) can print to the printer that attaches to the print server. Figure 9.38 illustrates this concept.

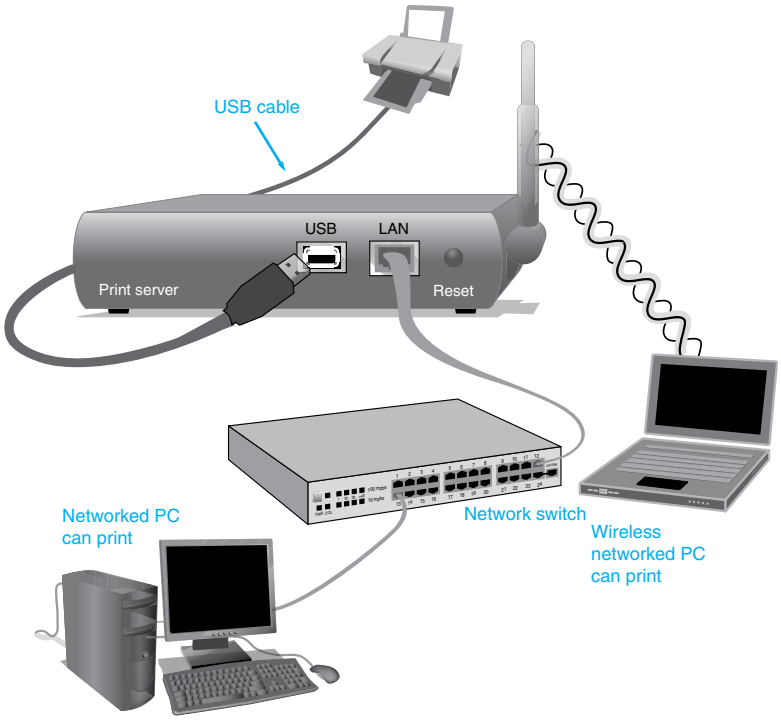


FIGURE 9.38 Wireless and wired print server connectivity

Accessing a Network, Wireless, or Bluetooth Printer

To access a networked printer, use the Windows *Settings* > *Devices* > *Printers and scanners* > *Add a printer or scanner* > *The printer that I want isn't listed* link. These are some of the available options (see Figure 9.39):

- Use the *My printer is a little older. Help me find it.* Option.
- Browse for a network printer.
- Type the path to the printer.
- Enter the IP address or printer hostname.
- Add a Bluetooth, wireless, or network-discoverable printer.
- Manually add a printer.

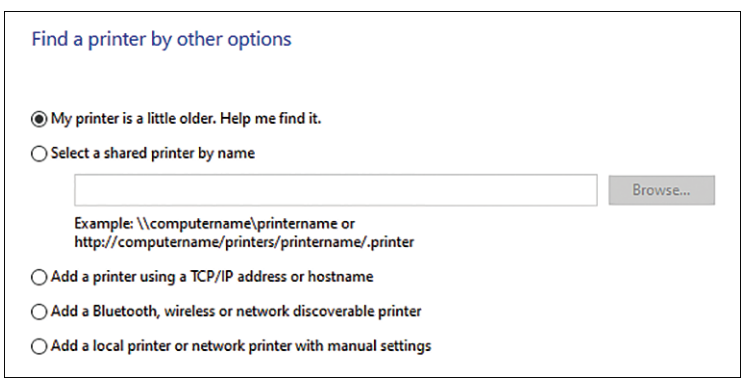


FIGURE 9.39 Finding a shared printer

An older PC can be used as a software print server so that it does nothing except handle print jobs sent to the printer attached to the PC. Software such as Apple's AirPrint or Bonjour can also

be used to create a print server. AirPrint is provided with macOS devices and can be used to print to any AirPrint printer without downloading device drivers. Bonjour allows Apple and Windows devices to share printers without any configuration. (See Chapter 13 for more information on configuring network devices.)

Cloud Printing/Scanning

What if a company wants to be able to print something in a remote location or if a user is on a wired computer and wants to print to a wireless printer? Other companies might want users to be able to scan a document and store it so others can retrieve or view that document. **Cloud services** support network scanning and retrieval as well as printing to remote devices, whether the user connects to the network where the printer is located or not. Some all-in-one devices support scanning or printing directly to an online cloud storage provider or emailing a copy directly to someone, as do some copiers.

Cloud printing/scanning can be done through a service provided by the device manufacturer or through a provider such as Google. People already access email, files, music, and other devices by using the cloud, so it makes sense that an app can allow a print job or scanned document to do the same. Figure 9.40 shows how a document or a photo can be printed from a cell phone if cloud printing is enabled.

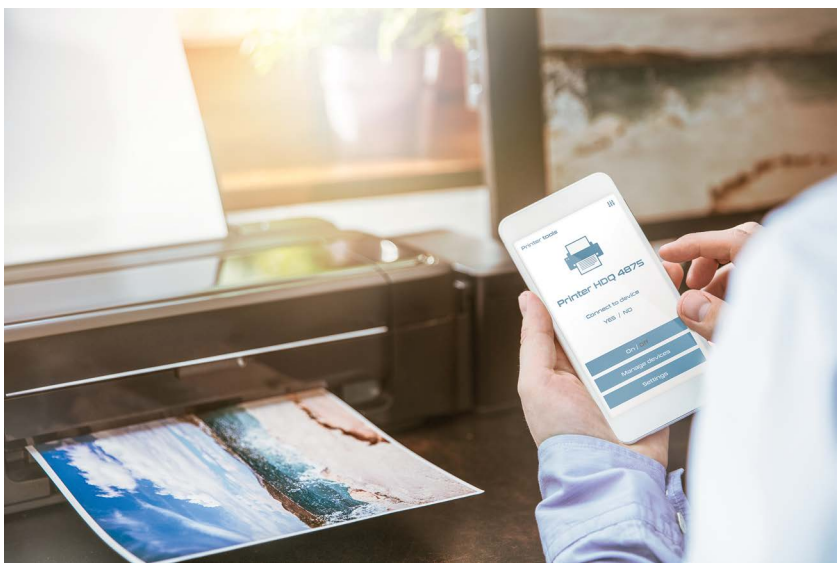


FIGURE 9.40 Cloud printing

You can also scan and have the scan sent to someone's email address or to a network folder that can be accessed by others. Every all-in-one printer is different, but look for the option to scan and send or email, and you will be allowed to enter an email address. Once the scan begins, it is not saved locally on the computer but sent through the network to the email address specified. (See Chapter 13 for information on how to configure an all-in-one device or networked scanner for this feature.)

Printing/Scanning Data Privacy

A printer can be a security weakness in a corporate environment. People might leave printouts on a printer, unauthorized users might use a copier or printer, and hackers use access to networked printers as a way to gain access to other network devices. One way to protect a printer that connects to the network is to require **user authentication** and require the user to input a user ID and password, input

a PIN, or use **badging** as an access control method, where the user scans their ID in order to print. Someone in the company should periodically check **audit logs** as a security measure.

Another option might be to use **secure print**, which might be a security option on a networked printer, copier, or all-in-one unit from within the *Printer properties* > *Printing options*, *Output method*, or other drop-down menu. Select *Secure Print* from the job type or other menu. Commonly you are required to enter a passcode and that same passcode is used in order to get the printout(s) from the printer.

Technicians need to be aware of the drawbacks to printing to a shared, public, or cloud-based printer:

- When printers are shared through a PC, that PC must be powered on at all times.
- Sharing a printer through a PC means that print jobs are spooled to the PC hard drive (hard drive caching). If someone sends an inappropriate print job or prints something that is sensitive corporate information, a technician must realize that the spooled data can be recovered even after the print job completes.
- Privacy can be an issue. For printers shared wirelessly, it may be necessary to give the wireless network password to anyone who wants to print. Printers involved in cloud-based printing require a user to authenticate and register with the app vendor.

General Printer Troubleshooting

The printing hardware subsystem consists of the printer, cable, and communications port. If something is wrong with the hardware, the problem is normally in one of these three areas. Always check the connections and the power between the areas. The printer has the highest failure rate of the three because it is a mechanical device with motors, plastic gears, rollers, and moving parts.

Printer firmware is software inside the printer that can be updated to fix software/app problems, increase security, or update features. Printer firmware updates can normally be obtained from the printer manufacturer's website.

Some printers beep or have indicator lights. If an error code or message appears on the front panel, refer to the manual or online documentation. Figure 9.41 shows that one particular printer has indications for power, paper out, and low ink.

FIGURE 9.41 Printer indicator lights

A printer normally has a self-test routine. Refer to the printer's documentation to determine how to run the test. If a printer's self-test operates properly, the printer is operational. In this case, any remaining print problem has to do with the port, cable, or software.

Running the self-test from the computer shows that printer connectivity works (that is, the computer can issue a command to the printer, and the printer gets it). The self-test is commonly run from the printer's *Properties* or *Printer properties* option from the *Printers & scanners* Windows *Settings* link. Access the *General* tab > *Print test page* button (refer to Figure 9.29).

TECH TIP

The paper is not feeding

If a printer is having trouble with the **paper not feeding**, you should look to see how far the paper went along the paper path before it jammed or could not go any farther. Check the quality of the paper and the efficiency of the rubber rollers that move the paper along the paper path. Over time, rollers can become slick from use and stop working properly.

If a printer makes a **grinding noise** or has **paper jams**, ensure that there is paper in the paper tray. Then, once you have powered off the printer, look for paper bits or misfed paper along the paper path. Check for paper clips or staples that might have been accidentally fed into the printer and gotten lost somewhere along the paper path. Also check for labels that might have loosened and bunched, causing a jam. Sometimes fixing a jam is simply a matter of pulling gently backward on the paper from the paper tray (although it is always best to try to take the paper through the natural direction of the paper path), fanning through the paper in the paper tray to loosen one piece of paper from the others, or pulling the paper the rest of the way through the paper path. Do not tug; do not tear paper, if possible, as doing so will make fixing the jam more difficult for you. Needle-nose pliers and tweezers are great tools for stuck paper. The grinding noise might also be gears located inside a toner cartridge. Replace the cartridge to verify.

TECH TIP

What to do when there is a line down the printed page

If there is a **line down the printed pages**, check the printhead (on impact, thermal, and inkjet printers). Verify the ink levels in an inkjet printer. Check the rollers and look for debris along the paper path. Check the drum on a laser printer.

If using an ADF and the paper doesn't feed or if you have a **multipage misfeed**, check the paper path through the ADF for a foreign object, something stuck to the rollers, slick rollers, the paper guides being the correct width, and a forgotten piece of paper on the scanner glass. For a multipage misfeed coming from a paper tray, fan the paper thoroughly. Check for damp paper.

If the printer will not print, check the following:

> If the printer attaches to a computer, see if any message appears on the computer.
> See if any message appears on the printer's front panel.
> Ensure that the printer has ink or toner and paper.
> Check **connectivity issues**, determine whether the correct printer is selected and configured for the correct port (in the *Printer properties* window). Check the cabling. If the printer is networked, ensure that the wired or wireless network is available. If a printer has worked on the wireless network before, re-associate with the wireless network. Wired network connectivity problems could relate to the cable being attached, the network infrastructure (jacks and cabling to connect to a switch), or network sharing. See Chapter 13 for more information on network printer connectivity.

TECH TIP

The paper could be the culprit

If a printer has trouble feeding paper, ensure that you're using the correct type of paper. Many paper jams are due to inferior paper quality, paper damage due to humidity, or operator-related problems such as the **incorrect paper size** selected in the software program (see Figure 9.42).

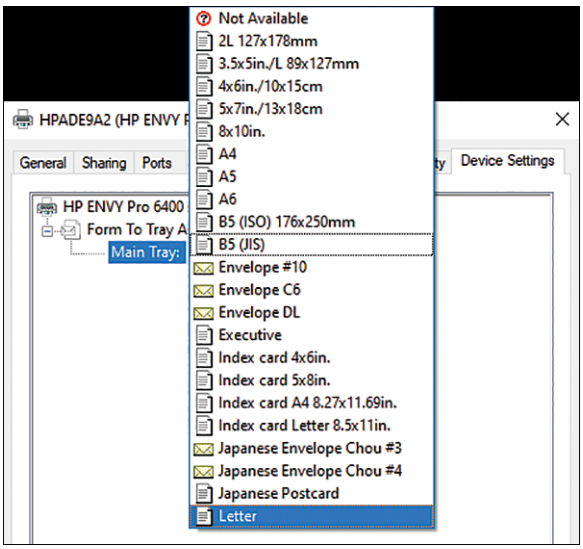


FIGURE 9.42 Printer paper size options

Some issues are due to the user selecting the wrong paper tray. You must select the appropriate paper tray for the paper size you want. If you see a **tray not recognized** error, re-insert the tray securely. Check the paper size settings and look for paper jams along the paper path.

If there is no image on the printer display, check that the printer is powered on. Also check the wall outlet by plugging a known working device into the same outlet; if applicable, check the power strip. The printer power brick could be faulty.

TECH TIP

Mixed-up output

If you see **garbled print** on the output, check the cable and then the print driver.

If a printer gives a "paper out" message (see Figure 9.43), but the paper is installed in the printer, check the paper sensor. Sometimes this sensor is an optical sensor, and sometimes it is a plastic piece that flips out. Take out the paper and reinsert it. Ensure that there is no blockage and that the sensor is not sticking (that is, not flipping out properly). Dust and debris can cause both blockage and sensor sticking.

TECH TIP

Faded or totally missing print

When the print output is **faded print** or blank, check the ribbon (in impact and thermal printers), ink levels (in inkjet printers), or toner (in laser printers). Check the quality setting. In a thermal printer, reduce the printhead energy or printhead pressure setting; ensure that the ribbon and media are compatible. Check the print driver as you may have to roll back the driver in Device Manager if a Windows update has just occurred.

FIGURE 9.43 Printer front panel message

If the printer outputs creased paper, check the following:

> Ensure that the paper guides in the paper tray are set to the correct size and do not push too tightly against the paper.
> Fan the paper before printing.
> Ensure that the paper being used meets the printer manufacturer's specifications.
> Check for **staple jams** and jams due to using paper that has been **hole punched** or the paper bits/dust from hole-punched paper. Check rollers and look all along the paper path for a stray staple. Gently pry out any staple found.
> Check the paper path for obstructions, such as a label or paper clip.

TECH TIP

What to do with slick printer rollers

Special rubber cleaners/rejuvenators are available for rubber printer rollers that have a hard time picking up paper and sending it through the printer. Some printers have a special cleaning page for cleaning rollers. If a cleaner page is unavailable, use a wire brush, sandpaper, or the sharp edge of a paper clip to roughen up the rollers a bit, which will enable them to pick up the paper better. Vacuum all debris before using the printer.

A printer may not have enough memory and may display a low memory message or just blink as if it is accepting data. Then the printer quits blinking, and nothing appears or the printer prints only half of the page. This issue could also be caused by insufficient free hard drive space when spooling is enabled.

TECH TIP

What if a printer needs more memory?

Alternatives to adding memory are to send fewer pages of the print job at one time, reduce the printer resolution, reduce the size of the graphics, or standardize the fonts (by not using as many font types, styles, or font sizes). Also, try freeing up drive space on the computer that is being used to send the print job.

USB-Attached Printer Troubleshooting

If a printer that uses a USB port is displaying problems, consult the following list of troubleshooting options:

- If the computer stops responding and the USB device is suspect, power off the device and then turn it back on again. Go into *Device Manager* and ensure that there is only one listing for the USB printer.
- The BIOS/UEFI settings may have to be enabled for USB devices. Different BIOS/UEFI manufacturers list the USB settings differently, such as *Enabling Onboard USB* or within the PCI section.
- Use *Device Manager* to check whether USB is listed. Look at the *Universal Serial Bus Controllers* section. If USB is not listed, check the BIOS/UEFI settings or update the BIOS. If the USB device is listed, ensure that there are no resource conflicts.
- If there is a USB hub connected to the USB port, disconnect the hub and connect the USB printer directly to the USB port to see if the hub is the problem.
- Disconnect the USB printer while the computer is powered on. Power down the computer. Then power on the computer. Insert the USB printer cable into the USB port. The system should automatically detect and install the printer.
- Verify that the USB device works by plugging it into another USB port or another computer's USB port.
- Check that the proper USB cable is being used.

On the software side, troubleshooting involves narrowing down the problem to the print driver. Because Windows uses one print driver for a specific printer within all applications, check the printing from within several software packages. Use a simple text program such as Notepad to see if simple text will print. Printers need memory to print multiple pages of complex graphics. If a printer prints a couple pages and then stops, or if it prints half a page, ejects the paper, and then prints the other half of the page and ejects the paper, free up hard drive space. If printing does not occur in all the software packages tested, the problem is most likely the software driver. See the next section for specific Windows printer troubleshooting tips.

Windows Printer Troubleshooting

The most common printing test is a test page from an application or from a specific printer's *Properties* or *Printer properties* window, using the *General* tab. Remember that Windows uses a single print driver for all applications. Windows has a troubleshooting tool that you use by searching for `troubleshoot printer` and selecting the *Find and fix problems with printing* link. If the Windows troubleshooting tool does not help, run a self-test on your printer by following the manufacturer's directions. If the self-test works, the printer is likely fine, and the problem lies in the cable, port, software driver, or printer settings.

TECH TIP

Print from Notepad

If a printer self-test works, try printing from Notepad. If the file prints, your problem may be a print problem that affects only one application, or the printer may not have enough memory for complex output, such as high-end graphics.

Free hard drive space is important for print spooling. Insufficient free space can cause problems with print jobs. Even if there appears to be enough hard drive space to spool a print job, the printer may still need more RAM installed to print a large or complex document.

A print spooler and/or associated services, such as RPC and HTTP, can cause problems and can be stopped or paused. Locate the Print Spooler, RPC, or HTTP service used by the printer (by typing `services.msc`). Right-click on the service and select *Properties*. In the window that appears, you can start, stop, pause, or resume a service. Figure 9.44 shows the Print Spooler Properties window. Because the service is started automatically, the only button currently available is Stop. If the printer works, then you know the printer, port, and printer cable are all operational, and the problem is in the operating system.

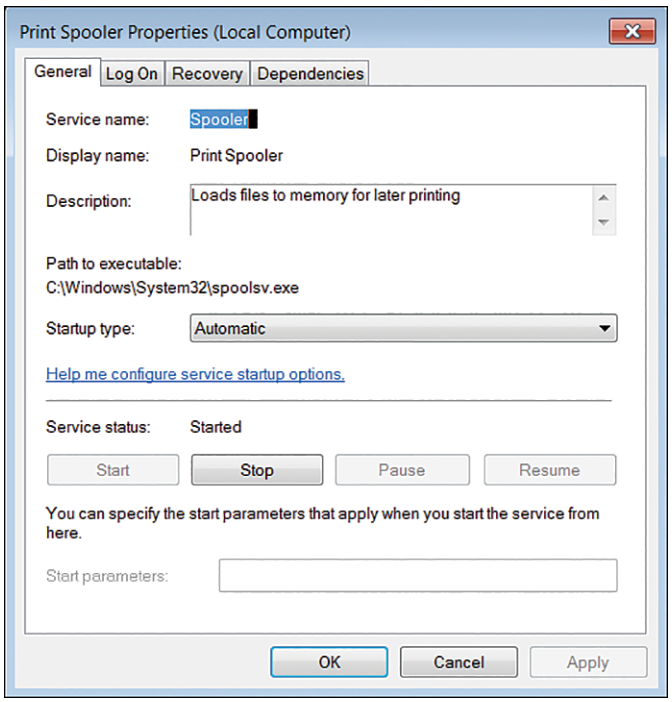


FIGURE 9.44 Managing the Print Spooler service

The print queue sometimes causes problems. A single document may be in the queue but not print for some reason, causing other print jobs added later to fail to print. Check the print queue to see if there are **multiple print jobs pending** in the queue. Multiple failed print jobs indicate a problem with the printer, such as a paper jam or lack of paper, being out of ink/toner, and so on. Check the printer's front panel to see if it indicates any errors.

After a problem is rectified or if you have a **frozen print queue** (that is, no print jobs are getting through), the print queue might need to be cleared. Depending on what rights the user has, sometimes a technician must clear the print queue. The following methods can be used:

> Open the *Printers & scanners* Windows Settings option. Right-click the specific printer icon > *Open*. Right-click the first document (the one that is causing the problem) > *Cancel*. To cancel all print jobs, select *Cancel All Documents* from the *Printer* menu option.

> If the print job has already gone to the printer and is no longer stored on the hard drive, you may not be able to use the first method. In this case, use the *Printer* menu or *Cancel* function on the printer to cancel the print job.

> Clear and restart the Print Spooler service. Note that you may have to delete all the files in the \Windows\System32\spool\PRINTERS folder and then restart the Print Spooler service.

> Turn off the printer and then turn it back on again.

If you get an access denied message, it means you must be logged on as an administrator to control the print queue. If a user gets the access denied message, the user account must be added to the printer. Access *Printer properties* > *Security* tab > add the user account.

If you reload a printer driver, the old version of the printer driver must be removed first. Some manufacturers have specific instructions for removing their drivers. Always follow their directions. Most of them say to do something similar to the following: Right-click the specific printer icon and click the *Delete* option. Click the *Yes* button when prompted if all the associated printer files are to be deleted. To reinstall the printer, use the *Add Printer Wizard*.

You can use Windows Event Viewer to both set up and check the print audit log (sometimes called a print log). Access *Event Viewer* > expand *Applications and Services* > expand *Microsoft* > expand *Windows* > expand *Print Service* > right-click on *Operational* > *Enable Log*. Return to this same area to view information related to printing problems.

Another Windows problem relates to setting the correct paper size. Changing the Windows *Region* setting affects the default paper size. Change the setting back by using the *Printer properties* link. The tab chosen is vendor dependent. Look back to Figure 9.42 to see an example of the various paper size options.

Another option available through the *Printer properties* link that can cause a problem is having the **incorrect orientation**. The two choices are landscape and portrait. Portrait prints the page with the long two choices are landscape and portrait. Portrait prints the page with the long side of the paper on the left, whereas landscape prints the page with the long side of the paper across the top. Figure 9.45 shows how the *Preferences* button is commonly used to access the paper orientation.

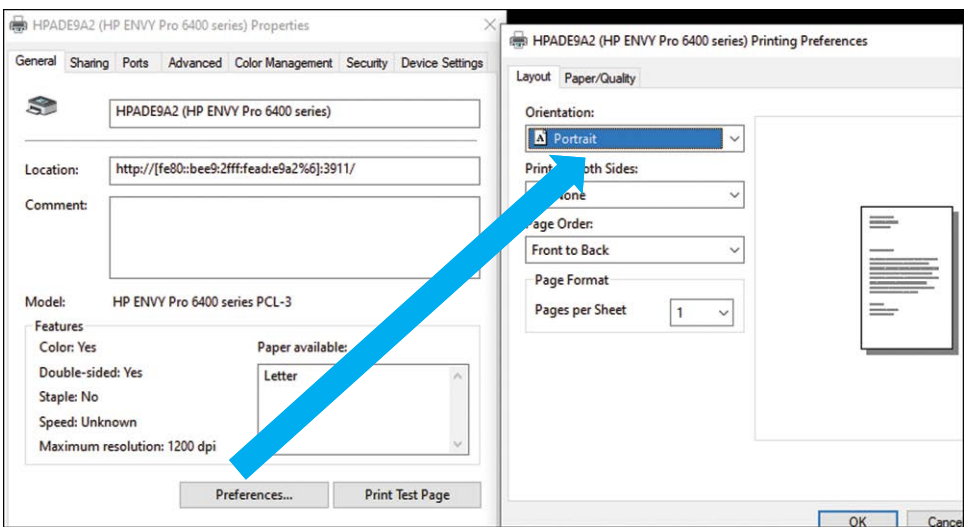


FIGURE 9.45 Printer Preferences > Orientation

If you are having trouble sharing a printer, ensure that Windows Defender Firewall is not blocking printer sharing. If another vendor's firewall is in use, follow directions from that vendor. Take these steps if Windows Defender Firewall is being used:

Step 1. Open the *Windows Firewall* Control Panel or *Windows Defender Firewall* Settings option.

Step 2. Select the *Allow an app or feature through Windows Defender Firewall* link.

Step 3. Locate the *File and printer sharing* option and make sure it is enabled. Click *OK*.

TECH TIP

Network printers

If a printer can be seen on the network but cannot be printed to, verify that the printer is on and shows no error conditions on the front panel or LEDs. Print a test page using the front panel menu, if possible. Verify that the network printer has a static IP address and is not configured for DHCP. (These concepts are covered in Chapter 13.)

Impact Printer Troubleshooting

When technicians state that a printhead is not firing, this means that one or more of the print wires are not coming out of the printhead to impact the ribbon. A printhead that is not firing is evidenced by one or more white lines appearing where the printed dots should be. On a printed page, the white line appears horizontally in the middle of a single printed line. The most likely problem is the printhead. However, the problem could be a bad driver transistor on the main circuit board or a loose printhead cable. However, because the printhead is a mechanical part, it is the most suspect.

If the print is light and then dark, the printer ribbon may not be advancing properly. One of the shafts that insert into each end of the ribbon may not be turning, or the set of gears under the shaft may not mesh properly. Also, there is a motor that handles ribbon movement, and it may need to be replaced. A faulty ribbon can also cause the carriage to seize up. Remove the ribbon and power up the printer. If the carriage moves when the ribbon is removed, but it will not move when the ribbon is installed, replace the ribbon. Some printers have belts that move the printhead across the page. A worn, loose, or slipping belt can cause erratic printing.

TECH TIP

How to fix light printing

Light printing can be caused by several issues. Adjust the printhead gap to place the printhead closer to the ribbon or replace the ribbon. Also, the platen could be misaligned with the bottom paper-feed rollers.

If the printer prints continuously on the same line, be sure the setting for tractor-fed paper or friction-fed paper is correct. Or, the motor that controls paper movement may need to be replaced. If the printer moves the paper up a small bit after printing, the model may have the Auto Tear Off feature enabled. The Auto Tear Off feature is used with the perforated forms that are needed in many businesses. See the printer's documentation to disable this feature.

Inkjet Printer Troubleshooting

Most inkjet printer troubleshooting involves the printhead. Inkjet printers frequently have a built-in printhead cleaning routine that can be accessed through the printer's buttons or through software. Most manufacturers recommend cleaning the inkjet cartridge only when there is a problem, such as when lines or dots are missing from the printed output. Otherwise, cleaning an inkjet cartridge with this method wastes ink and shortens the life span of the print cartridge. If **speckling** or random spots appear, check the ink cartridges for leaks and replace them, if needed.

Usually, inkjet manufacturers include an alignment program to align the dots more precisely. Use the alignment program when vertical lines or characters do not align properly. If the colors do not appear correctly, check ink levels and run the printer manufacturer–provided color calibration

routine. Some printers have a chroma optimizer that increases the black density and has better color tone gradations. Refer to the printer's documentation for troubleshooting programs, such as the printhead cleaning, calibration, and alignment routines.

TECH TIP

Troubleshooting color

If a page does not print in color, check the printer properties to see if the grayscale option is selected.

Laser Printer Troubleshooting

Laser printers have more mechanical and electronic circuitry than the other printer types, which means more things can go wrong. The following list describes some common symptoms and possible solutions:

> If black **streaks** appear on the paper, the problem may be the drum, toner cartridge, fusing assembly, or paper. If the drum cannot hold a charge in a particular place, it can't attract toner to that area, and the drum might have to be replaced. The drum can be part of the toner cartridge or might be a separate unit. The toner cartridge is the easiest thing to replace to see if the streaks stop. Some cartridges have a sliding plastic strip that can be used to remove excess toner from the opening. Some printers have a drum cleaning routine that helps show where on the drum an issue exists. Use a clean lint-free cloth or foam swab to clean the drum spot. A dirty or damaged fusing assembly can also cause black streaks. Allow the printer to cool and check the fuser cleaning pad for toner particles and then use a small screwdriver to scrape off excess particles. Finally, the paper might have a static charge, especially on low-humidity days, so fan the paper before re-inserting it.

> If speckling appears or if output appears darker in some spots than others, remove the toner cartridge. Gently rock the toner cartridge back and forth to redistribute the toner. If this does not fix the problem, turn down the toner density by using the *Printers & scanners* Settings option or software provided by the printer manufacturer. Replace the toner cartridge if the wiper blades that remove excess toner are worn or the erase lamp is faulty. Also, the paper could be too smooth.

> If printing appears light, adjust the darkness setting on the printer or through the printer's operating system settings. The toner cartridge could be low. Damp paper could also cause this symptom. Use fresh paper of the proper weight and finish. If the print appears consistently dark, adjust the darkness setting.

> If a horizontal line appears periodically throughout the printout, the problem is one of the rollers. Check all the rollers to see if one is dirty or gouged and needs to be replaced. The rollers in a laser printer are not all the same size; the distance between the lines is the circumference of the roller. This allows you to easily tell which rollers are definitely not the problem and which ones are likely candidates.

> When white vertical lines appear, the corona wires may have paper bits or something else stuck on them. Or something might be caught in the developer unit (located in the cartridge). Replace the cartridge to see if this is the problem.

> If the back side of the printed page is smudged, the fuser could be faulty or need an adjustment, the wrong type of paper could be being used, or the toner might be leaking. Some printers allow temperature adjustments. Increase the temperature if the image smears; decrease the temperature if the paper curls or burn marks appear.

Many laser printer problems involve the toner cartridge, which is a good thing because the cartridge is a part that people normally have on hand. Various symptoms can occur because of the toner cartridge, including **double images** (also called ghost images, or **echo images**), smearing, horizontal streaking, vertical streaking, faded printing, one vertical black line, one horizontal black line, a white streak on one side, and a wavy image. One of the easiest things to do is to remove the toner cartridge, hold the cartridge in front of you with both hands, and rock the cartridge away from you and then back toward you. Reinsert the cartridge into the printer and test it.

Sometimes, the primary corona wire or the conditioning roller inside the toner cartridge needs to be cleaned. Clean the corona wires with the provided brush or with a cotton swab. Dampen the cotton swab with alcohol, if necessary. Clean the conditioning roller with a lint-free cloth that is dampened with alcohol, if necessary.

When toner is not fused to the paper, you need to determine whether a problem is in the fuser assembly or elsewhere in the printer. Send any output to the printer. When the printer is through with the writing stage and before the toner fuses to the paper, open the laser printer cover and remove the paper. If the paper is error free, the problem is most likely in the transfer corona/roller or fusing assembly.

Experience is the best teacher when it comes to printers. If you work on a couple impact models, a couple inkjet printers, and a couple laser printer models, you will see the majority of problems. A printer has very few circuit boards to replace. Normally, the problems are in the moving parts or are software related.

SOFT SKILLS: WORK ETHICS

Ethics is a set of morals by which you live or work. Employers want employees to possess high ethical standards. This means they want people who are honest, trustworthy, and dependable. IT technicians are exposed to many personal things—passwords, private data, and visited internet sites, just to name a few. Employers do not want to worry about technicians taking things that belong to others, looking at data that does not relate to the computer problem at hand (such as the information that might be on the desk shown in Figure 9.46 or printed material in the printer tray), or taking/giving away things from the office.

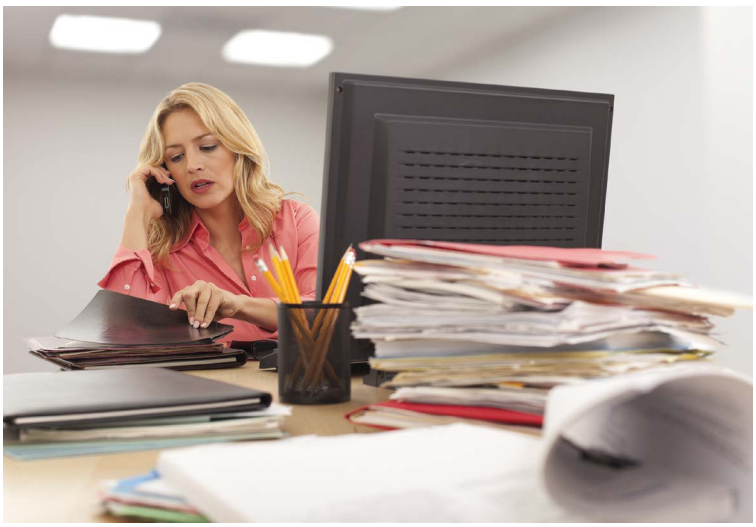


FIGURE 9.46 Work ethics: Do not look at or take information when working in an office

The best guideline in terms of ethics is to always be professional. For example, if you are in a situation where someone asks you to share another person's password, think about whether divulging the information is professional. When opening a customer's documents and reading them, ask yourself whether you are being professional. If the answer is no, stop reading. If you are in a customer's office and accidentally see the person's password taped to a keyboard, let the person know that you have seen it, suggest that passwords should not be kept in a conspicuous place, and recommend that the password be changed right away. One of the biggest assets an IT professional can have is their reputation. Being ethical at work goes a long way in establishing a good reputation.

Every IT person can probably remember at least one instance in which they were asked to do something unethical—charge for more time than was actually spent on a job, provide access to a room or an area where access is normally restricted, or grant privileges that others at the same level do not have. When put in such a situation, there are a few options: (1) Politely refuse, (2) adamantly refuse, or (3) report the person to a supervisor. Recommending what to do is difficult, but for most offenses, politely refusing is the best course of action and is the most professional. If a request is against corporate policy or could hurt others in the company, you need to report it to a company manager or security. Your own boss may be the best person to inform.

Chapter Summary

- Five types of printers commonly seen in businesses are impact, inkjet, laser, thermal, and 3-D printers.
- A multifunction device commonly has the ability to copy, print, scan, and possibly fax.
- Laser and inkjet printers do high-quality printing. A laser printer's supplies cost more than other printers' supplies, but laser printers last longer, and the cost per page is lower than for other types of printers.
- Printers can be shared using the operating system and a computer connected to a network.
- With wired networking, the printer has a direct connection to the network. Wireless networking includes 802.11 and Bluetooth technologies. A print server might be used to control and manage multiple printers. Printers can be registered through an app and managed/directed from that app to provide remote printing.
- Impact printers use print wires to impact a ribbon and are commonly used when multipart forms/output is needed.
- Impact printers can use normal-sized paper and fan-folded paper with pin holes that are fed by a tractor. Laser printers can have extra drawers for paper. A duplexing assembly option can be attached to allow a printer to print on both sides of the paper without human intervention. Impact printers use special heat-sensitive paper.
- Print drivers must match the operating system version.
- A printer uses a print spooler or hard drive space that keeps data flowing to the printer in large print jobs. The print spooler can be stopped and started by using the Services window (`services.msc`).
- If a printer doesn't work, check the printer display, check the computer for any messages, and ensure that the correct printer was chosen.
- A laser printer maintenance kit includes parts from a manufacturer that need to be changed after the printer has been used for a given number of hours. The contents of such a kit are vendor specific. The maintenance counter must be reset after a maintenance kit has been applied.
- Virtual printing can be accomplished through the print to file, print to PDF, print to XPS, and print to image options.
- Common printer problems include light print, double images, toner not fusing to the paper, paper path issues, problems with wired or wireless connectivity to the printer, print driver problems, security settings, and error codes that appear on the printer display.
- Print security can be enhanced by ensuring that a person is authorized to print. Authentication can be provided through a user ID/password, an employee badge, by entering an authorization PIN, or by using secure print.
- A computer technician needs to behave ethically around customers and peers.

A+ CERTIFICATION EXAM TIPS

- ✓ Know how impact, inkjet, laser, and thermal printers work and the basic parts in each one. Know how to properly unbox a printer or multifunction device and understand considerations for device location.
- ✓ Know the parts of a laser printer: imaging drum, fuser assembly, transfer belt, transfer roller, pickup rollers, separation pads, and duplexing assembly. Some printers allow adjustments to the fuser assembly. The temperature should be hotter if the image smears and turned down if the paper curls or has burn marks.
- ✓ Know the parts of an inkjet printer: ink cartridge, printhead, roller, feeder, duplexing assembly, and carriage belt.
- ✓ Know the parts of a thermal printer: feed assembly, heating element, and special thermal paper that is sensitive to heat and must be stored in a cool place.
- ✓ Know the parts of an impact printer: printhead, ribbon, tractor feeder, and impact paper.
- ✓ Know that a document can be scanned and sent to an email or remote scanning can occur using cloud services.
- ✓ Know how to operate and install a device that has an automatic document feeder (ADF).
- ✓ Know appropriate laser printer maintenance techniques, including replacing toner, applying a maintenance kit, calibrating, and cleaning.
- ✓ Know appropriate thermal printer maintenance techniques, including replacing paper, cleaning the heating element, and removing debris.
- ✓ Know appropriate impact printer maintenance techniques, including replacing the ribbon, replacing the printhead, and replacing paper.
- ✓ Know appropriate inkjet printer maintenance techniques, including cleaning the heads, replacing cartridges, calibrating the printhead for color, and clearing jams.
- ✓ Be able to configure and troubleshoot printer options, including duplex, tray settings, paper size, orientation, and quality settings.
- ✓ Know how to review and control the print driver and print spooler.
- ✓ Know how to network a printer by using a print server and printer sharing.
- ✓ Be aware of data privacy issues, including user authentication that may be required, using a user ID/password, PIN, badge, and Secure Print; hard drive caching; and access to corporate/private information that may be onscreen or printed.
- ✓ Review all the troubleshooting sections (especially the key terms) before taking the exam. Know how to troubleshoot and resolve paper jams, staple jams, and hole punch issues. Know how to resolve vertical lines in the output, garbled print, toner not fusing to the paper, multipage misfeed, multiple print jobs pending in the queue, speckling, double images, and grinding noises.

Key Terms

3-D printer, ADF, audit log, badging, calibrate (inkjet printer), calibrate (laser printer), clean a laser printer, clean the heating element, clean the printhead, cloud services, connectivity issues, default printer, double image, duplex, duplexing assembly, echo image, faded print, feed assembly, feeder, frozen print queue, fuser assembly, garbled print, grinding noise (printer), heating element, high sensitivity of thermal paper, hole punched, impact printer, impact printhead, incorrect orientation, incorrect paper size, ink cartridge, inkjet printer, inkjet printhead, laser printer, laser printer maintenance kit, line down the printed page, maintenance counter, multifunction device, multipage misfeed, multipart paper, multiple print jobs pending, orientation, paper jam, paper not feeding, PCL, PDL, PostScript, print driver, print ribbon, print server, print spooler, printer firmware, quality, remove debris, replace the ink cartridge, replace the paper (impact), replace the paper (thermal), replace the printhead (impact), replace the ribbon, replace the toner cartridge, resin, roller, secure print, setup location, SMB, special thermal paper, speckling, staple jam, streak, thermal printer, tractor feed, tray not recognized, tray settings, unbox a printer, user authentication, virtual printing

Review Questions

1. What method does a technician *normally* use to print a test page to prove that connectivity exists between a computer and a printer and to prove that the driver is working properly?
   - **a.** Use a self-test button on the printer.
   - **b.** Use Notepad and print.
   - **c.** Use at least two applications and print.
   - **d.** Use the *Print Test Page* button from the *General* tab of the *Printer properties* window.
2. Which type of printer would a glass blower who sells art at trade shows most likely use to print receipts?

   [impact | inkjet | thermal | laser]
3. Which program is used to restart the print spooler in Windows?

   [Device Manager | Services | System Information | DirectX]
4. A Samsung laser printer is showing an error message on the screen that says that the paper is out, but the user shows you that there is plenty of paper in the bin. What should you do?
   - **a.** Turn the printer off and back on again.
   - **b.** Check the paper sensor for debris or dust.
   - **c.** Use the reset sensor to reset the printer paper counter.
   - **d.** Use the *Print Test Page* button in Windows to verify connectivity.
5. Which type of printer contains a fuser assembly?

   [impact | inkjet | laser | thermal]
6. You are working on a printer that is missing an option in the printer menus that the manufacturer lists online. What upgrade is most likely needed?

   [storage space | electronic control board | memory | firmware]
7. For what do you use a printer-duplexing assembly?
   - **a.** two-sided printing
   - **b.** multiple paper trays
   - **c.** wired and wireless network connectivity
   - **d.** rasterization
8. Which component causes ghost images on laser printer output?

   [drum | fusing assembly | LED array/laser | pickup rollers | paper sensor]
9. An inkjet printer printhead appears to be stuck, and the printer is making a grinding noise. Which part should the technician check first?
   - **a.** print cartridge
   - **b.** paper feeder
   - **c.** carriage and carriage belt
   - **d.** printer mainboard
10. One of the technicians in your shop frequently swaps parts that do not fix the problem. The parts taken out of customer machines are taken to build private customer computers. This is an example of poor _____.

    [communication skills | work ethics | relations | troubleshooting skills]

11. Which type of printer maintenance commonly requires resetting a maintenance counter?

[impact | thermal | laser | inkjet]

12. Which printer option allows multiple copies of a document to be printed in page 1, 2, 3 order instead of printing all the page 1s, then all the page 2s, and then all the page 3s?

[fusing | collating | duplexing | conditioning]

13. A networked printer is visible through the network, but no one can print to it. What is the first thing the technician should check?

a. print spooler setting

b. printer IP address

c. errors or indicators on the printer

d. cabling

14. A laser printer outputs streaks on the paper. What is the issue?

[drum | roller | ink cartridge | laser]

15. An inkjet printer's output appears to have missing elements. What is the first thing a technician should try if the ink cartridge appears to be full?

_____

16. Which security options are relevant to printer control? (Choose all that apply.)

[user authentication | bollards | badging | universal security slot | antivirus]

17. What is the purpose of the roller in an inkjet printer?

a. It limits the amount of paper fed through the printer to one page.

b. It controls the amount of ink allowed onto the paper.

c. It moves the paper through the paper path.

d. It moves the carriage from one side to the other.

18. What happens if a heating element fails on a thermal printer?

a. missing printed output

b. paper not feeding through

c. incorrect colors being printed

d. garbled output

19. How is laser printer calibration commonly performed?

a. with a multimeter

b. with a special tool that is part of the maintenance kit

c. through the *Printer/Printer properties* menu

d. with calipers

20. The printed output prints about three-quarters down the page and then starts printing the rest on the next page. A technician has been contacted to help. On which option does the technician need to instruct the user?

[duplexing | paper size | collating | orientation | finishing]

Exercises

Exercise 9.1 Research a Local Printer

Objective: To use the internet or a magazine to research information about a printer

Parts: A computer with internet access

Notes: A printer is not required to be attached to the computer for this exercise to be executed.

Procedure: Complete the following procedure and answer the accompanying questions.

A business user is interested in purchasing two printers. Details for the printers are as follows:

Printer A: A printer to be shared by all employees through the wired Ethernet network. Output should be high-quality black-and-white, grayscale, or color. The printer will not be used for huge print jobs but to print a proposal for a client or a few handouts for a small number of participants in a presentation. Speed is not an issue.

Printer B: A printer model that will be standard for those who need a printer attached to their workstations. The printer should be able to support wired connectivity to the Ethernet LAN or IEEE 802.11 wireless connectivity. The printer might be shared with computers that do not have a local printer attached. The printer should support quality black-and-white, grayscale, or color. The printer will not be used for a large number of copies. Speed is not an issue. A scanner needs to be part of the printer, too. The cost of supplies is a concern.

1. Using the internet, provide the business user with three suggestions for Printer A. List the model number and at least five facts related to the criteria. Find three price quotes for each suggested model and the name of the company for each one.

   _____

   _____

2. Using the internet, provide the business user with three suggestions for Printer B. List the model number and at least five facts related to the criteria. Find three price quotes for each suggested model and the name of the company for each one.

   _____

   _____

   _____

Exercise 9.2 Printer Driver Research

Objective: To use the internet to research information about three printer drivers

Parts: A computer with internet access

Notes: A printer is not required to be attached to the computer for this exercise to be executed.

Procedure: Complete the following procedure and answer the accompanying questions.

Locate the latest driver for each of the following printers and operating systems. Write the driver version in the third column.

Printer model	Operating system	Latest print driver version
HP OfficeJet Pro 9730e wide-format all-in-one printer	Windows 11	
Lexmark CS720 color laser	Windows 10 (64-bit)	
OKI Data ML421 dot matrix	Windows 11	

Activities

Internet Discovery

Objective: To obtain specific information on the internet regarding a computer or its associated parts

Parts: Computer with access to the internet

Questions: Use the internet to answer the following questions.

1. A customer has a broken USB inkjet printer that would cost more to repair than to replace. The customer is considering an Epson Expression XP-4200 all-in-one printer as a replacement. The customer would also like to have wireless connectivity, individual color cartridges, and the ability to print from a camera memory card. Will this printer meet the customer's needs? Explain your answer and write the URL where the information was found.

   _____

   _____

   _____

2. A store uses the Epson TM-T20III receipt thermal printer and has asked you to look at it because the error LED light is flashing. What are at least three things that could cause this error, and at what URL did you find this information?

   _____

   _____

   _____

   _____

3. A user has a Lexmark MX431adw laser printer. What is the latest firmware version available for this printer? Write the answer and the URL where you found the solution.

   _____

   _____

4. How do you reset the HP LaserJet P2035 to factory default settings? Write the answer and list the URL where you found the answer.

   _____

   _____

5. You had to replace the drum on a Brother HL-L8250CDN color laser printer. What process is used to reset the drum unit counter?

   _____

   _____

   _____

   _____

Soft Skills

Objective: To enhance and fine-tune a technician's ability to listen, communicate in both written and oral forms, and support people who use computers in a professional manner

Activities:

1. The class is divided into seven groups. Each group is assigned a laser printing process. The group has 20 minutes to research the process. At the end of 20 minutes, each team explains its process to the rest of the class.

   _____

2. Pretend you have a job as a computer technician. You just solved a printer problem. Using good written communication skills, document the problem as well as the solution in a professional format. Exchange your problem/solution with a classmate and critique each other's documentation. Based on suggestions and your own background, refine your documentation. Share your documentation with the rest of the class.

_____

_____

_____

_____

_____

_____

_____

Critical Thinking Skills

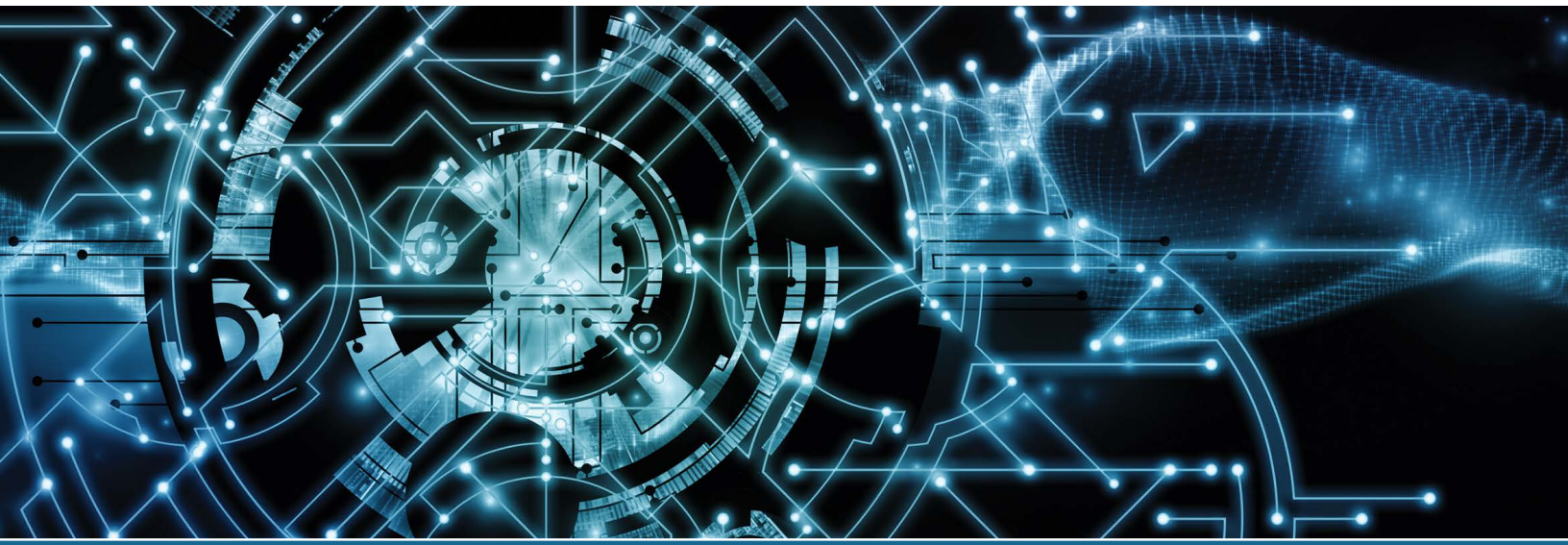
Objective: To analyze and evaluate information as well as apply learned information to new or different situations

Activities:

1. Two networked PCs and a printer are needed for this activity. Connect a printer to a PC. Install the printer, configure the default settings to something different from the current settings, share the printer, and then print from another PC that connects to the same network.
2. Interview a technician regarding a printing problem. List the steps the technician took and make notes about how they might have done the steps differently, based on what you have learned. Share the experience with the class.

This page intentionally left blank

10 Mobile Devices



In this chapter you will learn:

- About the operating systems mobile devices use
- How to configure mobile devices
- How to back up and secure mobile devices
- How to troubleshoot mobile devices
- The importance of personal appearance in the IT field

CompTIA Exam Objectives:

- ✓ 1201-1.1 Given a scenario, monitor mobile device hardware and use appropriate replacement techniques.
- ✓ 1201-1.2 Compare and contrast accessories and connectivity options for mobile devices.
- ✓ 1201-1.3 Given a scenario, configure basic mobile device network connectivity and provide application support.
- ✓ 1201-2.2 Explain wireless networking technologies.
- ✓ 1201-2.5 Compare and contrast common networking hardware devices.
- ✓ 1201-2.6 Given a scenario, configure basic wired/wireless small office/home office (SOHO) networks.
- ✓ 1201-2.7 Compare and contrast internet connection types, network types, and their characteristics.
- ✓ 1201-2.8 Explain networking tools and their purposes.
- ✓ 1201-3.2 Summarize basic cable types and their connectors, features, and purposes.
- ✓ 1201-3.3 Compare and contrast RAM characteristics.
- ✓ 1201-3.4 Compare and contrast storage devices.
- ✓ 1201-3.5 Given a scenario, install and configure motherboards, central processing units (CPUs), and add-on cards.
- ✓ 1201-5.4 Given a scenario, troubleshoot common mobile device issues.
- ✓ 1201-5.5 Given a scenario, troubleshoot network issues.
- ✓ 1202-1.1 Explain common operating system (OS) types and their purposes.
- ✓ 1202-1.6 Given a scenario, configure Microsoft Windows settings.
- ✓ 1202-2.1 Summarize various security measures and their purposes.
- ✓ 1202-2.2 Given a scenario, configure and apply basic Microsoft Windows OS security settings.
- ✓ 1202-2.8 Given a scenario, apply common methods for securing mobile devices.
- ✓ 1202-2.10 Given a scenario, apply security settings on SOHO wireless and wired networks.
- ✓ 1202-3.2 Given a scenario, troubleshoot common mobile OS and application issues.
- ✓ 1202-3.3 Given a scenario, troubleshoot common mobile OS and application security issues.
- ✓ 1202-4.7 Given a scenario, use proper communication techniques and professionalism.

Mobile Device Overview

Mobile devices are an integral part of today's society. Wearable devices such as smartwatches, fitness monitors, glasses, and headsets allow us to take our technology wherever we go. New laptop features, tablets, Android phones and tablets, Apple iPhones and iPads, and other electronics are continuously being introduced. Many mobile devices are all-in-one units. Mobile devices are designed to be quick, light, durable, and portable (see Figure 10.1), and in some cases, a mobile devices is a user's main computer. Table 10.1 lists characteristics of various mobile devices.

FIGURE 10.1 Mobile devices

TABLE 10.1 Mobile devices

Device	Description
Tablet	A tablet is a mobile device that has a touch screen, camera(s), microphone, and possibly one or more ports. Tablets connect to the internet, and they can be used to take, send, receive, and store pictures and video. Apple's tablet is known as an iPad, and there are variations such as the iPad mini, iPad Air, and iPad Pro (see Figure 10.2).
Drawing pad	A drawing pad, also known as a drawing tablet or graphics tablet, is a device used to draw, annotate an existing document or drawing, type, or write. Drawing pads are used by teachers, graphic artists, space planners, and engineers.
GPS	The Global Positioning System (GPS) is a series of satellites that provide location, movement, and time information to a single device or to a component integrated into a mobile device.
Smartphone	A smartphone has the capability to make calls and run apps, play music, track movement using GPS, connect to wireless networks, connect wirelessly to other devices, connect to the internet through the phone network or wireless network, and take high-resolution pictures and videos. Two popular smartphone operating systems are Android and Apple iOS.
Phablet	A phablet is a cross between a smartphone and a tablet that tends to have a larger screen than a smartphone for taking notes and viewing documents more easily (see Figure 10.3). It may include a stylus.

Device	Description
E-reader	An e-reader, also known as an e-book reader, has an LCD screen designed for reading. It stores digital books, magazines, and other online materials.
Smart camera	A smart camera has capabilities such as facial recognition, measuring, inspection for quality assurance, surveillance, and robot guidance. A smart camera may include a mobile operating system, have internet access, and have support for wired and wireless networking. Figure 10.4 shows a smart camera attached to a drone.

FIGURE 10.2 Tablet

FIGURE 10.3 Phablet

FIGURE 10.4 Smart camera

Mobile Operating System Basics and Features

A mobile device, like any other computer, needs an operating system (OS). A mobile operating system can be proprietary or open source. Android (based on Linux), iOS (Apple's system), Windows, and Chrome OS are prominent examples of mobile platforms that power smartphones and tablets. **Android** is an open source OS that is based on the Linux kernel and used mainly on phones and tablets, but it is also available on laptops and PCs. Open source operating systems allow vendors to use the core source code and customize the operating system. Google owns Android, which is one of the most popular mobile operating systems in the world.

Apple's **iOS** is used only on Apple devices, and **iPadOS** is used on Apple tablets. Microsoft Windows operating systems are used on many laptops and tablets. Microsoft used to have its own mobile operating systems, including a phone operating system, but they have all been discontinued. The Windows 10 and 11 Internet of Things (IoT) Core operating system is used on Advanced RISC Machine (ARM) devices.

Many are familiar with Chrome as a browser option, but **Chrome OS** is also an operating system that was developed by Google as an open source project (called the Chromium OS project). Developers can use or modify the code developed from this group, but Chrome OS is supported by Google and Google partners. Laptops that use Chrome OS, known as Chromebooks, are very popular in schools and commonly use cloud-based apps. The Chrome OS is also used on ARM mobile devices.

Mobile Storage

A mobile device needs a place to store data, and mobile storage uses the same technology as some PC storage, but of course the storage media is smaller. Mobile devices do have RAM. For example, laptops commonly have as much **laptop RAM** as desktops. Sometimes this RAM is not upgradable in mobile devices such as tablets and smartphones. However, mobile devices commonly use flash memory. **Flash memory** is a type of nonvolatile, solid-state memory that holds data even when the computer power is off. Smartphones, tablets, and other mobile devices use flash memory to store the operating system, apps, and data/video. Flash memory cards for mobile devices include various types of Secure Digital (**SD**) cards (see Figure 10.5): SD, SDHC, SDXC, SDUC, and probably more since this book has been published.

FIGURE 10.5 SD storage

Flash memory cards, or storage cards, are used in mobile devices and laptops, as well as in desktop computers. In Apple and Android products, use the *Settings* > *Storage* option to view the internal memory capacity and any additional memory storage.

A laptop or tablet may have an SD card slot built in. If a device has an SD tray that pulls out, insert the flash card into the tray (with the contacts facing down) and then push the tray into the device. Sometimes in order to insert a microSD card into a laptop or tablet, an adapter may have to be purchased so that the microSD card can be used. Figure 10.6 shows how the microSD card inserts into an adapter. That adapter must match the slot size (normally SD) of the mobile device.

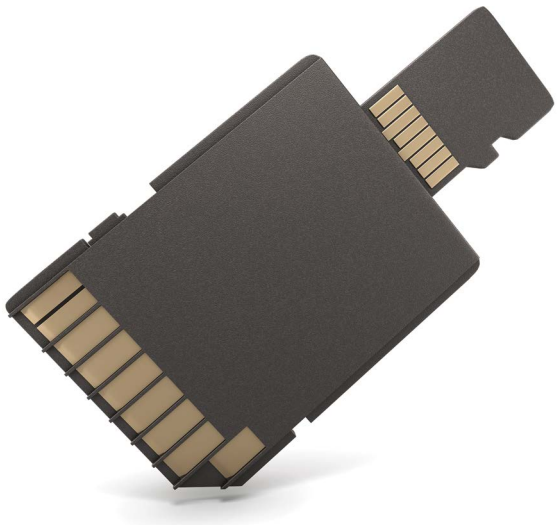


FIGURE 10.6 Flash media adapter

Some people like to use a smart card reader (also known as a multi-card reader, media card reader, or flash/flash **memory card reader**) to quickly and easily transfer pictures, data, movies, and so on to a PC. Some card readers accept 75 different types of media storage. A card reader attaches to a USB port or is integrated into a laptop. Insert the flash media into an appropriate slot. Look at Figure 10.7 to see some of the media slots. Once a smart card is inserted, the OS assigns a drive letter to the memory card.

FIGURE 10.7 Smart card reader

Mobile Accessories

Mobile devices have some accessories that are unlike PC accessories. Table 10.2 describes various mobile accessories a technician may need to know about and discuss with customers.

TABLE 10.2 Mobile accessories

Accessory	Description
Headset	A headset can use a wired (through a USB port) or wireless connection to provide sound and typically fits over one (see Figure 10.8) or both ears. See the "Bluetooth" section, later in this chapter, for wireless headset configuration.
Webcam	A webcam is an integrated or USB-connected device used to record or provide live video and optionally sound. A privacy slide may be used to block a webcam lens.
Speaker	Speakers are built in to mobile devices; some devices have audio ports for external speakers. Speakers can be wired or wireless. See the "Bluetooth" section, later in this chapter, for wireless configuration. Use *Settings* to mute or otherwise control a speaker.
Stylus	Also known as a touch pen or an active pen, a stylus might be vendor specific and is used to provide input into a mobile screen. Proprietary pens are more expensive and have additional buttons and features compared to pens that are just used to touch a spot on the screen or write something. Cases or screen covers can interfere with styluses. Use *Settings* to ensure that a stylus is enabled.
Mobile docking station	A mobile docking station provides a stable environment for mobile computers while traveling, such as for a laptop in a police car or for military operations. Docking stations are also available to charge one or more mobile devices. Figure 10.9 shows a mobile docking station.

Accessory	Description
Track pad/ drawing pad	A track pad or drawing pad is a USB or wireless device (see Figure 10.10) that is used to input drawings, annotations, or text, sometimes on top of other information. A track pad is sometimes used with drawing software, and the pen has to be calibrated before use.
Track point	A track point (also known as a tracker, tracking device, or device tracker) is a device used for locating a wallet or another important item. An app shows the location of the track point.

FIGURE 10.8 Wireless headset

FIGURE 10.9 Mobile docking station

FIGURE 10.10 Track pad integrated into a laptop

Using Mobile Devices

A mobile operating system is different from other operating systems in that, instead of primarily using a mouse or keyboard to interact with the operating system, a finger, a stylus, spoken word, or multiple fingers are used. A home page might be displayed, or a system bar might extend across the bottom of a mobile device's screen. There might also be a mobile notification area that contains icons for information such as the battery life, wireless signal strength, time, and external media connectivity. Note that on a smartphone (see Figure 10.11), the notification area and settings are commonly available with a swipe from the top of the display. Figure 10.12 shows an Apple iPhone home screen. An Apple iPad or iPhone may have a physical home button (not an icon to tap) beside or below the screen.

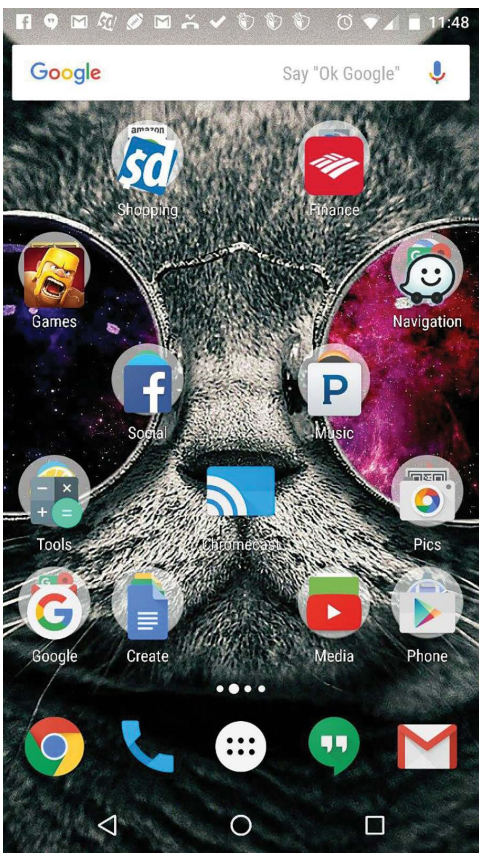


FIGURE 10.11 Android smartphone home screen

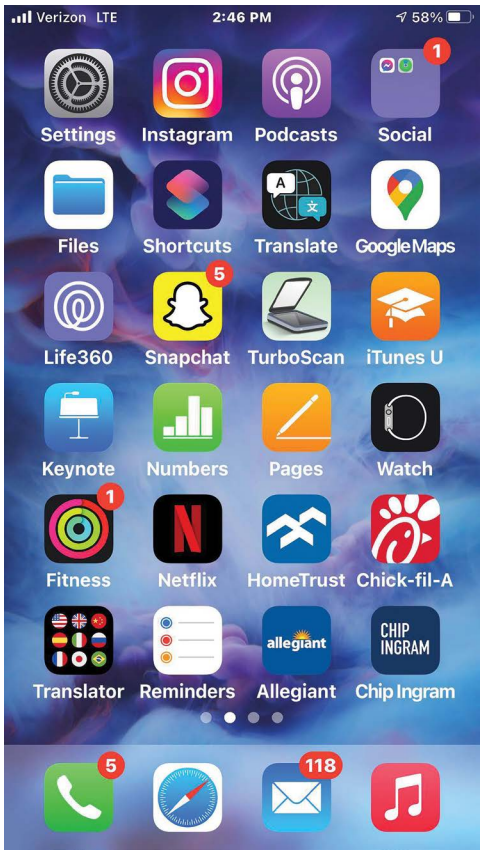


FIGURE 10.12 iPhone home screen

Interacting with a Mobile Operating System

Configuration is commonly performed through a mobile device's *Settings* option, but before we get into configuration, you need to understand touch displays. Touching a display instructs the operating system to do something. Swiping is used to go to the next (or previous) page of an application/screen or go to the next (or previous) photo or other item. Multitouch technology makes a device capable of accepting multiple touches, such as when two fingers or a finger and a knuckle are used. 3-D touch involves lightly tapping the touch screen to open an application, tapping and holding for a second to perform a different function, or pressing down firmly on the same area to perform a third function. This technology is continually evolving.

Table 10.3 lists the terms commonly used for different means of interacting with a mobile OS. As you can see from this list of terms, some interaction requires multitouch, and not all screens support this feature. Figure 10.13 shows some multitouch techniques.

TABLE 10.3 Mobile operating system interaction terms

Term	Description	Function
Touch or tap	Press an icon or area.	Opens an application.
Double-tap	Press an icon or area twice in quick succession.	Enlarges an area of a screen or an item such as a picture.
Long touch or touch and hold	Press and hold on an icon or area.	Moves an icon from one home screen to a different home screen or unlocks a tablet.

Term	Description	Function
Swipe or flick	Press and move to the left or right or up and down.	Moves from one home screen to another or opens the notification area on a smartphone.
Scroll	Press and move up or down.	Quickly goes through a list of files or pictures.
Pinch or pinch close	Using two fingers spread apart, bring the fingers closer together.	Zooms out from an object or area.
Spread or pinch open	Using two fingers close together, move the fingers apart.	Zooms in on an object or area, such as when you want to be able to see a closer view of a map or to enlarge words.

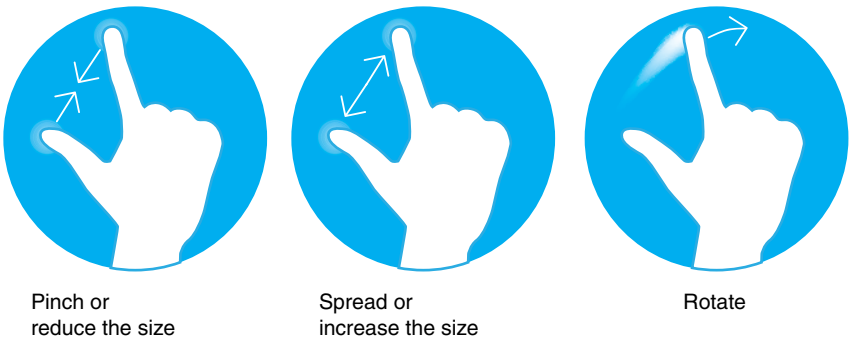


FIGURE 10.13 Multitouch techniques

TECH TIP

What if a device goes to sleep?

Press the power button and optionally enter the appropriate pattern, PIN, or passcode. On an Android device, press and drag the lock icon to the unlock icon in the center of the display. Pressing the home button, swiping up from the bottom edge, or tapping the screen quickly also awakens an iPhone or iPad. Slide the *Slide to Unlock* bar to the right and enter the passcode if one is set.

Cell Phones

Most people are familiar with what a cell phone is, but technicians need to know a little more about phones than typical users. Also, some companies issue phones to employees and have technicians support them. Learning about how phones are identified and when they should be updated is important.

A cellular network is a collection of devices that allow mobile phones/smartphones to communicate. A cellular network is divided into cells, and each cell provides coverage within a specific geographic area. Cell phones connect to and send data through the air to a cellular network composed of antennas and/or satellites that transmit the call or data onward to a destination. Figure 10.14 shows a cellular network and an example of how cell phone towers are being replaced by fake pine and palm trees that contain antennas.

FIGURE 10.14 Cellular network and communications tower in fake tree

Cellular networks are known as **3G/4G/5G** networks. The older 3G networks used either Code Division Multiple Access (CDMA) protocol or Global System for Mobile Communications (GSM) technologies. Today's cell networks, starting with 4G networks, use Long Term Evolution (**LTE**). Each of these technologies is like a language of its own.

Table 10.4 lists the cellular network technologies a technician needs to be familiar with.

TABLE 10.4 Cellular network technologies

Technology	Description
3G	Third generation of wireless cellular technology, which allowed mobile devices to have internet connectivity of at least 200 kb/s and up to 2 Mb/s.
4G	Fourth generation of cellular network, which supports IP telephony, gaming services, mobile TV, and video conferencing at speeds up to 1 Gb/s.
LTE	A version of 4G that optimized the network for video streaming and online games.
5G	Fifth generation of cellular networks, which enables faster speeds (up to 20 Gb/s) at some new lower frequencies, from 600 MHz to 40 GHz.

IMEI and IMSI

International Mobile Equipment Identity (IMEI) is a unique number—much like a serial number—given to a particular cell phone or satellite phone. IMEIs are stored in a database or the Equipment Identity Register (EIR). When phones are reported stolen, the database can be updated to mark the number as invalid. When buying a used phone, you might want to check the IMEI number against a mobile block list to ensure that the phone has not been lost or stolen.

A company may ask its IT department to track cell phones paid for by the company. The IMEI is commonly found on the back of the phone (see Figure 10.15), under the battery, or under the SIM card.

FIGURE 10.15 Cell phone with the IMEI on the back

The international mobile subscriber identity (IMSI) is a unique number that is stored in a smartphone's subscriber identification module (SIM) card. **SIM** cards are used in mobile phones, satellite phones, mobile devices, and laptops. A SIM card contains electronics that store information such as personal contacts, numbers, phone services on a GSM network, security authentication, and a security personal identification number (PIN). Figure 10.16 shows a SIM card being inserted into a cell phone as well as the different sizes of SIMs.

A smartphone or smartwatch today is likely to have an embedded SIM (**eSIM**), which is not a physical card. An eSIM allows you to change your network provider without requiring a SIM swap. eSIMs also let you have multiple phone numbers. A phone may have a physical SIM and an eSIM or two active eSIMs.

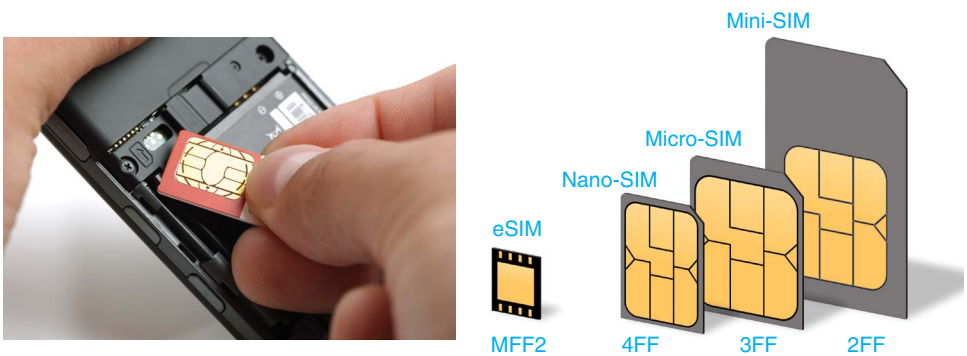


FIGURE 10.16 SIM and eSIM cards

Mobile Apps

Applications, commonly called *apps*, come with a device, can be downloaded free of charge, or can be purchased through the App Store (Apple iOS devices), Google Play (Android devices), or Microsoft Store (Windows devices). New apps are being developed constantly, and applications

that might not be of much use with a desktop computer are very handy on mobile devices. Table 10.5 lists common mobile apps.

TABLE 10.5 Common mobile apps

Android app	iOS app	Windows app
Gmail	Mail	Mail
Google Maps	Maps	Maps
Gallery/Google Photos	Photos	Photos
Chrome	Safari	Edge
Play Music	iTunes	Music
Bluetooth > File Manager	AirDrop	Nearby Sharing
Clock	Calendar	Calendar
Play Store	App Store	Microsoft Store
Google Drive	iCloud	OneDrive

Common Apps and Features

Apps on mobile devices have individual settings that users might need help with. For example, some people do not like the clicking noise a camera makes when taking a picture. Check the settings of the particular app for potential changes. Personal information on a phone can also be shared with the app developer. In both Android and iOS apps, use the *Settings* menu and select either *Permissions* or *Privacy* to remove unnecessary permissions.

One commonly used feature is GPS. With GPS, satellites send location information to a receiver on a mobile device. Mobile apps provide directions to get to a store or to where another person is located, and they show how far you have walked.

Some people disable the GPS capability until they want to use it in order to prevent geotracking. Geotracking involves tracking the location and movement of a mobile device (see Figure 10.17). Social media and other applications, known as **cellular location services** or **locator applications**, rely on such data to "publish" your current location or the locations of friends you have selected. Vendors have plans that include the ability to track family members. Companies use geotracking to locate lost and stolen mobile devices. Note that some devices also use a geotagging feature; for example, a camera app may use geotagging to include with a photo information such as where the photo was taken. It is possible to disable the geotagging feature, and many users do so for privacy reasons.

Configure Android devices for GPS by using the *Settings* > *Biometrics and security* > *Location* option. For Apple iOS devices, use the *Settings* > *Privacy* > *Location Services* option.

Because a mobile device screen is used to interact with the operating system, screen calibration may need to be performed. Android users use the *Settings* app. Windows users use *Settings* > *Calibrate the Screen for Pen and Touch Input* > *Calibrate*. You can also download an app to perform screen calibration tasks, such as color, sensitivity, one-hand configuration, or motion/gestures configuration.

FIGURE 10.17 Geotracking

Table 10.6 explains some mobile operating system features.

TABLE 10.6 Mobile operating system features

Feature	Description
Internet calling	Use an app such as Skype, Google Voice, Viber, or WhatsApp to call another person.
Wi-Fi calling	Make a call using a Wi-Fi connection rather than the cell phone network; beneficial when the phone network has a weak signal or to avoid using cell phone network minutes or roaming. Some vendors offer this as a built-in service.
Virtual assistant	Use voice commands to obtain information such as directions or current sports scores and to dictate emails or texts; examples include Apple's Siri, Microsoft's Cortana, Google Assistant, and Amazon Alexa.
Emergency notification	Obtain wireless emergency alerts (WEA); a U.S. method for propagating emergency alerts such as announcements from the National Weather Service, presidential messages, and emergency operation centers messages to mobile devices.
Mobile payment service	Pay for services or goods by using a mobile device instead of with cash or a credit card (see Figure 10.18). Transactions can be conducted using technologies such as near field communication (NFC), Wireless Application Protocol (WAP), direct mobile billing, and Short Message Service (SMS). Popular mobile payment apps include Apply Pay and Google Pay.

FIGURE 10.18 Mobile wallet

Obtaining, Installing, and Removing Apps

Mobile device apps are obtained from a source such as Google Play, Apple's App Store (or iTunes), the Microsoft Store, Amazon's Appstore for Android, and a host of other content sources. There are other ways to get an app: by manually installing it (called *side loading*), using a USB cable (which commonly requires a file management app), using your storage media and a media reader, using an app such as Bump to transfer an application, or using a quick response (QR) code between two devices. For an example of a QR code, look at the bottom of the cell phone screen in Figure 10.18. Note that whatever method you use to install an app, you must ensure that the app is from a trusted source or a trusted app developer.

Some folks use Settings on an Android device to enter **developer mode**—a mode where tools can be used to change the normal way the device operates or increase the performance in some way. Improper use of developer mode could open security vulnerabilities or prevent the device from operating properly.

Two important terms related to apps are APK and SDK. Android application package (APK) is the file format used to distribute and install Android apps. So if you download an app, it is an APK file. A software development kit (SDK) is a set of tools (application programming interfaces [APIs], documentation, programming tools, analytic tools, sample code, and so on) used to develop an app for a specific mobile OS or platform.

Mobile Device Wired Connectivity

Mobile devices have many of the same ports as computers but in smaller versions. Proprietary vendor-specific ports are primarily for power connections or provide communication options. Let's explore these ports in a little more detail starting with USB and Lightning Ports.

Mobile USB and Lightning Ports

A mobile device is likely to have either a USB, **microUSB**, **miniUSB**, or **USB-C** port. Figure 10.19 shows the standard Type-A USB port found on a PC and the mini-B, micro-B, and USB-C ports found on mobile devices. The USB-C port is now a standard interface for smartphones.

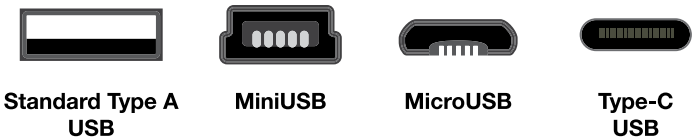


FIGURE 10.19 USB Type-A, mini, micro, and USB-C ports

Apple used to have an 8-pin **Lightning port** for its devices, but it has moved to the USB-C port. Both the Lightning port and USB-C cables can be inserted either face up or face down because they are non-directional. Figure 10.20 shows a Lightning connector and port. Figure 10.21 shows Apple's two connectors on the left, along with microUSB, miniUSB, and traditional USB connectors.

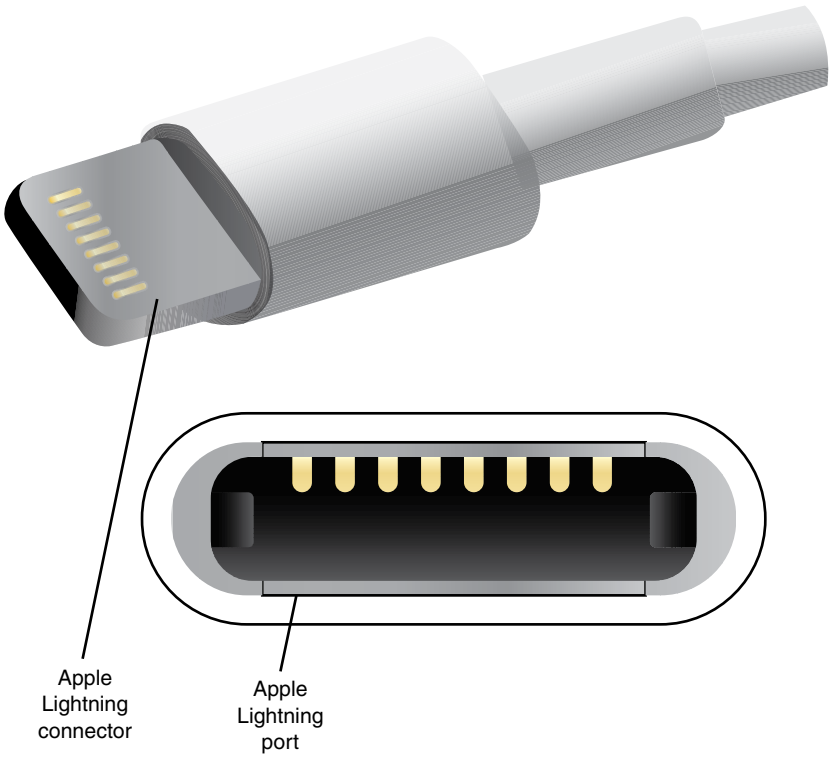


FIGURE 10.20 Apple Lightning port and connector

FIGURE 10.21 Mobile connectors

With a device that doesn't have a wired RJ45 network connector but that does have a USB port, a USB-to-RJ45 converter can be used. Wired network connections are faster than wireless connections and are commonly found on laptops, but other mobile devices lack RJ45 jacks. Refer to Figure 2.11 for a photograph of a USB-to-RJ45 (Ethernet) dongle.

Mobile Device Wireless Connectivity

The whole purpose of having a mobile device is to be able to move around with it. However, mobility is only part of the picture. The other part involves connecting to some type of network, such as a cellular, satellite (for GPS), wireless (Wi-Fi), or Bluetooth network.

Note that because Android devices are created using an open source operating system, configuration options can be different from one device to another. Apple and Windows have different versions of their mobile operating systems. By default, when most mobile devices are configured for wireless networks, the devices autoconnect. If you walk out of range of that wireless network and another one is configured, your device is likely to switch over to the second wireless network. If no wireless networks are within range, the mobile device switches over to an available and compatible cellular network.

Bluetooth

Bluetooth is a radio-based wireless technology used to connect two or more devices that are commonly within close range of one another. This type of connectivity is called a wireless personal area network (PAN). Bluetooth operates in the unlicensed 2.4 GHz range. Bluetooth includes 128-bit security and supports a data rate up to 24 Mb/s. Up to eight devices can be connected in a central/peripheral relationship (with only one device being the central). Bluetooth has three classes of devices:

- **Class 1:** Range up to 328 feet (100 meters)
- **Class 2:** Range up to 33 feet (10 meters)
- **Class 3:** Range up to 3 feet (1 meter)

Note that the Bluetooth 5 standard supports a longer range of up to 800 feet (242 meters). The Bluetooth standards do not define the maximum range. Rather, the range depends on the type of Bluetooth radio installed. Most mobile devices use a Class 2 radio but seldom can have connectivity 33 feet away.

Many mobile devices support Bluetooth. Refer to Figure 10.8 to see a Bluetooth headset used with a cell phone. Figure 10.22 shows controls in a car to enable Bluetooth connectivity. The Bluetooth symbol is shown in Figure 10.23.

FIGURE 10.22 Enabling Bluetooth connectivity

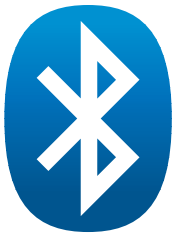


FIGURE 10.23 Bluetooth symbol

The basic concept behind configuring Bluetooth is that each device must have Bluetooth enabled and must "pair," or connect, with another Bluetooth-enabled device. Once enabled, Bluetooth broadcasts a wireless signal that other Bluetooth-enabled devices can detect. The basic steps for configuration are as follows:

Step 1. Enable Bluetooth.

Step 2. Ensure that pairing is enabled.

Step 3. Pair with another Bluetooth-enabled device.

Step 4. Enter the security PIN code.

Step 5. Test connectivity.

To enable Bluetooth on an Android phone, you can swipe from the top and tap the *Bluetooth* icon. On an iPhone, swipe up from the bottom edge of the screen to display the *Control Center*. Then tap the *Bluetooth* button to enable/disable it.

Laptops frequently use a function (Fn) key along with a key that has the Bluetooth symbol ( ) to activate Bluetooth. In Windows, search for bluetooth > *Change Bluetooth Settings* option > *Options* tab > ensure that the *Allow Bluetooth Devices to Find This Computer* checkbox is enabled.

Here are some basic Bluetooth configurations for the various operating systems after a device is powered on and ready for pairing.

- Windows—Ensure that Bluetooth is enabled. Use the *Add a Bluetooth device* link > select the device > *Next*. If the device is a Bluetooth printer, use the *Add a printer or scanner* link. You may have to enter a passkey or PIN. Verify connectivity.
- Apple iOS—Access *Settings* > *General* > *Bluetooth* > *ON*. In the *Devices* field, you should see the name of the device. Select the device > *Pair*. You may have to enter a passkey or PIN. Verify connectivity.
- Android—Access *Settings* > *Wireless and Network* > *Bluetooth Settings*. Ensure that Bluetooth is enabled > *Scan Devices*. Select the device once it appears > *Accept*. You may have to enter a passkey or PIN. Verify connectivity.

Laptops commonly have Bluetooth installed. To determine whether Bluetooth is installed in Windows, open the *Devices* Settings option. If Bluetooth is installed, a Bluetooth on/off setting appears. Bluetooth can be used to share photos or files between Android devices. To share a photo, open the photo and tap the *Share* icon > *Bluetooth* and select the Bluetooth device to share with. To share a file, open *File Manager* > select the file > tap the *Share* icon > *Bluetooth* and select the device to share with.

If a device does not have Bluetooth capability or if the Bluetooth circuitry fails and the device has a USB port, a USB-to-Bluetooth adapter can be used. Plug the dongle into a USB port on your laptop. In Windows, use the *Settings* > *Devices* > *Bluetooth* option. Your Bluetooth device appears > select *Next* > follow any additional instructions such as entering a PIN. Be sure to follow the manufacturer's directions.

IEEE 802.11 Wireless (Wi-Fi)

The 802.11 wireless standard is used to connect a mobile device to a wireless network that operates in the **2.4 GHz**, **5 GHz**, or **6 GHz** range. A wireless access point is used to coordinate and connect multiple wireless devices in the immediate area. Data rates depend on the distance from the access point and what type of walls and materials are between the mobile device and the access point. 802.11 wireless networks are commonly referred to as Wi-Fi. Table 10.7 shows the 802.11 standards related to wireless and the frequency range/speed used with each type.

TABLE 10.7 IEEE 802.11 wireless standards

Standard	Frequency range and speed
802.11a	5 GHz up to 54 Mb/s
802.11b	2.4 GHz up to 11 Mb/s
802.11g	2.4 GHz up to 54 Mb/s
802.11n	2.4 GHz and 5 GHz up to 600 Mb/s
802.11ac (Wi-Fi 5)	5 GHz up to 1+ Gb/s
802.11ax (Wi-Fi 6)	2.4 GHz, 5 GHz, and 6 GHz up to 14 Gb/s
802.11be (Wi-Fi 7)	2.4 GHz, 5 GHz, and 6 GHz up to 46 Gb/s

The reason it is important to know the frequency is so you can determine whether a mobile device can attach to the wireless network. If an 802.11n access point is used, it has the capability to be programmed in both the 2.4 and 5 GHz ranges, but someone could just configure it to operate in one of these ranges, such as 2.4 GHz. That would mean a mobile device would have to support the 802.11b, 802.11g, or 802.11n standard. The access point could also be configured to support only 802.11n devices (but this is not common except perhaps within a company). The more devices that connect and transmit/receive data on a wireless network, the worse the network's performance. Some access points allow a limited number of wired connections in addition to all the wireless devices connected to it, as shown in Figure 10.24.

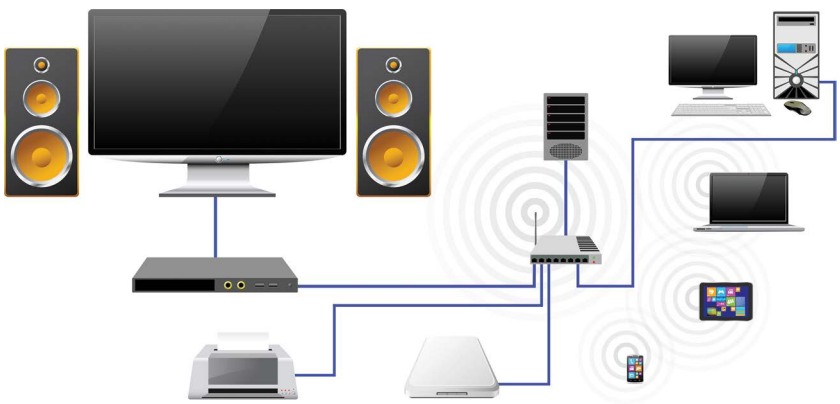


FIGURE 10.24 IEEE 802.11 wireless network

To configure a wireless mobile device for IEEE 802.11 wireless networking, ensure that the Wi-Fi option is enabled. Use the same process as outlined for enabling Bluetooth but select Wi-Fi instead. The basic configuration steps for accessing 802.11 wireless networks are as follows:

Step 1. Enable Wi-Fi through the device's *Settings* option.

Step 2. Select the Wi-Fi wireless network to join.

Step 3. Enter the security password, if required.

For a wireless network that does not broadcast the SSID (see Chapter 13, "Networking," for more information on that), the network can be manually configured on a mobile device. To manually add a wireless network on an Android device, use *Settings* > *Add Network* and manually enter the SSID, security type, and password. Similarly, on an iOS device, use *Settings* > *Wi-Fi* and follow the same process.

If the 802.11 Wi-Fi circuitry fails or is unavailable on a mobile device, and the device has a USB port, a USB Wi-Fi network card (see Figure 10.25) can be obtained and installed.

FIGURE 10.25 USB wireless NIC

Airplane Mode

Airplane Mode allows you to disable all wireless communication: Wi-Fi, mobile broadband, Bluetooth, GPS or GNSS (Global Navigation Satellite System), and NFC. In this mode, you can still view a movie or play a game, as long as doing so does not require internet, cellular, or wireless connectivity. To turn on Airplane Mode, use the *Settings* > *Airplane Mode* option. Airplane Mode saves on power, secures your mobile device because no wireless communication can occur, and is used on airplanes (hence the name) and in other communication-sensitive situations.

Table 10.8 lists the basic network connectivity configuration options for Android and Apple iOS devices.

TABLE 10.8 Mobile device network configuration options

Connectivity method	Android	iOS
802.11 wireless	*Settings > Wireless and Networks > Wi-Fi*	*Settings > Wi-Fi*
Bluetooth	*Settings > Wireless and Networks > Bluetooth*	*Settings > Bluetooth*
Cellular	*Settings > Wireless and Networks > More Networks > Mobile Networks*	*Settings > General > Cellular Data*
GPS	*Settings > Location Services > Location*	*Settings > Location*
Airplane Mode	*Settings > Wireless and Networks > Flight Mode > Airplane Mode*	*Settings > Privacy > Location Services*

Hotspot/Tethering

A Wi-Fi **hotspot** is a wireless network that provides internet access. Hotspots can be found in cities, parks, stores, restaurants, hotels, libraries, government buildings, airports, and schools; they can also be made through a cell phone or cell provider device. Security can be a concern with hotspots if no encryption or authentication is required. To configure an Android device as a hotspot, access *Settings* > *Hotspot* > *Configure*. For an iPhone, access *Settings* > *General* > *About* and name the personal hotspot; then return to *Settings* and turn on *Personal Hotspot* and configure password settings.

Another way of gaining access to the internet is through tethering. Say you are at a gas station and need to use your PC to look up something on the internet. There is no free Wi-Fi in the area, but your phone has internet connectivity. In such a case, you can get access to the internet on the PC by tethering it to your phone. **Tethering** allows sharing of an internet connection with other mobile devices in the nearby area. Tethering might also be considered to be a hotspot. Common methods of using tethering are through Bluetooth, Wi-Fi, or a wired USB connection. Some phone vendors charge for the tethering option.

Configure tethering on an Android device by using the *Settings* > *Wireless & Networks* option. Then select whether you are using USB, Wi-Fi, or Bluetooth to tether. On an iPhone, access *Settings* > enable *Personal Hotspot* > the directions for connecting through Wi-Fi, Bluetooth, and USB appear. Figure 10.26 shows wired tethering through USB and the concept of wireless tethering.

FIGURE 10.26 Wireless tethering

Near Field Communication (NFC)

Near field communication (**NFC**) is a radio-based wireless technology that allows two devices that are physically close to each other to exchange information either by being near and doing a tap, bumping the two devices, or swiping the device against an NFC reader/scanner. There are three modes of NFC operation:

- **NFC card emulation:** Enables a mobile device to act as a smart card and perform business transactions such as wireless payment-related or ticket purchases, display, inspection, or in-validation transactions
- **NFC reader/writer:** Allows an NFC device to read information from a tag
- **NFC peer-to-peer:** Allows two NFC-enabled devices to exchange information

NFC is also used to allow keyless entry into cars, buildings, and rooms, connect speakers, and provide wireless charging. If your phone has NFC capability and your printer supports NFC, then you can stand next to the printer, tap the *Print* option, and send something to the printer. Figure 10.27 shows someone making a payment for purchases by using an NFC-enabled smartphone. Note that NFC transactions are secure and commonly include a haptic (vibration) and/or audio feedback indicating that a transaction has occurred.

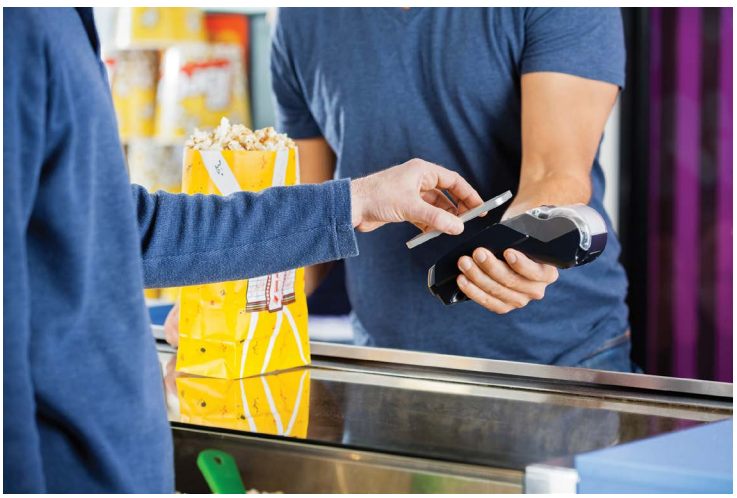


FIGURE 10.27 NFC transaction

To configure an Android device for NFC, go to *Settings* > *NFC* and ensure that it is turned on. To be able to pay using your phone, you need to have an app such as Google Wallet or Samsung Pay installed. To configure an iOS device for NFC and Apple Pay, go to *Settings* > *Wallet & Apple Pay* > add a credit or debit card, and follow the directions for the type of card chosen.

To use NFC, the devices must be within close proximity to one another (1.5 inches (38.1mm) or less), which in itself is a security feature. In addition, a user must initiate the payment process on their mobile device and may need to use two-factor authentication with a passcode or **biometric** features such as a fingerprint or face scan. Be sure to put in place security features for any device used for NFC; for example, set a password for opening the device, avoid storing username or login information on the mobile device, and have antivirus/anti-malware software installed.

Some mobile devices, such as the Microsoft Surface machines and Dell, HP, and Lenovo business laptops, have NFC built in so that a user can authenticate to their device and exchange data with a nearby NFC-enabled device or gain access to specific files or apps.

Using NFC is as easy as tapping an NFC-enabled token, key, or badge (commonly located near the touchpad or on the display corner) to an NFC sensor. Note that the NFC key might have a USB connector as well, as shown in Figure 10.28.

FIGURE 10.28 NFC key

Infrared

Infrared (**IR**) is a radio-based wireless technology that operates in the 300 GHz to 430 THz range, but many devices use either 2.4 GHz or 27 MHz. IR is used for very short distances and is cheaper than other wireless technologies. IR requires line of sight; anything from a human to a chair can get in the way and cause lack of connectivity. For that reason, IR is commonly used for short distances to connect wireless devices such as motion detectors, intrusion detectors, TV remotes, hand scanners, a mouse, or a keyboard.

Cellular Data

Cellular data usage is usually tracked and, unless you have an unlimited data plan, charged for. Cellular data is any type of data sent over a cellular network, including emails, web pages viewed, music streamed, photos or videos uploaded or downloaded, and text messages. Two methods for sending data over a cellular network are Short Message Service (SMS) and Multimedia Message Service (MMS). SMS is used for text messages, and MMS is used for visual data such as photos or video.

Many phone providers charge for these services, so some users disable them. On an iOS device, use *Settings* > *General* > *Cellular Data*. On an Android device, access *Wireless and Networks Settings* > *Mobile Networks* > *Data*. A **data cap** is a limit on the amount of data that can be used by an internet subscriber. Some vendors throttle or slow down internet access once the data cap has been reached, and some imposed additional fees. Using nearby wireless networks for data transmission instead of the cellular network helps reduce cellular data usage.

Mobile apps can be set to use cellular data, and a large number of ads will increase data usage. To block ads on an Android device, use *Settings* > *Site settings* > *Pop-ups and redirects* > *Ads blocked*. For an iPhone or iPad, use *Settings* > *Privacy* > *Apple Advertising*. You can also use an ad blocker.

Mobile Device Email Configuration

Many people want to check their email on a mobile device. Email can be accessed and delivered using a variety of protocols, including the following:

- **Post Office Protocol version 3 (POP3):** Used to retrieve email using TCP port 110; saves email to the local device.
- **Internet Message Access Protocol (IMAP):** Used to retrieve email using TCP port 143; good when two or more people check the same account or a user wants email access from multiple devices.
- **Secure Sockets Layer (SSL)/Transport Layer Security (TLS):** Used to encrypt data between an email client and the email server.
- **Simple Mail Transfer Protocol (SMTP):** An older protocol used to send emails using TCP port 25.
- **Multipurpose Internet Mail Extensions (MIME) and Secure MIME (S/MIME):** Used along with SMTP so that pictures and attachments are supported; S/MIME allows encryption and signing of MIME data.
- **Exchange Online:** Microsoft's application that uses the messaging application programming interface (MAPI) to connect to Microsoft Exchange servers for email, calendar, and contact information. Microsoft supports storing copies of messages or calendar events in personal storage table (`.pst`) files, such as when items from the Microsoft Exchange server are archived and stored locally.

The email server used determines which email client may be used on a mobile device. Several key pieces of information are commonly needed to configure the client (see Table 10.9). Some

organizations configure the email server to support autoconfiguration (sometimes called autodiscovery) so that all you have to enter is a username and password, and all the other configuration parameters are automatically provided to the device. Not all email client apps support autoconfiguration. You might have to get the email configuration parameters from the IT support staff, an FAQ page, or a website.

TABLE 10.9 Email configuration parameters

Parameter	Description
Email address	The address used to send you an email, such as cheryl.schmidt@gmail.com.
Email protocol	The protocol(s) used to send and receive email.
Server name or host name	The name of the incoming or outgoing mail server (which you can get from network staff).
Username	The name assigned to you by the company that hosts the email server. This may be your email address.
Password	The password used in conjunction with a username to access an email account.
Domain	The network domain name.
SSL/TLS	Secure Sockets Layer (SSL)/Transport Layer Security (TLS), when enabled, is used to encrypt data between the mobile device and the email server.

Most mobile devices include email configuration as part of the mobile OS. Common email providers include Yahoo, Outlook, AOL Mail, Microsoft Exchange (included with Microsoft 365) Google Gmail, and Apple Mail, as well as other commercial email providers, such as Airmail, GMX, Canary Mail, Samsun Email, and ProtonMail.

When you first configure an Android device, you are prompted to either enter your Google account information or create a Google account. The email app that comes with the phone simply opens Gmail. You can add an account by selecting *Settings* > *Email* option. Use the *Personal (IMAP/POP)* option for selecting which protocol is used to access email. Use the *Exchange* option for configuring Microsoft Exchange.

Similarly, on Apple iOS devices, use *Settings* > *Passwords & Accounts* (or *Mail, Contacts, Calendars* on older versions, as in Figure 10.29) > select *Add Account* > select the particular type of account desired (Exchange, Google, Yahoo, and so on).

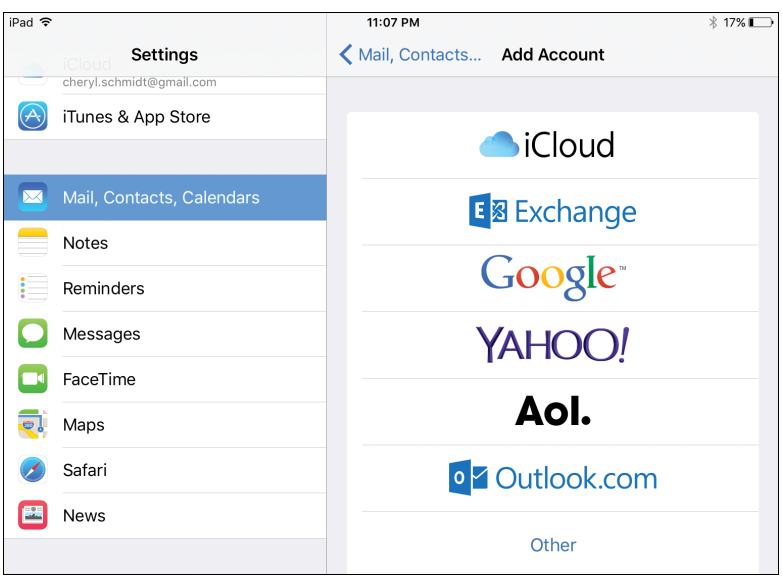


FIGURE 10.29 Email configuration on an iOS device

Mobile Device Synchronization and Backup

Synchronization means making the same data available on multiple devices and/or in multiple locations. Synchronization is sometimes known as a **remote backup**, cloud backup, or **cloud storage** (which can be used not only for backup but for any type of data). The types of data synchronized include **contacts**, applications, email, pictures, music, videos, **calendar** appointments, browser bookmarks, documents, folders, location data, social media data, e-books, and passwords.

Synchronization makes life easier because you do not have to log in to a work computer or bring up a web browser in order to see what is scheduled tomorrow. You can also synchronize your fitness results and maintain them on both your cell phone and mobile fitness device or smartwatch.

TECH TIP

Think before you sync

Be careful about synchronizing cached passwords (that is, passwords you have directed the browser, operating system, or app to save) across the cloud because as such transmissions can have security ramifications. There are also issues synching music files due to file formats and multiple platforms (Apple, PC, car, mobile device, for example). Be sure to research your synchronization method.

Synchronization Methods

Synchronization can be done through a particular operating system, browser, email provider, applications, and/or third-party vendors. For example, Microsoft has a product called **OneDrive** that can be used for synchronization and/or backup and restore operations. People who use Microsoft Outlook through an Exchange server from any mobile OS can save files and photos to OneDrive and then access them through a web browser or mobile device app. Microsoft Exchange ActiveSync is used to synchronize a person's contacts, calendar, and email. Use *Settings* > *Mail* > *Accounts* on an iPhone or iPad to configure Exchange ActiveSync. Use *Settings* > *Accounts* > *Sync* on an Android device.

TECH TIP

Watch out for data caps when synching

Keep an eye out for storage limits when synchronizing data.

People commonly use one or more of the following synchronization methods for mobile devices:

- **Synchronize to the cloud:** It is possible to store data in a remote location, where it can be viewed, retrieved, saved, shared, and/or forwarded based on the cloud vendor used and user preferences (see Figure 10.30).
- **Synchronize to the desktop:** A mobile device can be synchronized with one or more desktop computers using an app, software, the operating system, or a combination of these.
- **Synchronize to the automobile:** It is possible to connect/synchronize a Bluetooth headset, smartphone, or other mobile device to a car. A vehicle, for example, can sync to a cell phone, and the address book is transferred to the car and kept in an internal database.

Note that whichever synchronization type is used, it is important that the software requirements needed to install the app and actually synchronize the data are met on each of the devices that have data to be synchronized.

FIGURE 10.30 Synchronization to the cloud

TECH TIP

Use vCards for synching contacts

A vCard (also known as a virtual contact file [VCF]) is used for electronic contact information; it is basically an e-business card. A vCard file can have the extension `.vcf` or `.vcard`. If a vCard is imbedded in an email, you can normally right-click on and add it to your contacts.

Synchronization Connection Types

In order for devices to synchronize data, they have to establish connectivity with each other. Synchronization commonly occurs using one of three types of connections:

> **Wired USB connection:** Two devices may attach to one another using a USB port on each device. An example is an iOS device connected via USB to a computer and using iTunes to synchronize music.

> **Wireless connection:** Devices can attach to one another using any wireless method, including an 802.11 Wi-Fi connection and cellular network.

> **Wired network connection:** Devices can attach to a wired network and access the internet and a cloud-based solution through a web browser.

Figure 10.31 shows synchronization between a mobile phone and a desktop computer.

FIGURE 10.31 Synchronization between a mobile phone and a PC

Synchronization on Android Devices

Google software is commonly used to synchronize data between an Android device and other devices. Google Drive can be used to store and share documents for free. The Google Chrome browser allows bookmark synchronization. Google Photos allows storage and sharing of photos. When you use Google software to synchronize, an Android user authenticates once in order to access multiple services. This is known as mutual authentication for multiple services, or single sign-on (SSO), and it is available through the other mobile operating systems as well. When you use a third-party product to synchronize data, you may be required to install an app on one or more mobile devices and PCs.

An Android device is configured with a Google ID and password using the *Settings* > *Accounts* option and then the three vertical dots in the top-right corner can be tapped to select what to synchronize. Figure 10.32 shows the synchronization settings for email (which is turned on).

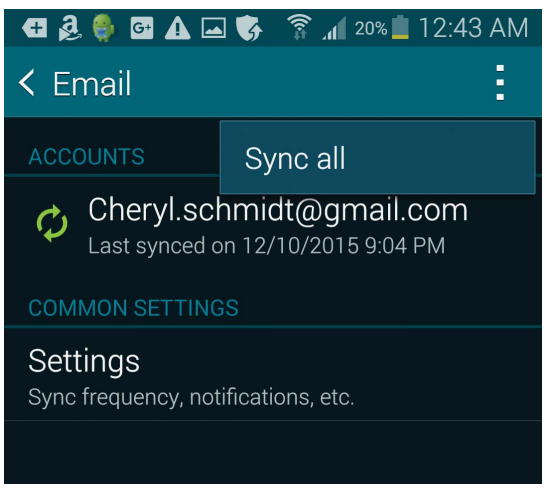


FIGURE 10.32 Android email synchronization

Synchronization on iOS Devices

iOS devices can use Google Gmail and other apps to synchronize Google contacts and calendar. An individual app may also support synchronization with Google. You can view and add apps by using *Settings* > *Personal* (which is not used on some Android devices) > *Accounts and Sync* or whatever method is used by the particular application.

iOS users tend to use Apple solutions, such as iCloud and iTunes, for synchronization. iCloud is used to store, share, and manage data from any device, including contacts, calendar, ringtones, photos/videos, and data. Apple provides iCloud Photo Library for photos and video and iCloud Drive for document storage. Apple provides free storage with the option to pay for more. A Windows device requires download and installation of iCloud for Windows in order to access data stored there. Figure 10.33 shows the configuration for iCloud on an iOS device.

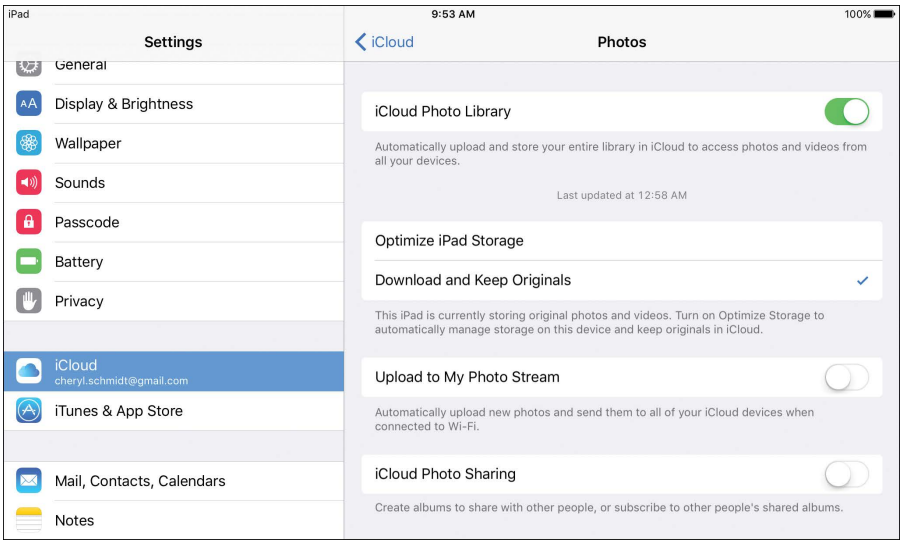


FIGURE 10.33 iCloud configuration screen

iTunes can be used to synchronize Apple devices and to play and manage music, video, books, and lectures. You can also synchronize your data using Apple apps. iTunes is available in a 64-bit version for Windows (but not for Android devices).

Backup and Restore Overview

Synchronization of apps is one way of backing up information, but it doesn't provide an operating system backup. A mobile device should have the system backed up in case of an operating system update failure, a virus infection, or inability to remove malware. Apps are available that allow you to remotely back up a mobile device. Backup and restore techniques are just as important in the mobile environment as they are in the desktop arena.

Android-Based Backup and Restore

Android devices have different backup options based on what type of data you want to back up and/or restore. The Android Backup Service backs up the following data and settings: Google Calendar, Wi-Fi networks and passwords, home screen wallpaper, Gmail settings, apps installed through Google Play and backed up using the Play Store app, display settings, language settings, input settings, date and time, and some third-party app settings and data.

Sometimes you may need to do a **factory reset**, such as when a device cannot be repaired using any other method. As the name of the option implies, it resets the mobile device to the original settings. Android phones keep the OS separate from the apps and data. The OS is read-only. A factory reset resets only the apps and data. That is why you need to back them up.

iOS-Based Backup and Restore Overview

With iOS you can back up your operating system using iCloud or iTunes. If you use iCloud, the backup is stored in the cloud (up to 5 GB free at press time), it is encrypted, and it can be

accomplished wirelessly. With the Apple Devices app, the backup is stored on a Mac or PC, the storage limit is based on storage available on that Mac or PC, and encryption is optional.

iCloud Backup and Restore Overview

iCloud backups do not include data that is already in the cloud, data from other cloud services, Apple Pay information, Touch ID, or content that you got from other vendors (even if available in iTunes or iBooks). In order to make a backup using iCloud, ensure that the device connects to a Wi-Fi network > *Settings* > *iCloud Backup*/*Storage & Backup* > enable (turn on) iCloud Backup > *Back Up Now*.

You can verify that the backup is stored by using the following steps: *Settings* > *iCloud* > *Storage* > *Manage Storage* > select the device. The details shown include the date, time, and backup file size. Backups are automatically made on a daily basis if the device meets the following criteria:

- The device connects to a power source.
- The device connects to a Wi-Fi network.
- The device has a locked screen
- iCloud storage space is available.

Other Mobile Software Tools

Mobile devices sometimes require other tools for troubleshooting and management. You might also have to download apps to perform specific tasks or to help with troubleshooting. You might consider installing some of the apps described in the following sections as a standard in a business environment.

Mobile Device Management

Mobile device management (**MDM**) is the ability to view and manage multiple mobile devices (see Figure 10.34). In a corporate environment, mobile devices are challenging for IT staff. Companies use MDM to push OS and **application updates** and to track and remotely wipe data and configurations. **Configuration profiles** can be used to customize the settings based on the employee role. Mobile application management (MAM) is used to control corporate applications on mobile devices that may be employee personal devices. MAM allows new apps to be pushed out after testing, allows updates to be controlled, and enables additional device management and/or security features. Examples of corporate applications include project management software, enterprise resource planning (ERP) dashboards (that is, the main business programs for purchasing, payroll, HR, and so on for the running of the business), productivity apps (such as word processing and spreadsheet apps), and travel, communication, and mobile pay apps.

MDM is used to register a mobile device on the corporate network, track the device, provide app updates, configure and monitor devices, provide **policy enforcement**, and enable remote troubleshooting. Some companies allow employees to use their own devices via a bring your own device (**BYOD**) policy, which adds additional challenges for IT personnel. While BYOD allows an employee to work on their platform or OS of choice and may potentially save the company hardware costs, the company may need to enforce an acceptable use policy when the device is used for company business. The company MDM tool may monitor/track a user's device, ensure that it has the proper OS version/update as well as anti-malware software installed, and ensure security compliance.

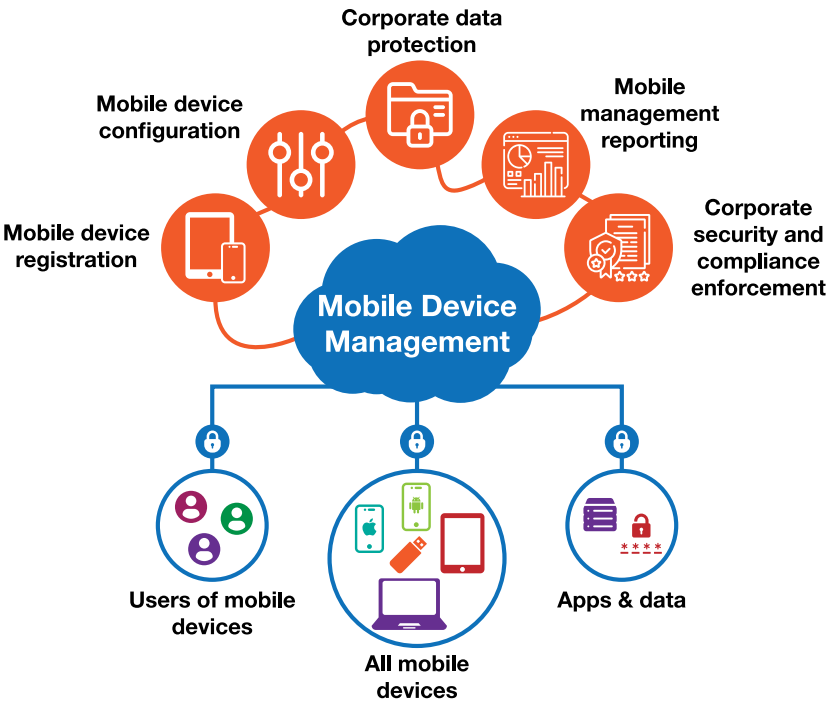


FIGURE 10.34 Mobile device management

Mobile Antivirus/Anti-malware

Mobile devices can have **malware** (software that causes a device to misbehave or spy on the user) installed, just as desktop computers can. See Chapter 18, "Computer and Network Security," for more details on security issues such as malware. A variety of products are available for mobile devices, such as Malwarebytes for anti-malware and AVG Antivirus security for multiple security threats. Free versions typically have antivirus and/or anti-malware. Paid versions add features such as app backup, app locks, SIM locking, antitheft, antiphishing, tracking, and secure web browsing.

App Scanner

One way of preventing malware and preventing apps from revealing your personal information is to install an app scanner. An app scanner is an online tool in which you can type the name of an app to see whether any of your data is at risk and generate a risk score to get an idea of how risky the app is. Other app scanners may be part of security apps, such as Sophos Mobile Security. There are also app scanners that manage particular apps and ensure compliance, cloud-based management for specific mobile devices, and enterprise-based mobile device management.

Wi-Fi Analyzer

A **Wi-Fi analyzer** app (sometimes known as a wireless locator, Wi-Fi scanner, or wireless scanner) is used to identify what wireless networks are in the area and what frequencies (channels) are being used and to find less crowded channels for any wireless installations, hotspot, or tethering that may be needed in a particular area. Some Wi-Fi analyzers give you additional feedback, such as a quality rating based on the channel you might select. One optional feature is a signal meter to see the wireless range of a particular wireless network. Wi-Fi analyzers are particularly useful to technicians in allowing them to identify potential sources of other wireless interference. See Chapter 13 for more detail on wireless networks and wireless configuration. Figure 10.35 shows a Wi-Fi analyzer.

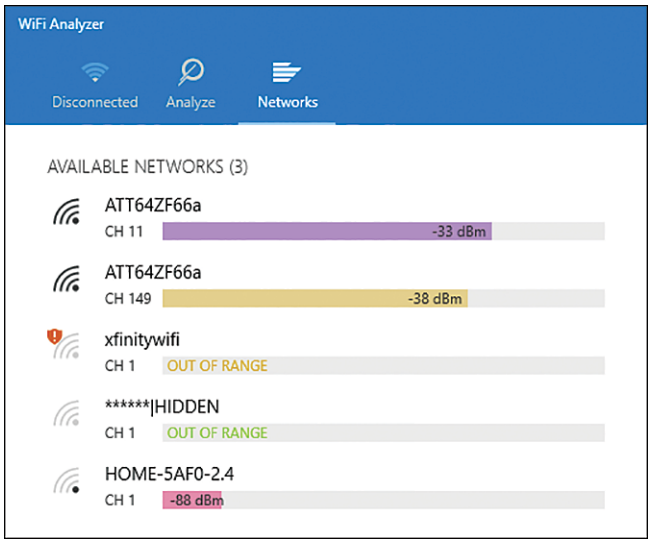


FIGURE 10.35 Wi-Fi Analyzer app screen

Cell Tower Analyzer

A cell tower analyzer app (also known as a cell signal analyzer) provides details about the cell phone network and possibly wireless networks. The information can include signal strength, data state, data activity, mobile network code (MNC), mobile country code (MCC), IP address, roaming state, phone type, and so on. You can use other apps to see all the cell towers in the area in order to get an idea of cell phone coverage in the areas most used.

Laptops Overview

Mobile devices are fun to explore, but let's move on to laptops now. Laptops were the first mobile devices that technicians had to support. They are an integral part of the IT scene. Anyone in an IT position is expected to know some technical laptop basics. Technical support staff are expected to know more. Keep in mind that every laptop is different. Consult the particular computer manufacturer's website for instructions on replacing anything on your laptop.

Laptop Hardware

A laptop has parts and ports that are similar to those of a desktop computer, but some of these components are, naturally, smaller. Figure 10.36 shows common laptop parts. Notice in the figure how many of the components are built into the laptop motherboard.

Whenever taking anything out of a laptop, one of the major issues is that tiny screws could be hidden under plastic or rubber caps; most screws are accessible from the bottom of the laptop (see Figure 10.37). Use a magnetic screwdriver to remove the screws or place the screws on a magnetized tray. Some manufacturers label the type of screws or location for ease of explaining disassembly. Keep like screws together (in containers or an egg carton) and take notes and photos. All the parts are manufacturer dependent, but the following explanation and graphics and photos should help.

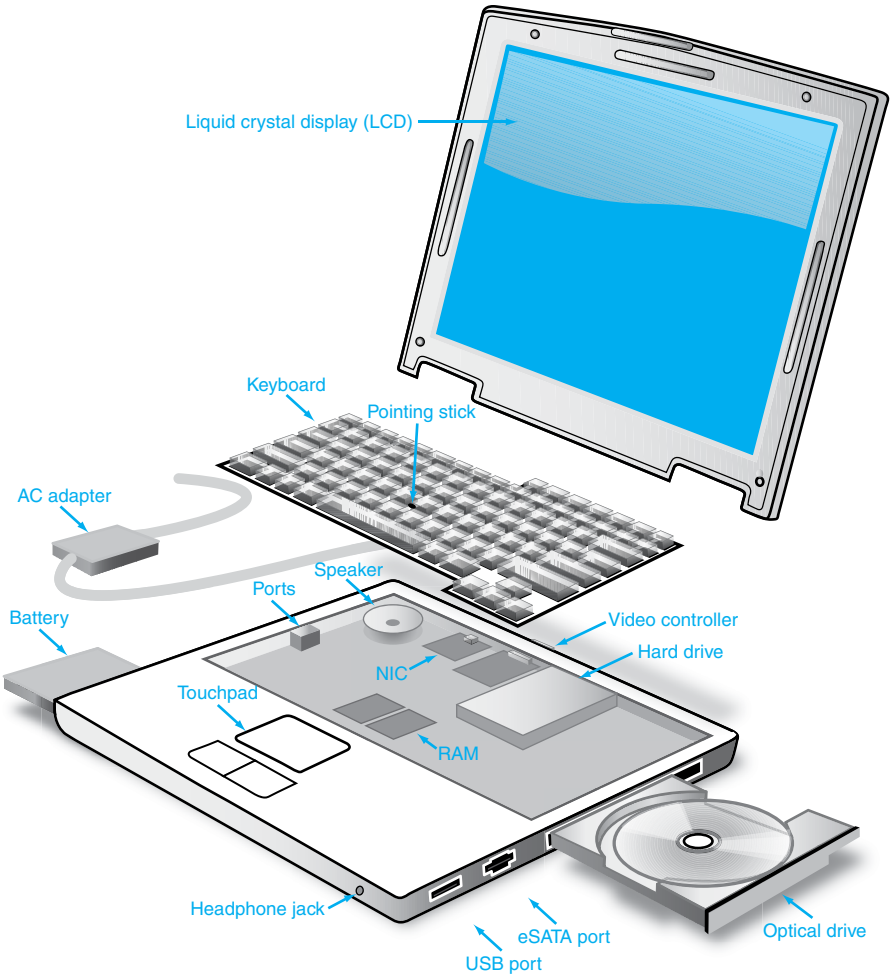


FIGURE 10.36 Laptop parts

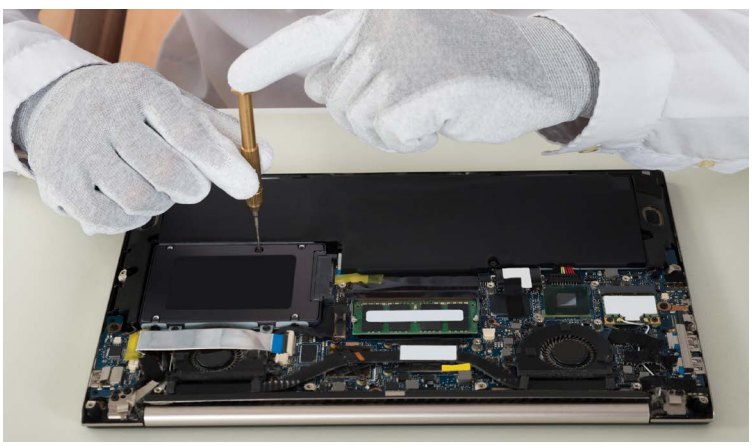


FIGURE 10.37 Laptop screws and covers

External Laptop Devices

Laptops might also have external devices attached. The USB port is the port used most commonly for external connectivity. For laptops that do not have a USB port, you can use an eSATA port for an external device or add a USB hub. Types of external connectivity include the following:

> **External monitor:** An external monitor attaches to a video or USB port. Common video ports on laptops include USB, VGA, HDMI, Thunderbolt, and DisplayPort. HDMI can carry audio and video signals. Thunderbolt can carry not only video but data and power as well. That is why Thunderbolt can be used for other connections besides video connections. Thunderbolt is also used to connect to docking stations (covered next). Some devices have miniature versions of these ports. Figure 10.38 shows the difference between DisplayPort and mini DisplayPort.
> **External hard drive:** An external hard drive commonly connects to a USB, Thunderbolt, or eSATA port.
> **External optical drive:** An external optical drive commonly connects to a USB port.

FIGURE 10.38 DisplayPort and mini DisplayPort

Some people like having more expandability when in the office than when traveling with a laptop. For these folks, two devices can help: a docking station and a port replicator. A **laptop docking station** allows a laptop computer to be more like a desktop system. A **docking station** can have ports for charging devices and connections for a full-size monitor, keyboard, mouse, and printer. In addition, a docking station can have expansion slots or cards and storage bays.

Docking stations tend to be vendor proprietary, which means that if you have a particular brand of laptop, you must use the same brand of docking station. Typically, to install a laptop into a docking station, you close the laptop and slide the laptop into the docking station. Figure 10.39 shows the concept of a laptop docking station and the ports that can be found on the back.

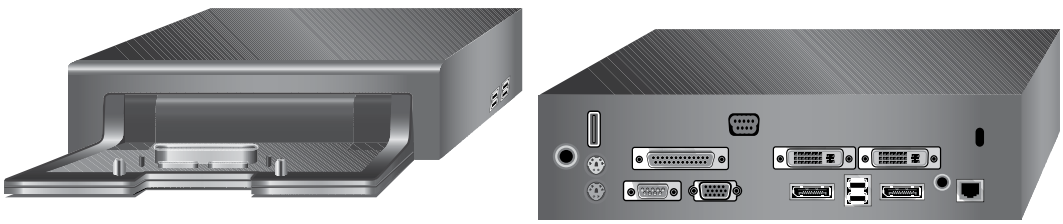


FIGURE 10.39 Laptop docking station

A **port replicator** is similar to a docking station but does not normally include expansion slots or drive storage bays. A port replicator attaches to a laptop and allows more devices to be connected, such as an external monitor, keyboard, mouse, and printer. Port replicators can be proprietary or may support multiple laptop vendors.

Other Laptop Expansion Options

Laptops can also be expanded by adding expansion cards. The **miniPCIe** is a 52-pin card that fits in the bottom of a laptop or on the motherboard/system board (but not in a tablet). Two uses are to install a wireless card or a cellular card. A **wireless card** is used to connect a laptop to an IEEE 802.11 or Bluetooth wireless network. A **cellular card** is used to connect a laptop to the cell phone network. Note that some adapters have both wireless and cellular abilities built into the same card. Also, these adapters could be attached via a USB port instead of a miniPCIe adapter.

To install a miniPCI/PCIe adapter, you may have to disassemble the laptop or remove a screw from the bottom, as shown in Figure 10.40, or you may have to lift a lid to access the slot. An expansion slot is shown in Figure 10.41.

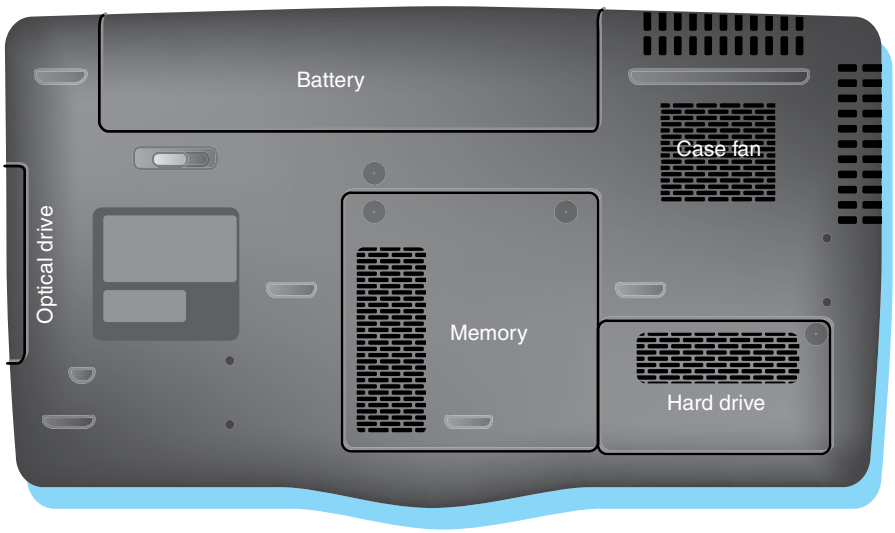


FIGURE 10.40 Laptop underside

FIGURE 10.41 Laptop expansion slot

M.2 and NVMe

A type of expansion slot found in both laptops and desktop computers is M.2. The **M.2** expansion slot is quite flexible in that the specification allows different module sizes, including widths of 12, 16, 22, and 30 mm and lengths of 16, 26, 30, 38, 42, 60, 80, and 110 mm. Usually a longer slot allows the short cards to be installed. You will see card sizes that are made up of both numbers—for example, 2280. M.2 cards are also keyed, with B, M, and B+M being the most common keys. A card with the B key uses two PCIe lanes, and an M key uses up to four PCIe lanes. Look back at Figure 7.9 in Chapter 7, "Storage Devices," to see this again.

M.2 expansion cards in laptops and desktop computers are used for Wi-Fi, Bluetooth, and cellular network cards as well as solid-state drives (SSDs). The support of various card lengths and advanced technology makes M.2 an attractive expansion capability option for SSDs and cards in all computer systems and mobile devices. Figure 10.42 shows an M.2 Wi-Fi expansion card and an SSD.

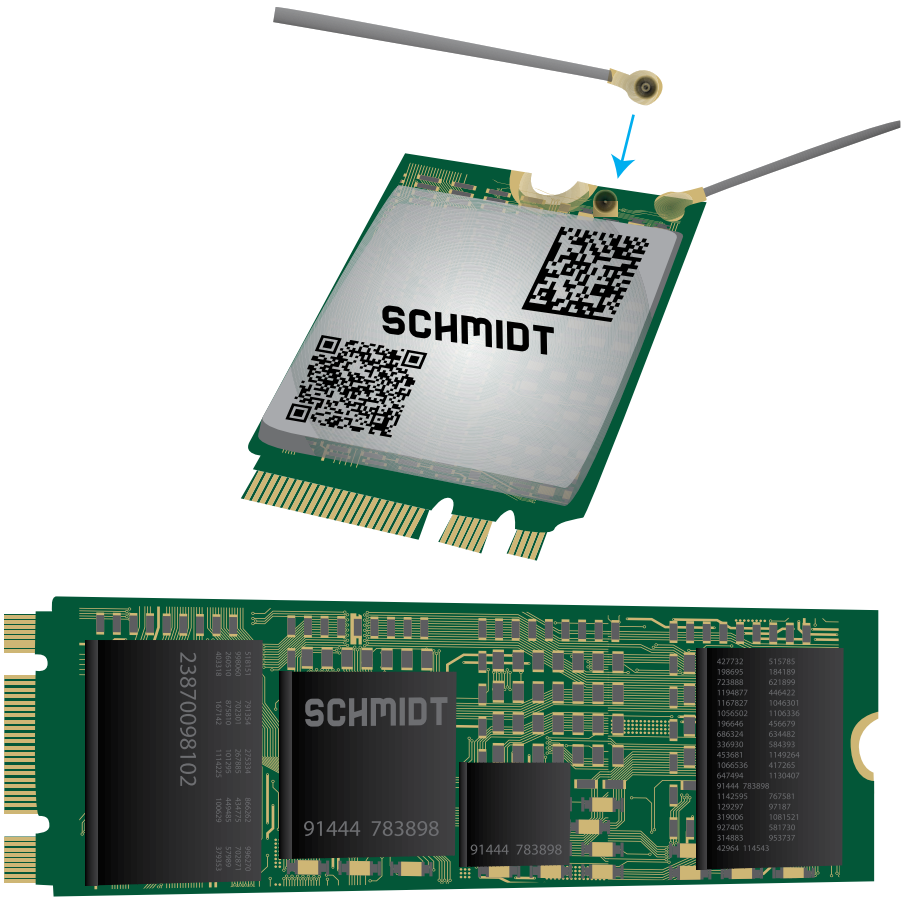


FIGURE 10.42 M.2 wireless card and SSD

SSD storage comes in the form of 2.5-inch cases, mounted on a PCIe card for desktops, on an M.2 card, and on a Non-Volatile Memory Express (**NVMe**) card. For a laptop, an SSD on an NVMe is the fastest option. M.2 and the 2.5-inch case connect to a µSATA (microSATA) connection. The NVMe card uses the PCIe bus and provides a faster connection but is more expensive. Look back at Figure 7.10 to see an NVMe card.

Laptop Power

A laptop normally uses a battery as its power source, but a laptop can also be powered through an AC wall outlet connection that recharges the laptop battery. A power adapter (sometimes called a wall adapter) converts the AC power from the wall outlet to DC and connects to the rear of the laptop (near where the battery is located). When a laptop has an AC adapter attached, the battery is being recharged on most models. The port sometimes has a DC voltage symbol below or beside it. This symbol is a solid line with a dashed line below it (⎓). Note that the laptop manufacturer might also support a wireless charging mat that allows a laptop battery to be charged without an AC adapter. Figure 10.43 shows an example of a power adapter that would be connected between the laptop and the AC outlet and the power connection on a laptop.

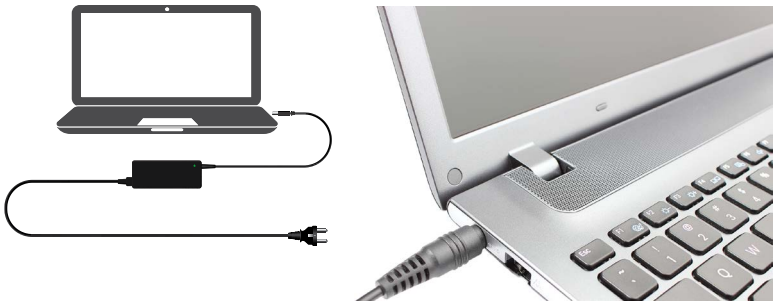


FIGURE 10.43 Laptop power adapter and power connector

When purchasing a new power supply for a laptop or battery for a mobile device, ensure that it has the same specifications as the one from the manufacturer. Less expensive replacements might not provide the same quality as approved models. Ensure that the replacement has a power jack that does not wiggle when it is inserted into the device. Ensure that a laptop power brick has the appropriate DC voltage required by the laptop. Current (amperage) should be equal to or greater than in the original power brick.

TECH TIP

Do not power on after a temperature change

Computers are designed to work within a range of temperatures, and sudden temperature change is not good for them. If a mobile device is in a car all night and the temperature drops, allow the device to return to room temperature before powering it on. Avoid direct sunlight. It is usually 40°F hotter inside the computer case than outside it.

Laptop Battery Removal

Laptop batteries fail, or you might experience **improper charging** and need to replace a battery. Ensure that you disconnect the AC adapter and power off a laptop before removing its battery. You may have to turn the laptop over to access the battery compartment. Laptop batteries are normally modules that have one or two release latches that are used to remove the module (see Figure 10.44).

FIGURE 10.44 Release latch for laptop battery removal

Battery technologies have improved in recent years, partly driven by the development of more devices that need battery power, such as tablets, digital cameras, and portable optical drive players. Laptops use lithium-ion (Li-ion) batteries, which are very light and can hold a charge longer than any other type. They are also more expensive than other battery types. Mobile phones, tablets, portable media players, and digital cameras also use Li-ion batteries. These batteries lose their charge over time, even if they are not being used. Use your laptop with battery-provided power. Some vendors recommend not leaving a laptop with a Li-ion battery plugged into an AC outlet all the time.

TECH TIP

Keep Li-ion batteries cool

Li-ion batteries last longer if they are kept cool (not frozen). When you store a Li-ion battery, the battery should be only 40% charged and placed in a refrigerator to prolong its life.

Li-ion polymer batteries are similar to other Li-ion batteries except that they are packed in pouched cells. This design allows for smaller batteries and more efficient use of space, which is important in the portable computer and mobile device industries. For environmentalists, the zinc-air battery is the one to watch. AER Energy Resources, Inc., has several patents on a battery that uses oxygen to generate electricity. Another upcoming technology is fuel cells. Fuel cells used for a laptop can provide power for 5 to 10 hours.

Getting the Most from Your Laptop Battery

Mobile devices rely on their batteries to provide mobility. The following tips can help you get more time out of your batteries:

- Most people do not need a spare Li-ion battery. If you are not using a Li-ion battery constantly, it is best not to buy a spare. The longer the spare sits unused, the shorter the life span it will have.
- Buy the battery recommended by the laptop manufacturer.
- For a mobile device or smartphone, use an AC outlet rather than a USB port for faster charging.
- If using a USB port for charging a mobile device or smartphone, unplug all unused USB devices. Note that not all USB ports can provide a charge if the host device is in sleep mode.
- Avoid using an optical player when running on battery power.
- Turn off the wireless adapter if a wireless network is not being used.
- In the power options, configure the mobile device for hibernation rather than standby.
- Save work only when necessary and turn off the autosave feature.
- Reduce the screen brightness.
- Avoid using external USB devices such as flash drives or external hard drives.
- Install more RAM to reduce swapping of information from the hard drive to RAM to CPU or to just be more efficient.
- In mobile devices, keep battery contacts clean with a dab of rubbing alcohol on a lint-free swab once a month.
- Avoid running multiple programs.
- If possible, disable automatic updates.
- Avoid temperature extremes.
- Turn off location services.

Select a *Power & sleep* Settings Windows link for a laptop: *On battery power, turn off after, When plugged in turn off after,* or *When my PC is asleep and on battery power, disconnect from the network*. Users and technicians should adjust these settings to best fit how the laptop or mobile device is used. The *Additional power settings* link opens up the *Power Options* Control Panel and allows customization of a power plan, as shown in Figure 10.45.

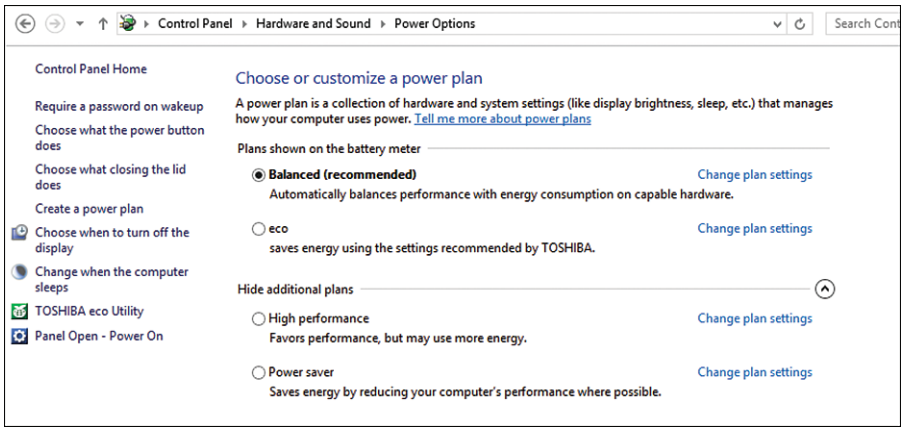


FIGURE 10.45 Laptop power settings

Another way to control the power settings on a Windows laptop is through the battery meter in the bottom-right corner of the screen on the taskbar. When you hover a pointer over the battery meter, the percentage of battery power remaining is shown. By clicking on the meter, you can change the power option or adjust the screen brightness.

Laptop Repairs Overview

It is a bit more difficult to get replacement or upgrade parts in a laptop than in a desktop PC. Most laptop parts are manufacturer dependent except for storage devices and memory. Laptop repairs require more attention to detail than do desktop repairs because there are so many screws, the screws are much smaller, and there is little space in which to work. Be patient. The following is a good list of items to remember when disassembling and reconnecting everything in a laptop:

- Use proper antistatic procedures. There are not always good places to attach an antistatic wrist strap. Consider using antistatic gloves (refer to Figure 5.3 in Chapter 5, "Disassembly and Power"). Maintain skin contact when touching parts if no other antistatic tools are used; this is known as self-grounding.
- Organize your parts. Use an egg carton and label individual sections with screws of like length and type, as well as where the screws came from. Otherwise, place like screws on tape that is sticky side up to and make notes to go with them.
- Take photos.
- Take notes.
- Use appropriate tools. Scribes, described shortly, are very handy when removing plastic pieces. Very thin needle-nose pliers are great with laptop connectors. It is important to have #1 and #0 Phillips screwdrivers.
- Refer to the manufacturer's directions when removing and installing parts. Having a tablet or phone you can use to pull up this document while you work is fine. Use your resources. No person can know all models of all machines they work on.

Some laptop and mobile device compartments require levering the compartment cover away from the case or removing plastic parts such as the cover or frame that fits over a mobile computer keyboard. A plastic **scribe** is the best tool to use for this levering. Figure 10.46 shows a plastic scribe being used to lift the plastic part that is between the keyboard and the laptop case.

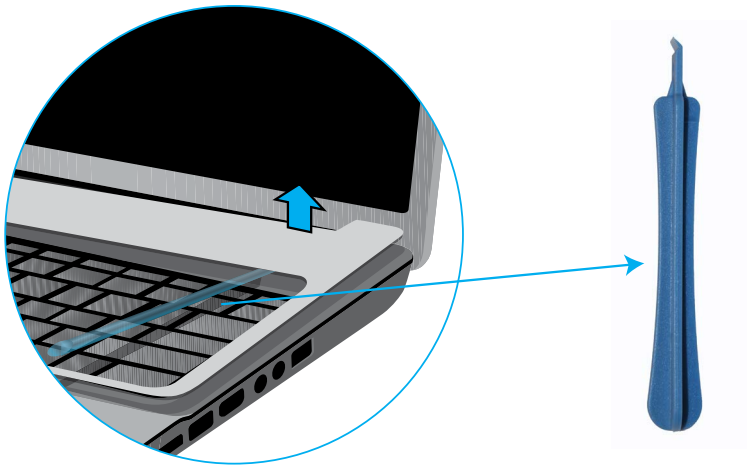


FIGURE 10.46 Plastic scribe

Laptop Motherboard/Processor Replacement

A laptop or **mobile motherboard** (system board) is similar to a desktop motherboard. It holds the majority of the electronics, contains a processor, has memory, is usually vendor specific, and supports having ports attached. The processor on a mobile device is typically not as powerful as the processor on a desktop model, it might have less memory that may not be upgradable, and it has fewer ports. However, some powerful laptops have more power, upgradability, and ports than some low-end desktop models.

In order to get to the motherboard, at a minimum, screws from the underside of the laptop have to be removed. Sometimes a hard drive, a drive that inserts on the side, the keyboard, and memory must be removed before you can remove the motherboard. Figure 10.47 shows a laptop motherboard.

FIGURE 10.47 Laptop motherboard

Before replacing a motherboard, it is important to do all the following:

- Disconnect the AC power connector.
- Remove the battery.
- Disconnect external devices, such as the mouse, keyboard, and monitor.
- Remove adapters.
- Remove memory from expansion slots.
- Disconnect cables, taking care to use any release tabs and not to pull on the cables but on the connector. Needle-nose pliers or tweezers may be needed.
- Remove the optical drive and hard drive.
- Remove the processor and cooling assembly. Note that this may be done after removing the motherboard. Store the processor in an antistatic bag. It will have to be reinstalled, and some new thermal paste may need to be applied when the new motherboard is installed.
- Remember that replacement motherboards do not come with RAM, a processor, or adapters.
- Make a note or take a photo of the CPU orientation before removing it from the bad/older motherboard.

Laptop processors are not normally upgraded, but they do sometimes have to be replaced. Refer to the laptop documentation for motherboard removal procedures. Power off a laptop and remove the laptop battery before working inside the machine. Use proper grounding procedures. A laptop processor may have a heat sink and/or fan assembly attached (refer to Figure 10.47). Furthermore, some processor sockets may need to be loosened, or a screw may need to be loosened/removed before you lift the processor from the socket, as shown in Figure 10.48.

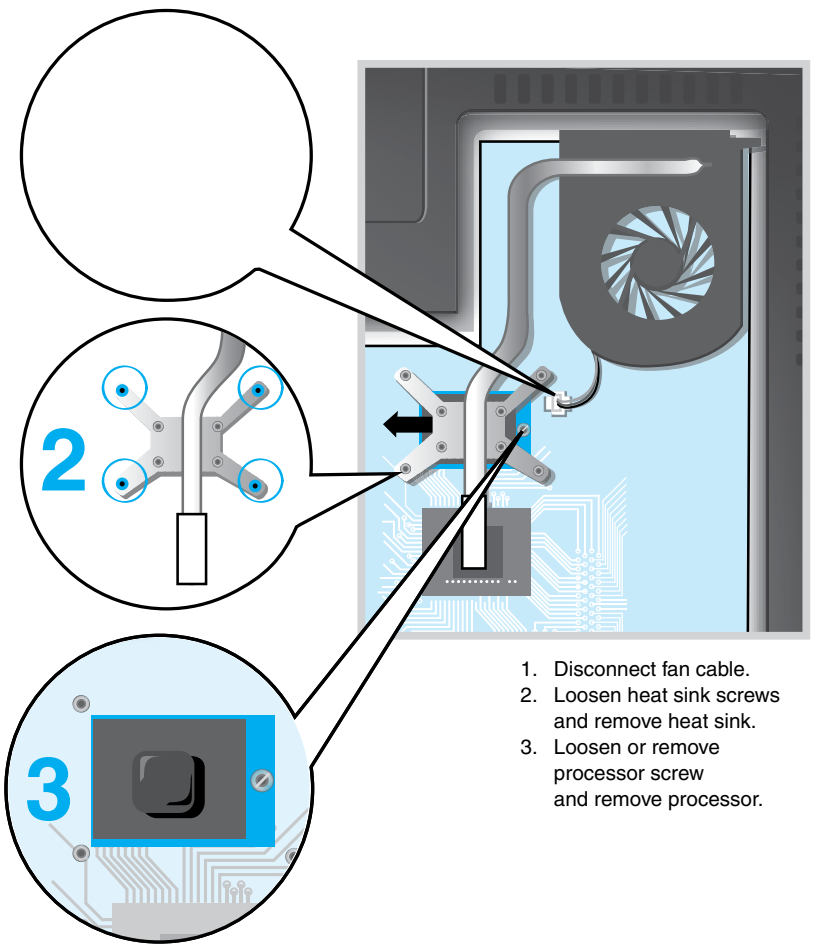


FIGURE 10.48 Laptop processor removal steps

Laptop Keyboards/Touchpad Removal/Installation

Laptops usually have integrated keyboards and a variety of mouse replacement devices, such as a touch stick, touchpad, and/or one or two buttons used for clicking and right-clicking. You should remove the battery and AC power cord before removing a laptop keyboard or any other internal laptop part. To remove a laptop keyboard, you commonly remove screws from the top or bottom of the laptop and slide or lift the keyboard out of the case. Refer to the manufacturer's documentation before removing or replacing a laptop keyboard.

Figure 10.49 shows the laptop keyboard removal process. Figure 10.50 shows a laptop keyboard that has been removed.

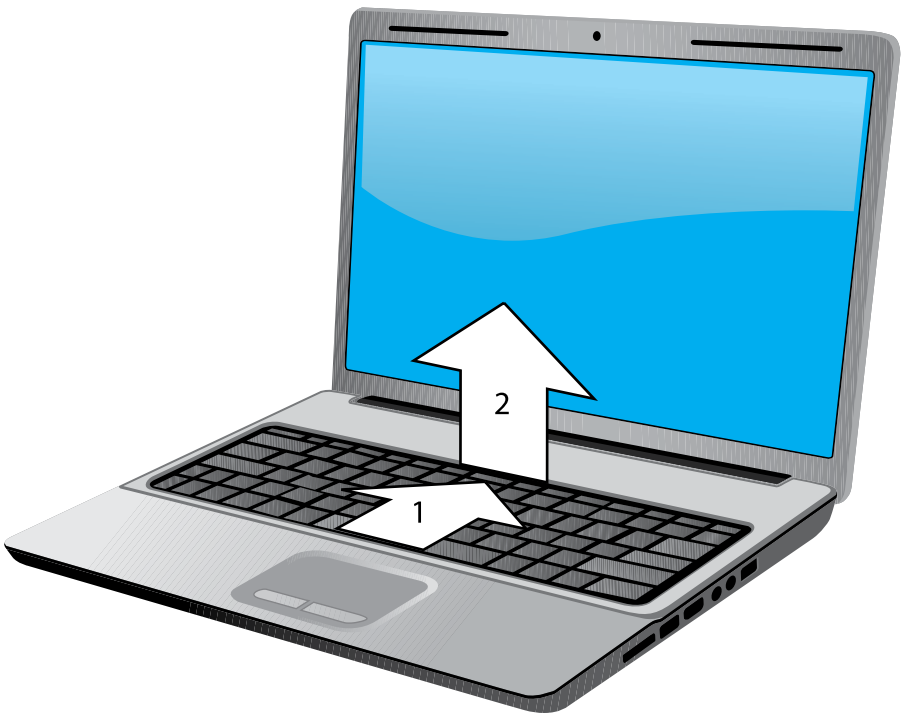


FIGURE 10.49 Laptop keyboard removal process

TECH TIP

These concepts relate to Apple computers, too

Even though this book focuses on PCs, concepts related to CPUs, motherboards, expansion slots, caches, and chipsets also apply to Apple computers. Apple computers and PCs have similar CPU and memory requirements.

Replacing the touchpad on laptops requires a little more work and disassembly than are required for replacing a keyboard. Sometimes an internal drive, memory, the keyboard, the wireless network card, and/or the system board must be removed before you can access the screws, connector, and/or cable that hold the touchpad in place. Sometimes the keyboard must be turned upside down to get to the touch stick. Look at Figure 10.50, and you can see the blue touch stick attached to the keyboard.

FIGURE 10.50 Removed laptop keyboard

Touchpads are also sensitive and may need to be adjusted through the operating system during regular use or after replacement. For a Mac, use the Apple icon in the upper-left corner to select *System Preferences* > *Trackpad*. The touchpad settings in Windows are accessed through either the *Mouse* Control Panel or the *Touchpad* setting, as shown in Figure 10.51. Some vendors have their own touchpad Control Panel.

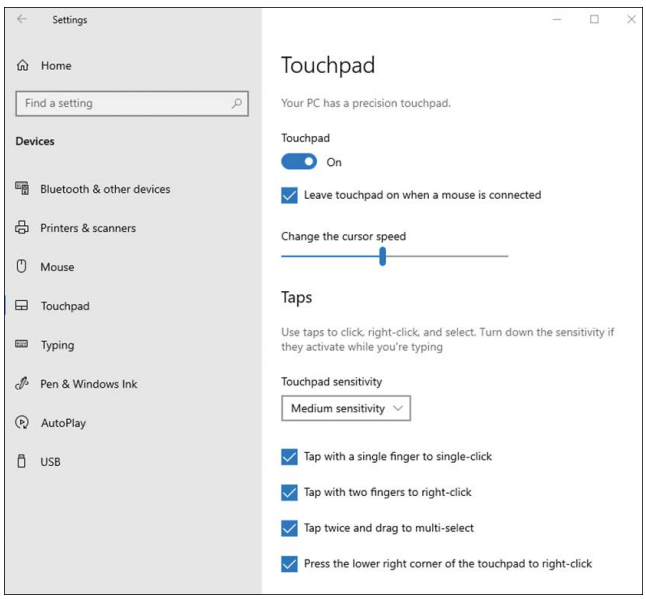


FIGURE 10.51 Touchpad configuration from Windows Settings

TECH TIP

What to do if the laptop keyboard or touchpad goes bad

You can replace mobile keyboards/pointing devices or use external wired or wireless ones.

Laptops have **special function keys**. These keys are in the uppermost part of the keyboard. They are labeled F1, F2, and so on through F10 or F12. They allow you to quickly control screen brightness and hibernation, turn Wi-Fi on and off, mute sound, and perform other functions. For example, on some laptops when you press the Fn key (lower-left side of keyboard) while simultaneously pressing the F5 key, your screen brightness increases. Refer to your particular device's user manual or look at the symbols on the keyboard for a clue about what they can do when combined with the Fn key. Table 10.10 lists one vendor's function keys. Look back at Figure 10.50 to see some of the laptop function keys. See if you can guess what features they perform.

TABLE 10.10 Sample laptop function keys

Fn + ____	Description
F1	Mute the speaker
F2	Decrease the sound volume
F3	Increase the sound volume
F4	Turn off the system
F5	Refresh the browser window
F6	Enable/disable the touchpad
F7	Decrease the display brightness
F8	Increase the display brightness
F9	Switch the display output to an external device
F10	Switch power modes
F11	Enable/disable Bluetooth
F12	Enable/disable Wi-Fi

Other function keys may be available for the following operations:

- Enable/disable cellular
- Enable/disable the touchpad
- Change the screen orientation
- Enable/disable GPS
- Enable/disable Bluetooth
- Enable/disable Airplane Mode
- Enable/disable keyboard backlighting
- Use media options such as fast forward and rewind for video or audio playback
- Use video controls such as dual displays, external display, laptop display and external display, and blanking the display (See Figure 10.52 for a couple examples of video controls that require the use of a function key.)

FIGURE 10.52 Laptop video output special function keys

Laptop Memory

Laptop random-access memory (RAM) modules are different from the memory modules used in desktop or tower computers. Laptops use a special form factor called a small-outline DIMM (**SODIMM**). Other types exist (microDIMMs and small-outline RIMMs [SORIMMs]), but SODIMMs are the most popular, and they come in 144-, 200-, 204-, 260-, and 262-pin versions for 64-bit transfers. An up-and-coming type of memory is the low-power compression attached memory module (**LPCAMM** or LPCAMM2),which requires less power, takes up less space, and is faster than a SODIMM. Some LPCAMMs can be replaced with higher-capacity ones. Figure 10.53 shows the difference between DDR2, DDR3, DDR4, and DDR5 SODIMMs. Each type of SODIMM is notched differently and cannot fit in another type of slot (so, for example, a DDR4 module requires a DDR4 SODIMM memory slot).

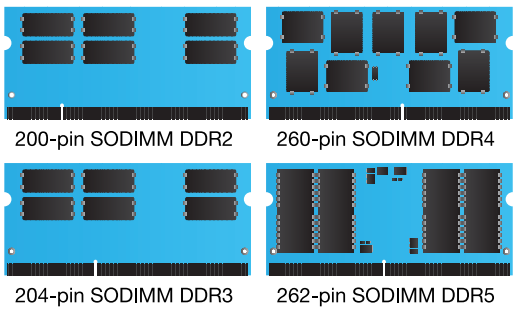


FIGURE 10.53 SODIMM form factors

Some laptops cannot be upgraded because the memory module is soldered onto the motherboard. Many laptops have soldered memory or only one memory slot, so when you upgrade, you must replace the module that is installed. Some smartphones, tablets, and laptops can be upgraded with flash memory cards.

Planning a Laptop Memory Upgrade

When upgrading memory on a laptop, in addition to determining what type of memory chips are going to be used, you must determine what features the memory chip might have. The computer system or motherboard documentation delineates what features are supported. Refer to Table 6.3 in Chapter 6, "Memory," for a refresher on memory technologies and features. Laptop memory advertisements are similar to desktop memory advertisements, as shown in Table 10.11.

TABLE 10.11 Sample SODIMM advertisements

Memory	Advertisement
16 GB kit (2x8 GB)	260-pin SODIMM DDR4 2,400 MHz (PC4-19200) CL16 (16-16-16-39) Non-ECC Unbuffered 1.2V
32 GB (2x16 GB)	260-pin SODIMM (PC4-19200) DDR4 2400 CL16-16-16-39 1.20V
32GB	SODIMM DDR5-5600MT/s 2R x8 Non-ECC memory 1.10V Unbuffered

Pretend that you want to upgrade the memory in a laptop. First, you would open a web browser and search for the specific model and look for the memory specifications (that is, how many slots and what type of memory the laptop allows). Say that the laptop came with 8 GB of RAM, but it has the capacity to hold 16 GB; it has two memory slots, and it currently has two 4 GB SODIMMs installed. In order to upgrade, you will have to purchase two memory modules of 8 GB each and replace the modules that are currently in the laptop.

Laptop Memory Removal/Installation

Many laptops have only one memory slot, so when you upgrade, you must remove the module that is installed. Refer to the manufacturer's documentation when doing this. Before installing or removing laptop memory, turn off the laptop, disconnect the AC power cord (if installed), and remove the battery.

When installing memory into a mobile device, refer to the documentation to see whether a retaining screw on the bottom of the unit must be removed or if the keyboard must be removed in order to access the memory slots. Be sure the laptop memory notch fits into the memory slot key. Laptop memory is normally installed at a 45-degree angle into the slot. Press down on the module until it locks into the side clips. The trick to installing memory is to push firmly into the slot and then into the side clamps. Figure 10.54 shows how to access the memory module in a laptop and the installation process. Note that the laptop battery should be removed before replacing modules.

FIGURE 10.54 Accessing and installing a laptop memory module

Laptop Storage

Laptop hard drives come in two major form factors: 1.8-inch and 2.5-inch form factors. The 2.5-inch form factor is designed for laptops. The 1.8-inch form factor is found in laptops, ultrabooks, and ultraportable devices such as MP3 players, and it is also used for SSDs. Figure 10.55 shows a 2.5-inch hard drive installed in a laptop.

FIGURE 10.55 Installed 2.5-inch laptop hard drive

TECH TIP

What to do if you want more storage space for a laptop

A laptop typically does not allow a second hard drive. However, you can add an additional hard drive to the USB, eSATA, or combo eSATAp port.

Hard drives in laptops tend to be one of three types, as described in Table 10.12.

TABLE 10.12 Laptop hard drive types

Type	Description
Mechanical drive	This is a traditional drive that requires a motor to spin and has read/write heads that float over the hard drive platters. Most modern laptops have moved away from mechanical drives in favor of SSDs.
SSD	An SSD uses flash memory technology to store data. It has no moving parts and produces less heat than a mechanical drive. It is very fast but more expensive than a mechanical drive.
Hybrid drive	This type of drive is sometimes known as a solid-state hybrid drive (SSHD). Part of the drive is an SSD to store the operating system, and the other part is a traditional mechanical drive to hold user data.

Internal Laptop Drives

Laptops traditionally had a PATA or SATA hard drive installed, but today they have an SSD instead of or in addition to these hard drive types. Other mobile devices, such as ultrabooks and tablets, use SSDs as well. A miniPCIe adapter, µSATA (microSATA), **mSATA** (miniSATA) (refer to Figure 7.13) connector, or M.2 connector (refer to Figures 7.9 and 7.10) can be used to connect a drive to the system. Additional storage can be provided by devices that connect to USB, eSATA, or eSATAp ports.

External Drives

An external drive may need to be attached to external power. Some USB devices use external power, some are powered and connect to one USB port, and still others require two USB ports. Some manufacturers may require you to install software before attaching an external drive. Once a drive is attached, use *Device Manager* to ensure that the drive is recognized by the operating system.

Replacing a Laptop Hard Drive

Two installation methods are used with hard drives installed in portable computers: proprietary or removable. With a proprietary installation, the hard drive is installed in a location where it cannot be changed, configured, or moved very easily. Proprietary cables and connectors are used. With removable hard drives, the laptop has a hard drive bay that allows installation/removal through a single connector that provides power as well as data signaling. Otherwise, the drive could have separate data and power connectors.

To remove a laptop hard drive, follow the manufacturer's instructions. Also ensure that you are replacing the drive with a drive of the correct size and interface before starting the process. The following are generic steps for removing/replacing a laptop hard drive:

Step 1. Power down the laptop and remove the battery.

Step 2. Turn the computer upside down and locate the panel used to access the hard drive. Take appropriate antistatic precautions. Note that some laptop models have hard drives that release to the side of the computer.

Step 3. Remove any screws to gain access to the drive. A sliding lock release may also allow access to the drive area. Do not lose these screws as screws may not come with the replacement drive.

Step 4. Slide the drive out of the connector and remove it from the unit. Do not force it. Some units have release levers, are mounted on a frame, and/or are mounted on rubber feet. You may need to gently rock a drive back and forth while pulling gently to ease the drive out of the laptop. Remember that this drive has probably never been removed since it was initially installed.

Reverse the process to install a new drive that has the same form factor. Figure 10.56 shows a SATA hard drive being mounted inside a frame before being installed in a laptop.

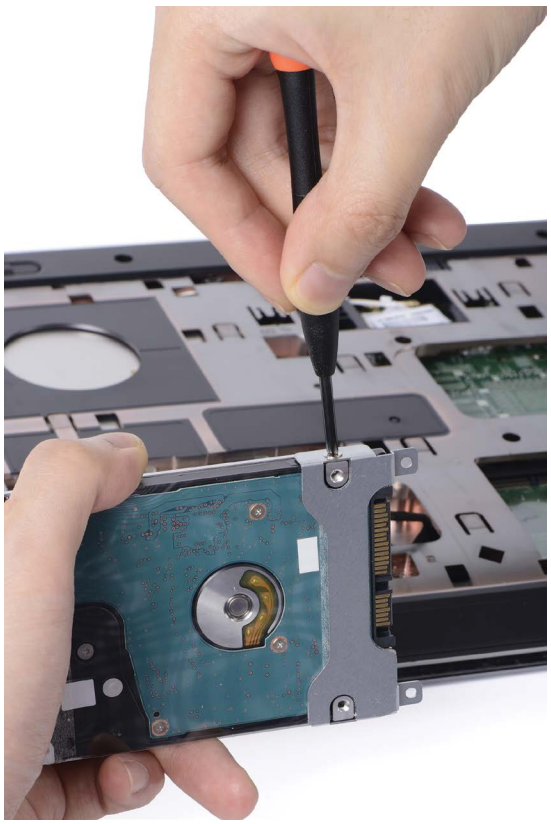


FIGURE 10.56 Installing a laptop hard drive

Migrating/Upgrading a Hard Drive to an SSD

When replacing a laptop hard drive with an SSD, because there is only one drive bay, an external drive enclosure that holds the SSD is needed for the installation process. The enclosure might later be used for the current hard drive to make it an external drive. Also, it is best to use third-party software that clones your computer and allows you to move selected applications over to the SSD without reinstallation of the software.

Figure 10.57 shows an M.2 SSD drive being installed in a laptop. Remember to remove battery and AC power while installing and running from AC power attached during this process. The following are generic steps used to migrate a hard drive with an SSD:

Step 1. Delete any unneeded files and folders. Uninstall any unneeded, unwanted, or unused applications.

Step 2. Defragment the hard drive or run Disk Cleanup.

Step 3. Create a system image.

Step 4. Put the SSD in an external enclosure, if necessary, and connect it to the laptop or install the M.2 SSD into the M.2 slot.

Step 5. Use the *Disk Management* tool to verify that Windows recognizes the drive. If the drive is listed as "Not initialized," right-click on the drive and select *Initialize Disk*. Also ensure that the used space on the current hard drive is less than the space available on the SSD. Depending on the software you use, you may have to shrink your current hard drive partition that has the operating system installed to less than that of the SSD. If you do, reboot the computer after all operations to ensure that the hard drive is still working properly.

Step 6. Use third-party software to clone the current hard drive to the SSD.

Step 7. If you used an external enclosure, power off the laptop. Remove the old hard drive and install the SSD.

Step 8. Power on the laptop and ensure that the SSD boots and all applications work. For more information, refer to Chapter 7.

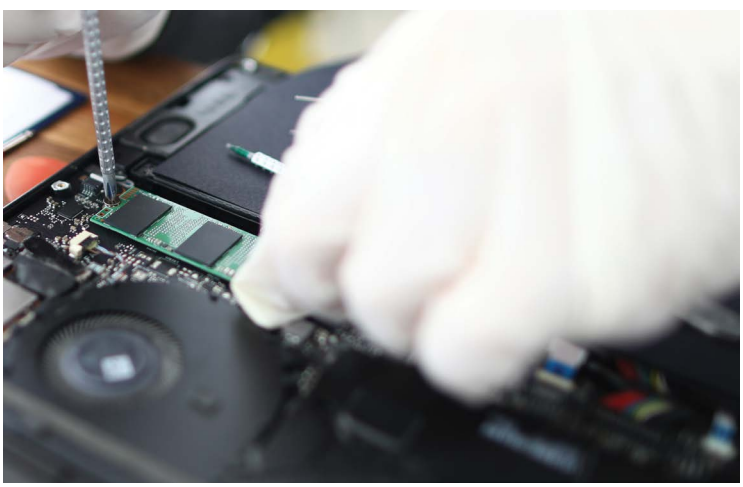


FIGURE 10.57 Installing a laptop SSD

TECH TIP

A noisy hard drive can be a warning

Mechanical hard drives tend to give indicators that failure is imminent. They make noises, the laptop fails to boot, data blocks are marked as bad, data access might be slow, or error messages appear. SSDs, on the other hand, might fail with no advance warning.

Laptop Wireless/Bluetooth Card Replacement

A laptop wireless card is commonly located under the keyboard or accessible from the underside of the laptop. Figure 10.58 shows an 802.11ac Wi-Fi and Bluetooth card. Note that Wi-Fi and Bluetooth cards can also use an M.2 connector.

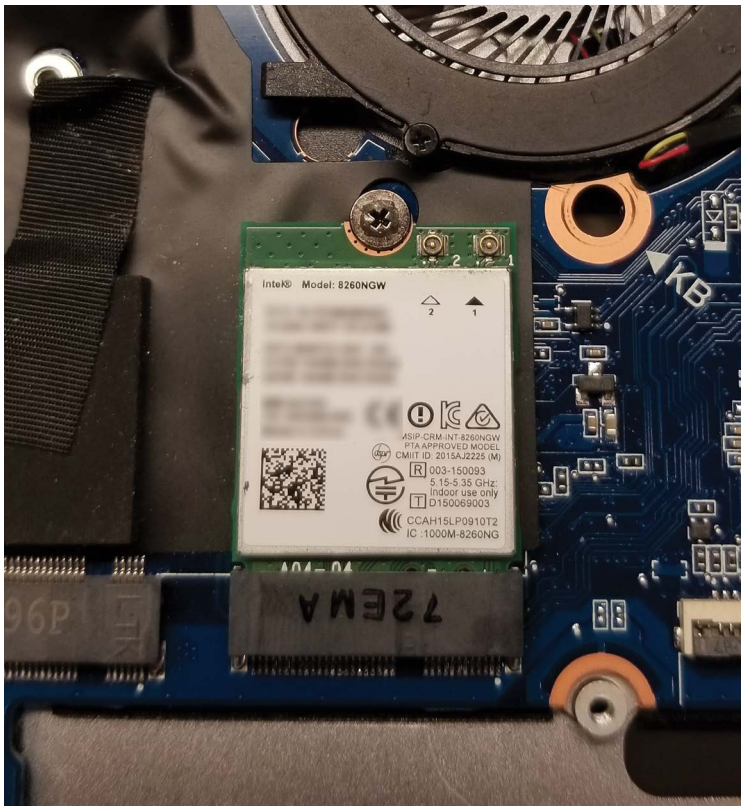


FIGURE 10.58 802.11ac Wi-Fi and Bluetooth laptop card

Refer to the manufacturer's website for the exact procedures. The generic removal steps are as follows:

Step 1. Disconnect the AC power and remove the battery. Take appropriate antistatic precautions.

Step 2. Locate the wireless card (see Figure 10.59).

Step 3. Disconnect any wireless antenna cables from the **Wi-Fi antenna connector**. Notice in Figure 10.59 that the wires attach to two posts on the wireless NIC. These wires connect the antenna to the wireless NIC. A small flat-tipped screwdriver, small needle-nose pliers, or tweezers might be used for this task. Be very careful with this step. Cables are not typically included with a replacement wireless card. If multiple cables are used, take a picture or make a note about which cable attaches to which connector.

Step 4. Ease the wireless card out of the laptop. Note that a lever or tab may be used, depending on the vendor. Make a note or take a photo of how the wireless card inserts into the slot.

Simply reverse these steps to install the replacement card.

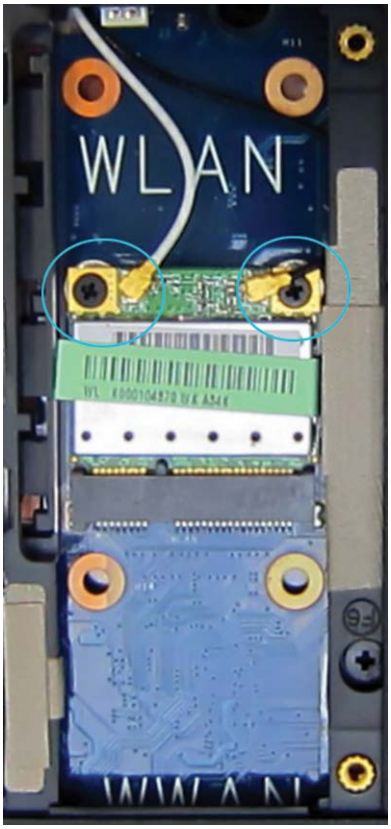


FIGURE 10.59 Laptop wireless NIC and antenna connections

TECH TIP

Where is the wireless antenna on a laptop?

For laptops that have integrated wireless NICs, the wireless antenna is usually built into the laptop display for best connectivity. This is because the display is the tallest point of the laptop and is therefore closest to the wireless receiving antenna. The quality of integrated antennas varies.

Laptop DC Jack Replacement

Because of the numerous times the AC-to-DC power brick is attached to a laptop, it makes sense that laptop power jacks need to be replaced sometimes. The **DC jack** is where you attach power to the laptop. You know the jack is problematic when a new power brick doesn't work, when you can see a broken pin or loose pin in the DC jack, or when you use a multimeter to test the DC voltage level coming out of the power brick, and it is fine, but the laptop will not power using the DC cord.

Figure 10.60 shows how a DC connector might connect. Disconnect the power brick and remove the battery before starting any repair. Note that the cable attached to the DC jack may have retaining clips or might be threaded through a very narrow space. Take care to avoid damaging adjacent parts. Document any parts that you have to remove in order to remove the defective DC jack. Refer to the manufacturer's replacement steps.

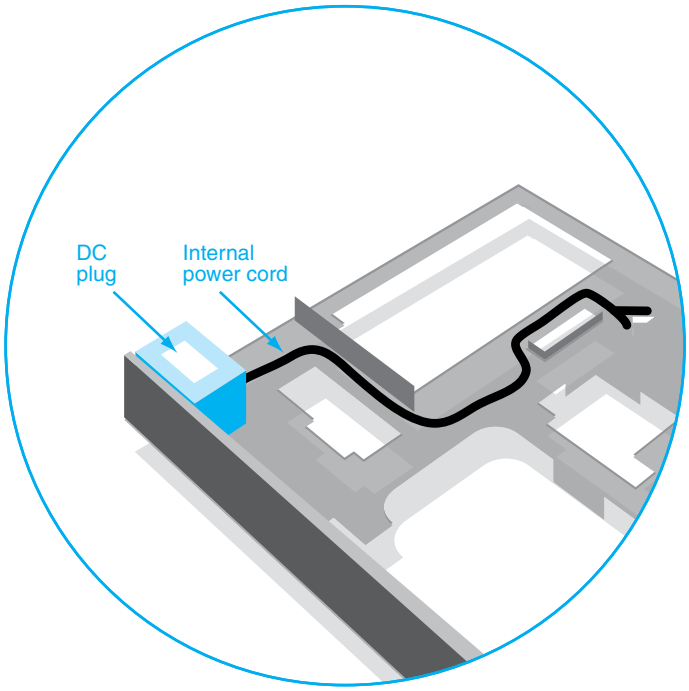


FIGURE 10.60 Laptop DC jack (plug) and power cable

Laptop Display

The laptop display is one of the most complex parts of a laptop. Besides the laptop screen, the display assembly contains other parts, and some of them have nothing to do with the screen. Table 10.13 describes some common components found in a laptop display.

TABLE 10.13 Mobile display components

Component	Description
Wi-Fi antenna	An antenna that attaches to the WLAN card (which is commonly under the computer and/or attached to the system board) and receives/transmits wireless signals.
Webcam	A camera used for video conferencing (or as a camera/video recorder). Some laptops have the ability to use the integrated camera for facial recognition as a security measure. However, because the biometric software cannot distinguish between a living face and a digitized image, it is possible to fool the software by using a photograph.
Microphone	A device used to digitize voice into 1s and 0s so that sound may be heard on a conference call or in a recording. Microphones are tested through the *Sound* Windows Setting *Input* section.
Inverter	A component that converts DC to AC for the CCFL backlight.
Touch screen/ **digitizer**	In a touch screen display, a thin layer of plastic that translates pressure, swipes, or other touch actions into digital signals. Replacement is sometimes difficult but is usually cheaper than replacing the display.

A laptop has a video cable that connects the LCD to the motherboard. Either a CCFL or LED **backlight** bulb is used on many models so images on the screen can be seen. The **CCFL** type connects to an inverter (see Figure 10.61). The inverter converts low DC voltage to high AC voltage for the backlight bulb. Screens larger than 15.4 inches may need two CCFL backlight bulbs. An

LCD with an LED backlight does not need an inverter. An OLED display doesn't need an inverter or a backlight.

The lid close detector (noted in Figure 10.61) can be a physical switch or a magnetic switch located near the back edge of the keyboard portion of a laptop. A laptop can be configured through power management configuration to go into hibernation, sleep, or standby mode when the laptop is closed.

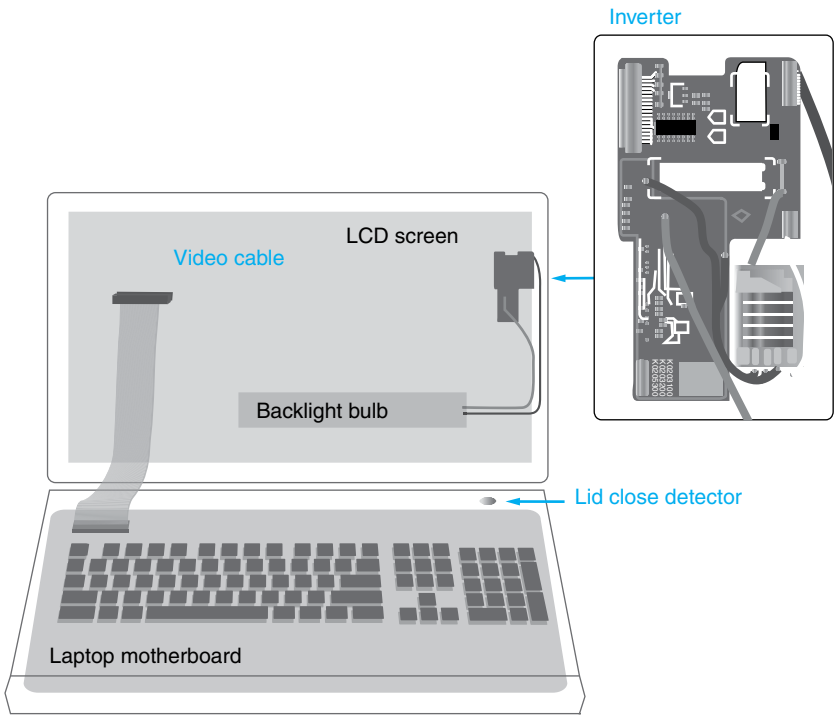


FIGURE 10.61 Laptop video connectivity

TECH TIP

Is it worth fixing a laptop display?

Laptop displays might be too expensive to repair, but if the inverter or backlight is the faulty part, the repair cost is negligible.

A laptop display may need to be replaced as part of a repair or due to a **broken screen**. When removing a laptop display, refer to the directions from the computer manufacturer. The following steps are generic:

Step 1. Use proper antistatic precautions and remove the screws that hold the screen bezel in place.

Step 2. If you have a display that is inside the plastic cover (and does not go right to the edge of the laptop), gently pry the plastic bezel that protects the screen edge from the case. Note that there may be little covers over screws. Remove the covers and then the screws, if necessary. There is a light adhesive, and you might want to use a hair dryer on low heat to warm up the adhesive so it is easier to pry off. The screen might also be held in place by hinge covers. Turn the laptop upside down and use a tool to separate the hinge cover at the seam.

Step 3. Remove the screen's retaining screws.

Step 4. Gently lift the screen from the case. Be very careful with the connectors. Flip the screen so the back of the screen is visible.

Step 5. Notice the ribbon cable that runs up the back of the display. Gently disconnect the cable at the top of the display and the cable that connects to the motherboard. Some cables you must squeeze to release; others have pull tabs or need to be gently pulled from the socket. Figure 10.62 shows the back side of an LCD that uses a CCFL backlight.

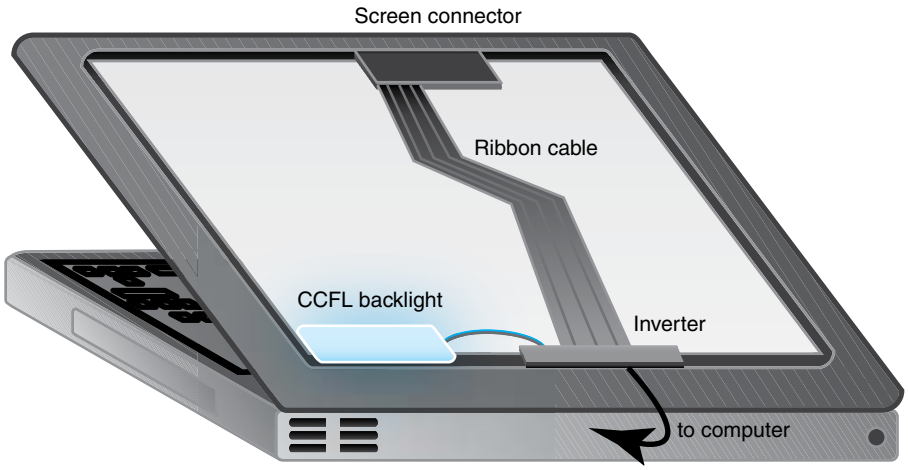


FIGURE 10.62 LCD cabling with a CCFL backlight

TECH TIP

What is the best resolution for a laptop display?

Set a laptop to the native resolution (the resolution for which the LCD was made).

Display Inverter Replacement

If the inverter needs to be replaced, follow the recommended installation directions provided by the manufacturer. Generic instructions for replacement are as follows:

Step 1. Remove the screen bezel, as described earlier in this chapter, to expose the inverter at the bottom of the display.

Step 2. If the inverter has a connector on either side of it, remove the cables from the inverter.

Step 3. Remove the retaining screw, if necessary.

Step 4. Remove the bad inverter.

Reverse the process to install the replacement part.

Microphone and Camera/Webcam Replacement

Microphones in tablets normally do not have controls, as those in laptops and PCs do. Instead, a tablet microphone is controlled through an application that supports a microphone, such as an application that allows you to add audio notes or record a lecture or an online conference application. Inside the application, there is normally a little icon of a microphone that you tap in order to start recording. External microphones can be added using wireless Bluetooth connectivity, USB, or a microphone jack. Smartphones, of course, have integrated microphones.

If a webcam and microphone are built into the display, they are commonly on the same circuit board. Before replacing a webcam or microphone, make sure that the part is actually faulty. Start by checking to see if Device Manager recognizes it. If you just upgraded the operating system, you might need an updated driver rather than a new webcam. Try another application with it, use a different browser with the application, use the webcamtests.com website, or try a video chat session with a friend. You might also consider adding an external device by using USB or Bluetooth instead of repairing the built-in device.

If a webcam or an integrated microphone really is faulty, use the documentation provided by the manufacturer. The generic directions for dealing with a microphone or webcam that is built into the display are as follows:

Step 1. Remove the screen bezel, as described earlier in this chapter, to expose the webcam (see Figure 10.63).

Step 2. If the webcam is held by a screw or a horizontal connector that has light adhesive holding it to the back of the display case, use a flat-tipped screwdriver or plastic scribe to pry the webcam from the case.

Replace the device by reversing this process.

FIGURE 10.63 Webcam removed from the back of an HP laptop

Mobile Device Security

Laptops have special physical security needs, and locking and tracking devices are available for them. Use a nondescript bag to carry a laptop to reduce the chance of theft. Have an engraved permanent asset tag attached. A physical laptop lock or laptop locking station can be purchased and installed on a desk. A user can place a laptop into the locking station without worrying about someone coming by and taking it.

Another option is to use the universal security slot (USS), which allows a cable lock or laptop alarm to be attached. Special software packages enable a laptop to automatically contact a tracking center in case of theft. Figure 10.64 shows a cable lock attached to the USS on a laptop computer.

It is important to install—and run—antivirus/anti-malware software on mobile devices. Depending on the device, the software may be able to automatically scan for viruses or even have a set scheduled scan time.

FIGURE 10.64 Laptop cable lock

Unauthorized apps (bootleg apps) are pirated software that could cause security issues and/or OS issues. A **malicious app** is malware that can install a virus, ransomware, or spyware onto the mobile device and cause many types of issues. Just because an app is in the Play Store or App Store does not mean it is a legitimate app. With **application spoofing**, a mobile app pretends to be another app, has ads that are not from a trusted source, obtains and steals information about/from the device, and/or provides location information without the user having a choice. Do your research before downloading an app. Check reviews, the version history, and the app name and app developer carefully.

Here are some more security suggestions:

> Mobile devices can run each app in a sandbox—a space separated from other apps. Using a sandbox provides a natural security mechanism for applications.

> Mobile device **OS updates** and upgrades are just as important as updates on a full-sized computer. MDM can be used to push out an update in the corporate environment after testing. Connect a device to AC power if possible during an OS update.

> In a corporate environment, mobile app updates should be tested before they are pushed out.

> A device exhibiting **degraded response time** could be a security risk. Check if there are any OS updates available. Consider whether any apps have been added or updated recently. Malware may be present. Restart the device or power it off and back on.

> Many mobile devices have GPS tracking capability that can be used to locate a lost or stolen device. This may be a paid service.

> A paid service or an app on a mobile device can provide the capability to perform a remote lock or a remote wipe. The remote lock disables the device so it cannot be accessed. The remote wipe deletes all data from the device. A **remote wipe** uses software to send a command to a mobile device to do one or any of the following: delete data, do a factory reset, remove everything from the device so it cannot be used, or overwrite data storage to prevent forensic data recovery.

> Beware of **fake security warnings** that could come through the OS, app, or browser. Don't call the number, tap or click on the link, or respond to the text. Interacting with one of these could result in a high number of ads.

> Doing a factory reset can help when some of the app issues and resolutions discussed in this section do not work.

> Verify that the device firmware is the latest version as an update may fix a security issue.

> A mobile device may have a lost mode option that enables you to display messages on the screen for anyone who might find the device.

Most mobile devices have the ability to do some of the following types of locks or **screen locks**: have a **swipe lock**, **PIN code**, passcode lock, **security pattern**, **facial recognition lock** or unlock, **fingerprint lock**, or password enabled that activates when the device is inactive. **Authenticator apps** can also be downloaded.

Biometrics are security settings associated with unique physical characteristics such as fingerprint scanning or facial recognition. Some laptops have fingerprint scanners/readers, but with others you may have to attach an external reader using a USB connection.

To configure biometrics in Windows, you can use *Windows Hello*, which is available through *Settings* > *Accounts* > *Sign-in options* (see Figure 10.65). Note that you might not be able to control or configure these sign-in options on a corporate-owned laptop.

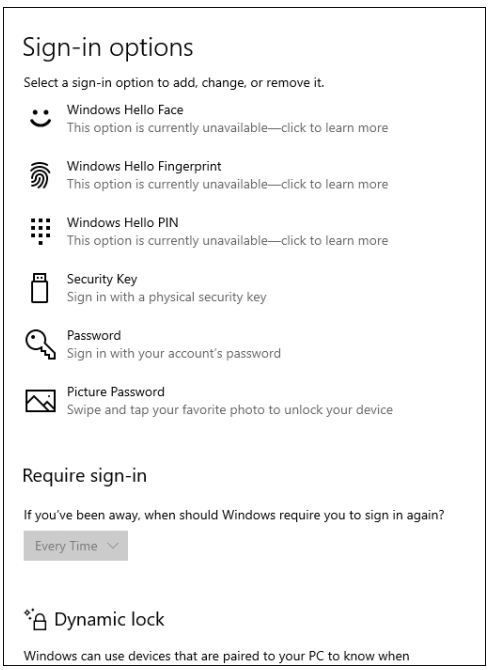


FIGURE 10.65 Windows Hello options

Let's take a look at the different Windows Hello options:

> **Windows Hello Face:** Uses facial recognition and requires an infrared camera that can do 3D depths. If the user changes appearance (such as hair style) often, you might consider recommending one of the other options.
> **Windows Hello Fingerprint:** Configures a fingerprint lock and requires an internal or external fingerprint reader.
> **Windows Hello PIN:** Configures a security PIN.
> **Security Key:** Requires a physical device such as a USB device or an NFC device like a phone or security access card and is used in addition to a fingerprint lock or PIN.
> **Password:** Uses common alphanumeric characters to unlock/log in to the mobile device.
> **Picture Password:** Uses a photo and requires three gestures to be performed on the photo (for example, a click, swipe, circled object, or drawn line).

Cellphones typically allow several options for implementing biometrics implementation; you may have to attach a fingerprint reader/scanner or replace one.

To configure basic mobile security, perform the following:

> **Android:** *Settings* > *Location & Security* > *Set Up Screen Lock*.
> **iOS:** *Settings* > *General* > *Passcode Lock On* option. Use *Settings* > *Passcode* for more passcode options. You can also configure the *Auto-Lock* time. On an iPad, you can use the *iPad Cover Lock/Unlock On* option.

Failed Login Attempts or Unauthorized Account Access

Some mobile devices have configuration settings for when the security method fails, such as an incorrectly entered password or **system lockout**. Some devices allow a default number of attempts. For extra security, some devices can be configured to take an action after a set number of failed attempts, such as disabling the device or even erasing the data. Most mobile device users who have this capability enabled have the data backed up to the cloud or onto a machine.

On an Android device, perform a factory reset from the Android system recovery menu. In iOS, you can use the *Passcode Lock* setting (refer to Figure 10.66) to set how long the system waits for the passcode (*Require Passcode* setting). After 6 failed attempts, the iOS mobile device will be disabled for 1 minute; after 7 failed attempts, it will be disabled for 5 minutes; after 9 failed attempts, it will be disabled for an hour. If you enable the *Erase Data* option, the device will be wiped after 11 failed attempts.

So what happens if someone gets into your account? Change your password immediately. Change the credit card used on the account. Notify the vendor (Apple, Microsoft, Google, and so on). If possible, enable two-step verification to prevent future issues. Some email products allow you to view account activity. Many vendors have an option to send you an email when an unusual device is used to access your account.

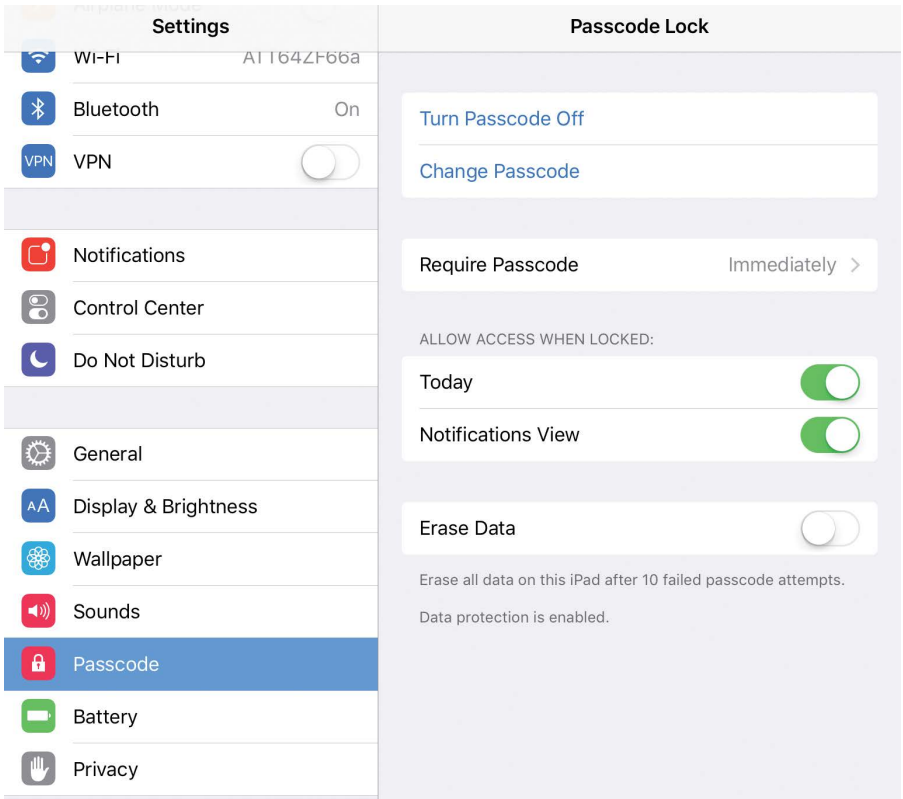


FIGURE 10.66 iOS passcode settings

Unauthorized Location Tracking

Although not all mobile devices have GPS, they can obtain information from other networks and browsers to provide location services. Apps that use location services also use battery life. To turn location services on and off, use the following:

- **Android:** *Settings* > *Location*.
- **iOS:** *Settings* > *Privacy* > *Location Services*. (Note that you can use the *System Services* option to select which services are allowed to track your location.) You can also use *Settings* > *Privacy* > *Advertising* > enable *Limit Ad Tracking* and *Reset Advertising Identifier* in order to be prompted for which apps can track your location. Another option is to change your Safari or other browser settings. To disable tracking in Safari, *Settings* > *Safari* > enable *Do Not Track*.

Android and iOS have apps for dealing with mobile devices that have been lost or stolen:

- **Android:** *Settings* > *Security* > *Device Administration*.
- **iOS:** *Settings* > *Find My iPhone*.

In addition, other free and paid apps are available for dealing with mobile devices that have been lost or stolen.

Leaked Personal Files/Data

There are a number of ways to protect personal information files and/or data on a mobile device. First, protect the device itself by securing the device with a passcode. Encrypt files or use **device encryption**, which uses an algorithm to protect the data and makes it unreadable without the security key. Don't enable GPS except when you need it. Carefully choose and research what apps you download. Monitor your accounts closely. If you think data has already been compromised, change all passwords on all accounts and devices. Watch accounts and notify credit companies, if applicable. You can also do a factory reset on the device.

Data-Usage Limit Notification

Many mobile devices that connect to the cellular network are subject to limits on the text, photo, and video data use allowed in the user's specific rate plan. A **high number of ads** can use up data on the rate plan. Refer to the "Cellular Data" section, earlier in this chapter, for recommendations for blocking ads. Be sure to check mobile device privacy, browser, and application settings for notifications, pop-ups, and advertising settings (*Settings* > *Privacy*). Also check settings or system preferences for location-based ads and services.

To view how much data has been used in a specific period or to turn off cellular data, use these steps:

- **Android:** *Settings* > *Data Usage* (optionally, you can set the mobile data limit).
- **iOS:** *Settings* > *Cellular* > *Cellular Data*.

Unauthorized Root Access

A user who has unauthorized root access has access to the mobile device's file system (see Figure 10.67). Through the file system, malicious programs can be installed, files can be downloaded and copied, and private information can be gleaned. **Jailbreak** (iOS) and **root access** (Android) are two terms that mean that the operating system has been compromised in such a way that the user has an increased level of privilege on the phone. On Android, this is known as having root

access. For iOS devices, users bypass some of the restrictions placed on the device. People do this for several reasons, including to be able to remove apps that are preinstalled, to gain free access to features such as tethering, to enable the device to operate faster, to ensure that the device is not tied to or monitored by the operating system vendor or the phone vendor, and/or to modify the operating environment.

FIGURE 10.67 Gaining root access to a mobile phone

Android is an open source operating system, and vendors are allowed to make modifications and customize it. For both iOS and Android devices, security and operating system releases are not received by phones that have been rooted or jailbroken. Rooting or jailbreaking a device may void the manufacturer's warranty; makes a device more susceptible to viruses, malware, and security issues; and increases the possibility of access to the root directory (the starting place for all files). If an iOS device has been jailbroken, the original iOS can be restored by using iTunes or a factory reset.

Mobile Device Troubleshooting Overview

Troubleshooting mobile devices is similar to troubleshooting desktop devices. Whether Android, iOS, or Windows is being used as an operating system, you use *Settings* or various system preferences in order to make changes to or adjust configuration settings on a device.

If a port does not work properly, check/clean the port of any dirt, corrosion, or obstruction. If the port has corrosion, disconnect power, remove the battery, and use an electronic contact cleaner solution. If it is the charging port, try a different cable. If you have a **physically damaged port**, see if the device is still under warranty. If the device is a laptop or tablet, you may have to replace the motherboard/mainboard. If it is a smartphone, you could buy a replacement circuit board (see Figure 10.68). Don't rule out using a repair shop.

If you drop a device in water and have **liquid damage**, remember that the term *water resistant* does not mean *waterproof*. There are companies that specialize in drying out mobile devices. Putting the device in rice and/or letting it dry for 24 hours are not good solutions as they cannot get all the water from the electronics.

The software and hardware of mobile devices are similar to those of desktop devices. For example, things that go wrong in a mobile device touch screen are similar to those that occur on a laptop touch screen. Overheating, a power issue, a misbehaving app, and/or the OS can all cause a device to do a **random reboot**, and you just have to eliminate each of these issues one by one to see which one it is. Let's dive deeper into some of the issues.

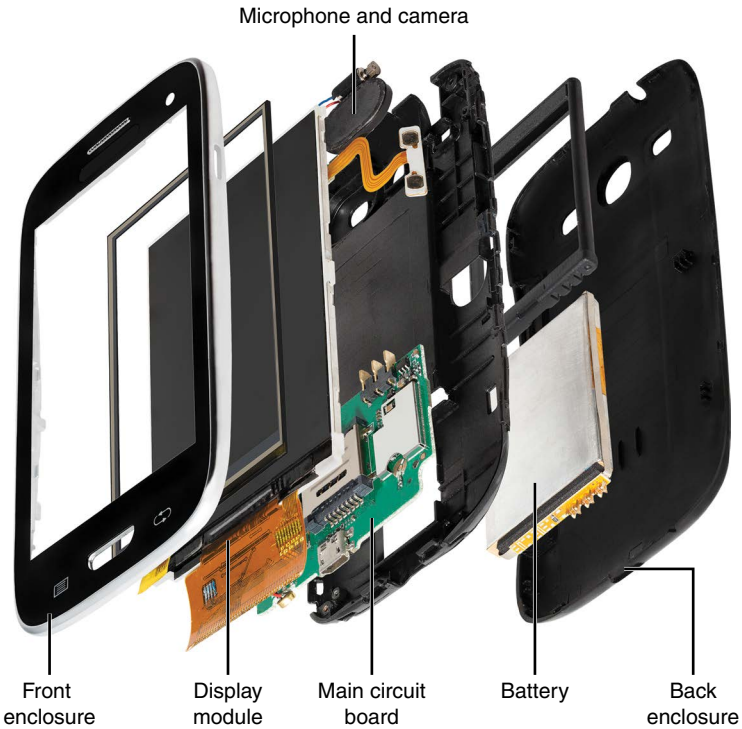


FIGURE 10.68 Disassembled smartphone

Hard and Soft Resets

Sometimes a simple soft reset (restart) is all it takes to fix a mobile device problem. You commonly see a soft reset after an OS update. In some instances, a phone might not restart, and you might need to remove the battery in order to power off the device. Reasons to do a soft reset include the following abnormal behaviors:

- Unresponsive touch screen
- Slow system response
- Inability to receive, make, send, and/or receive text messages or calls
- Audio issues
- Error codes (in which case you should record the codes before restarting; see Figure 10.69)

In contrast to a soft reset, a **hard reset** is a factory reset. (Hard resets for Android devices are covered earlier in this chapter.) You may need to do a hard reset if no other solution helps with the problem, if you have forgotten your password, if the screen is unresponsive and a soft reset does not help, or if you installed a software app that you cannot uninstall or that causes erratic behavior that cannot be solved in any other way:

- **Android:** Boot the device into *Recovery Mode* (typically accessed by holding down two or more specific buttons, such as the power, volume, and/or home buttons) while the device boots > *Wipe Data/Factory Reset* (press *Power* button to select) > *Yes – Erase All User Data.*
- **iOS:** *Settings* > *General* > *Reset* > *Erase All Content and Settings* > *Erase iPhone/iPad.*
- **Windows:** Check the manufacturer. Holding down the power button (or the power button and the increase volume button) for several seconds commonly prompts a hard reset. Sometimes, you might have to disconnect the AC power cord and remove the battery.

FIGURE 10.69 Cell phone error

Some devices can be fixed by removing the power brick (wall adapter) and the battery and leaving the battery out for about 30 seconds. On some Apple devices, you must hold down the power button for 5 seconds afterward. This is known as a System Management Controller (SMC) reset. Apple devices also keep configuration settings such as volume, date, and time in parameter RAM (PRAM). A small separate battery keeps these settings current. To reset these settings on an Apple laptop, hold the following keys down at the same time while the system is booting: ⌘+Option+P+R.

The following sections discuss troubleshooting of mobile devices by area of concern. Remember that the internet has a wealth of technical information available. Research is an important troubleshooting step that can help you see how others have solved similar problems.

OS Fails to Update

Operating system updates (see Figure 10.70) install important security patches and new features. If a mobile device **OS fails to update**, try a hard reset. If that doesn't work, check the following:

- Make sure the device is powered/fully charged and connected to a Wi-Fi network.
- Free up some space by removing apps, photos, and files that are no longer used. Store photos and files in the cloud or back them up and then remove them.
- If a device is an older one, check to see if the model is still supported by the manufacturer.
- Turn off Bluetooth and try the update again.
- Try the download again at a different time.
- On an Android device, clear the data and cache of the Play Store app by using *Settings* > *Applications* > *Google Play Store* > *Clear data* > *Clear cache*.
- On an iOS device, go to *Settings* > *General* > *Storage* and find the update in the list. Select *Update* > *Delete Update*. Then go back into the *General* setting and select *Software Update* and try again.
- Perform a factory reset using the mobile device manufacturer's directions.

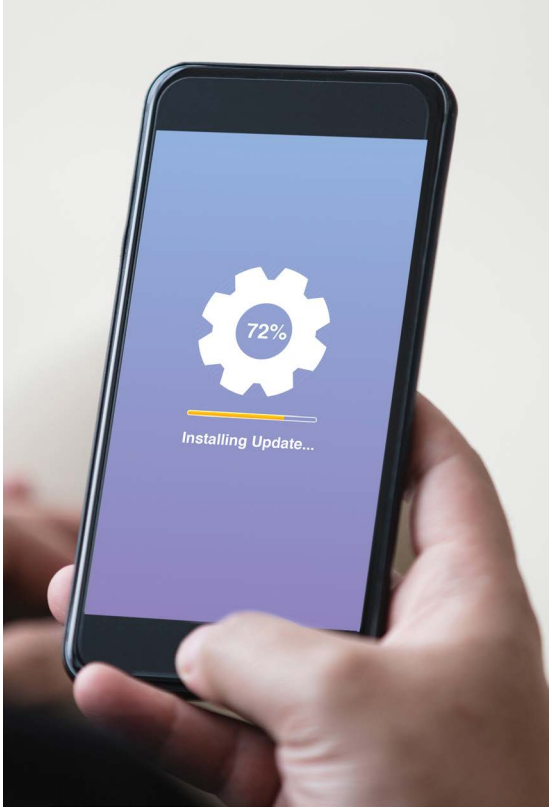


FIGURE 10.70 Cell phone OS update

Mobile Device App Concerns

An app problem can show various symptoms, including causing the device to be slow to respond or preventing other apps from loading. Many apps that are free (and even some that you pay for) do not play well with one another, have **unexpected app behavior**, or have issues with specific operating system versions. In order to troubleshoot apps, sometimes you need to stop an app (that is, perform a forced stop) or stop other apps because the mobile device is slow to respond due to high resource utilization (that is, apps taking all of the memory and processor power). Also, an app may be a malicious app and could pose a security risk.

Here are the generic steps for stopping an application if an **app fails to close** (crashes), but remember that Android is open source, so vendors can implement things differently, and both iOS and Android have different versions, so the exact steps may be different than those shown:

> **Android:** *Settings* > *Apps/Application Manager* > locate and select a particular application > *Force Stop*.
> **iOS:** Press the *Home* button two times quickly or swipe up from the bottom > swipe to find the app to close > swipe up on the app's preview to close it.

You might also be required to uninstall and reinstall an app if the app fails to respond or is not working. There are free app managers that allow you to do this easily, but mobile operating systems allow you to delete apps, too. (However, some apps that come with a mobile device cannot be removed but may be disabled.) Deleting an app deletes the data and settings. These are the generic steps for deleting an app:

> **Android:** *Settings* > *Apps/Application Manager* > locate and select a particular app > *Uninstall/Disable*.

> **iOS:** Press and hold on top of the app icon until all the icons shake (see Figure 10. 71) > tap the *x* in the corner of the icon > *Delete*.

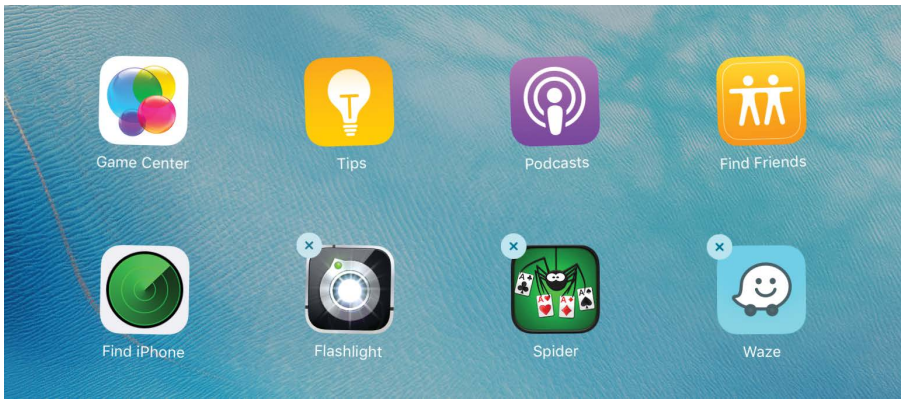


FIGURE 10.71 iOS app deletion

Depending on the type of mobile device, you might be able to use the operating system to check for app log errors. In Windows, use *Event Viewer*. On a Mac, access the *Utilities* folder from within the *Applications* folder. Ensure that the sidebar is shown (and click the leftmost button in the toolbar if the sidebar is not shown). Select *All Messages* from the tab bar. There are also log files located in the *Library* > *Logs* > *DiagnosticReports* folder. You might also try restarting or power the device off and back on again.

App Not Installing or Updating

When an **app fails to install**, ensure that your hardware/operating system is compatible with the app and has storage space available. Some apps do not run well from an SD card and might need to be installed onto the phone's internal storage. Ensure that an antivirus program isn't blocking app installation/upgrade. If an app hangs during the installation or upgrade process, ensure that you have a connection to a Wi-Fi or cellular network, restart the device, and start the process again. Try downloading the app from a different Wi-Fi network. Follow these generic steps when apps are not installing:

> **Android:** *Settings* > *Apps/Application Manager* > *All* > locate and tap on *Market* > *Clear Data* > *Clear Cache*.

> **iOS:** Try resetting the network settings: *Settings* > *General* > *Reset* and try again. You could reset all settings or take the device to an Apple Store.

App Not Loading

When you are faced with a situation where an **app fails to launch**, see if the mobile device believes it to be running already. Windows has *Task Manager* and Android has *Settings* > *Apps/Application Manager*. With iOS, some apps refresh their content automatically. You can see these settings with *Settings* > *General* > *Background App Refresh*. You can also try closing the app and opening it again. Try restarting the mobile device. Try powering down the device and restarting it. Check for operating system updates as well as app updates. If all else fails, delete the app and reinstall it.

Mobile Device Keyboard/Trackpad Issues

Sometimes when symptoms appear, the solution is not simply to replace the part. The key to such issues is to research what others have done when the particular problem has occurred. For example, software updates sometimes fix hardware issues.

Keyboard Issues

Not all devices have keyboards. Mobile devices can have wireless keyboards, optional keyboards, and wired keyboards. Three common keyboard issues are Num Lock indicator light, sticking keys, and ghost cursor/pointer drift.

The Num Lock key, shown in Figure 10.72, is used to allow keys on the numeric pad to be used as something besides numbers (arrow keys, a Home key, Page Up and Page Down keys, Delete key, Insert key, and End key). Pressing the Num Lock key so the Num Lock indicator light illuminates on the keyboard causes numbers to be used. Again pressing the Num Lock key so the indicator turns off causes the keys to be used for arrow keys and the like. Configure the system BIOS/UEFI for the default action (enabled or not enabled) according to the customer's preference.

FIGURE 10.72 Num Lock and numeric keypad

Mobile devices that have keyboards can get dirtier than desktop systems. For sticking keys, follow the same process you would use for a desktop keyboard. Shake out the dirt and spray with compressed air, as shown in Figure 1.22 in Chapter 1, "Introduction to the World of IT." Keys might have to be removed in order to get to the dirt or debris, to clean, or to spray compressed air. Figure 10.73 shows a laptop keyboard with a number of keys removed. A key may have to be pushed toward the top of the keyboard and then lifted up in order to remove it. Peek under the key to see how it attaches before prying off the key.

FIGURE 10.73 Removed laptop keys

Trackpad Issues

The trackpad is commonly problematic for someone who is not used to a laptop. Performing a **touch calibration** or adjusting the sensitivity settings can solve most problems. However, an annoying problem is the illustrious ghost cursor or **cursor drift**, in which the pointer moves across the screen even if no one is touching it. Cursor drift can often be fixed by adjusting the touchpad sensitivity settings or updating the touchpad driver. Malware or a virus can also cause this symptom. In Windows, you can search for troubleshoot touchpad for guidance. Some users disable the touchpad and use a wired mouse.

Mobile Device Display Issues

Displays are critical to mobile devices. They get viewed, touched, and swiped more than any other part. Screens can be stuck and may fail to rotate; a display may go out, dim, stop responding, flicker, or in some other way cause user dissatisfaction. Let's tackle some of the common issues.

Screen Does Not Autorotate

Not all apps support screen rotation and work only in landscape mode. But on a screen that **does not autorotate**, it is time to check the settings. On an Android device, go into *Settings* and ensure that the autorotate setting is on and not locked in portrait or landscape mode. On an iOS device, open *Control Center* and check that portrait orientation is turned off. On Windows, use the *System* Settings link > *Display* > check the Lock rotation and ensure it is in the *Off* position. An app could be causing problems, so close all apps and then open the app you want to rotate after you have ensured that the app supports autorotation. Also see if the OS needs to be updated or whether the G-sensor/accelerometer is faulty.

Dim Display, No Display, or Flickering Display

A **dim display** is commonly caused by a lack of interaction, the display setting, or a low battery. Move the pointer or tap the screen, adjust display settings, and attach AC power to see if the problem is a battery-related issue. On a laptop, the problem could also be caused by an improperly adjusted backlight, sticky lid actuator switch (the switch that detects when the laptop is closed or opened), or faulty inverter.

If a device has **no display**, attach an external display if possible and use the appropriate Fn key combination to send the output to the external display. If you cannot display to an external monitor or if showing a presentation, you might have to use the Windows *Change Display Settings* link to adjust the output to duplicate what is showing on the screen. Check video cabling. Also use the appropriate Fn key combination, even if an external display is not available in case the settings have been changed by mistake.

Check the laptop close switch that is located in the main part of the laptop, near the back, where the display attaches to the laptop. The lid close detector can be a physical switch or a magnetic switch located near the back edge of the keyboard portion of a laptop. A laptop and some mobile devices can be configured to go into hibernation, sleep, or standby mode when the laptop is closed. Check the power management settings. Also check the video cable from the laptop system board to the display.

TECH TIP

What to do if a laptop display goes black, red, dim, or pink

If a laptop display goes black, red, dim, or pink, most likely this is because the backlight bulb is faulty. Otherwise, the problem is the DC-to-AC inverter. Connect an external monitor to the laptop external video port. If the external monitor works, most likely the backlight bulb is the culprit.

For a mobile device, try turning it off and back on. On a laptop or tablet, see if the device appears to boot normally. If the device has recently been exposed to liquid, power off the device, remove the battery, and allow the device to dry thoroughly before trying to power it back on again. A bad LCD backlight or inverter can cause a dim or blank display, too.

A flickering display can sometimes be fixed by simply adjusting the resolution (to the native resolution) or refresh rate or tightening the display cable. If you have recently changed the display, check the driver. Move the display to see if the flicker is related to display movement. An inverter and backlight can also cause this problem or show horizontal/vertical lines. Refer to Figure 10.62 to see how the display attaches to the motherboard.

TECH TIP

What to do if the top of a web browser or File Explorer is missing

If the top part of a web browser window where you can enter a URL is missing, try pressing F11, which takes the window out of full-screen mode. If that doesn't work or if the top part of File Explorer is missing, try using Ctrl+Shift+⊞+B to restart the video.

Touch Screen/Stylus Does Not Respond or Is Inaccurate

The touch screen is a critical part of a mobile device. Users get frustrated by **touch screen non-responsive** issues. The following list suggests things to try if a touch screen is non-responsive or doesn't respond the way you expect it to:

- Close some apps to free up memory.
- Determine whether the problem is app specific, if possible.
- Restart the device. Force a shutdown even if doing so requires disconnecting the AC power cord and/or removing the battery.
- If the display has had any liquid on it, turn off the device and remove the battery. Allow the device to dry thoroughly before powering it on.
- If a screen protector is in place, remove it.
- Shut down the device and remove any memory cards, the SIM card, and the battery for about 60 seconds. Reinstall these items and power up.
- Use a calibration utility, if available, to calibrate for touch input. On an Android device, try *Settings* > *Display*. In Windows, search for and use *Calibrate the Screen for Pen and Touch Input* > *Calibrate*. For iOS devices, try resetting the phone.
- Perform a factory restart.

If a stylus is being used and the **stylus does not work**, try using your finger instead. The stylus could have a dirty, worn, or damaged tip. If the stylus uses a battery, check to see if it needs to be replaced.

The digitizer translates what your stylus or finger does. If a touch screen is unresponsive, the digitizer may need to be replaced. See the section "Digitizer or Touch Screen Replacement" in Chapter 8, "Video and Multimedia Devices," for details.

If the touch screen is broken, you should be able to still see what is on the device. When the LCD is damaged and cracks appear or when the screen has dark spots, the touch screen might still work in places. Screens can be ordered and replaced. Some repair shops specialize in mobile device displays.

Degraded Performance

Degraded performance, or slow performance, means a system is not responding as fast as it normally does. The problem can be a lot of things, but some people first notice the responsiveness of a touch screen or delays when waiting for data to download. If you suspect that the touch screen is the problem, troubleshoot that. But if you have ruled out the touch screen, consider the following tips:

> Check the battery power level.
> Close apps that aren't being used.
> Close services (Wi-Fi, GPS, location services, Bluetooth, and so on) that are not being used. Put the device in Airplane Mode.
> Attach to a Wi-Fi network.
> Move closer to the wireless access point if connected to Wi-Fi.
> On newer Android devices, use the option to reduce the amount of data needed by the Chrome browser: *Settings > (Advanced) Data Saver.*

Mobile Device Power Issues

A mobile device quickly becomes useless when it has power issues. Power is required for a device to be mobile. Power issues can include extremely short battery life, no power, swollen battery, and the **battery not charging**.

Battery Issues

A battery is critical for operations in a mobile device. A battery that has **poor battery health** (that is, it won't hold a charge for long or drains quickly) commonly needs to be replaced. However, the problem could be that many apps, wireless, location services, GPS, and Bluetooth settings are turned on. Check the display settings. Set the brightness/contrast setting to a lower setting instead of Auto. Inspect the battery to see if it is swollen. A **swollen battery** is a battery that bulges and might even leak (see Figure 10.74). Most batteries that won't hold a charge need to be replaced; a battery that is swollen should be replaced immediately. Also verify that the phone shows the battery actually being charged. Don't just assume that it is charged, based on the amount of time it has been plugged in. The physical connection to the charger could be a tenuous one. The charger could be faulty, too.

FIGURE 10.74 Swollen battery in a cell phone

Battery Not Charging

Improper charging could be due to the battery, the charger, or the connection on the phone. Inspect the connection on the phone first. Do you see any debris or dirt, or do you see pins that look like they do not align with the other pins? If so, power off the device, remove the battery, and clean it with compressed air; gently try to align pins that are misaligned. Do the same inspection on the charge connector. Take a voltage reading on the charger, if possible. See if it is outputting power. See if the same cable and/or charger can charge other devices that require the same voltage and connector type. Try to charge with a different connector, such as a car adapter.

No Power or Frozen System

An electronic device that has no power or is a frozen system is useless. Try the following when troubleshooting a mobile device that will not power up:

- Check for the power light.
- Ensure that the device has not gone into sleep mode. Try waking up the device or powering it down and then powering it up again.
- Check for a misbehaving app. Close all apps and only have one open at a time to see which one might be causing the symptoms.
- Attach the device to an AC adapter and power it up.
- Disconnect the AC power brick, remove the battery, and hold down the power button for a few seconds. Replace the battery and reconnect to AC power. Try to power on the laptop again.
- Inspect the power button and think about whether it has felt strange lately.
- When you attach the power brick to the mobile device, does the connector attach easily, or does it wiggle? If the device is a laptop, consider replacing the DC power jack.
- Check the display brightness.
- If the device is a laptop, check the lid close sensor.
- If the device is a laptop or a tablet with a keyboard, try closing the display and opening it back up fully.
- Check for malware or viruses.

Overheating: Warm/Hot to the Touch

Heat is one of the worst enemies of electronic devices. Symptoms of **overheating** include the device being warm or hot (see Figure 10.75) to the touch, losing battery strength faster than normal, and shutting down unexpectedly. Leaving mobile devices in hot vehicles and in the sun is bad. If a device is overheating, power down the device and let it cool. Do not just move it to a cooler spot.

See if you can determine a specific spot on the device that is getting hotter than other places. Determine whether that spot is where the battery or power is located or whether it is another spot on the mobile device. If it is near the battery, troubleshoot power problems after the device has cooled completely.

Check the battery health icon on the device. Inspect the battery. Replace the battery if you think it is the cause. Close unneeded apps and services. Remove the device from its case, if applicable. Ensure that you are not covering the device's air vents, such as by placing it on a lap or pillow. Place a laptop on something that elevates it from the desk, such as drink coasters. In addition, pads, trays, and mats can be purchased with fans that are AC powered or USB powered. Research the device vendor to determine if others are having similar issues.

FIGURE 10.75 Overheated laptop

Mobile Device Network Issues

Chapter 13 goes into more details on networking, but this section presents some basic troubleshooting techniques you can perform on mobile devices without providing more involved details about how these technologies work. The issues can be broken down into four areas: Wi-Fi, GPS, Bluetooth, and NFC issues.

Wi-Fi Issues

Use the following list when troubleshooting Wi-Fi issues such as **intermittent wireless** or **no wireless connectivity** on a mobile device:

- Ensure that the mobile device is not in Airplane Mode.
- Ensure that Wi-Fi is enabled.
- Ensure that the correct Wi-Fi network is chosen. If prompted, provide the appropriate security/login credentials.
- Turn off Wi-Fi and then re-enable it.
- If a laptop always has low signal strength, ensure that the wires are attached to the wireless NIC. If the display has been replaced recently, ensure that all connectors have been reattached properly and have not been damaged.
- For any device that has low signal strength, one issue might be **high network traffic**. Move around and try to see if you get more signal bars by moving. The more bars you see, the better the signal strength and speed of transmission (see Figure 10.76).
- With some laptops, you must turn the laptop to a different angle to attach to an access point or find a stronger signal strength (which means faster transfers). Antenna placement is important in a wireless network. Antennas on mobile devices tend to be in the edges or built into the displays.
- If the internet connection shows **limited connectivity** or you have **no internet connectivity**, try rebooting the device or the router that connects to the internet if in a home or small business network. With a wireless connection, check security settings and ensure that wireless (Wi-Fi) connectivity is enabled. If on a wired network, the cable could be an issue.

- If a mobile device connects to a Wi-Fi network unintentionally, turn off Wi-Fi. Some mobile devices have the ability to automatically switch between Wi-Fi and mobile networks in order to keep a solid internet connection. To disable this in iOS, use *Settings* > *Wi-Fi* > disable *Auto-Join*. On Android devices that have Wi-Fi enabled, use *Settings* > *Wi-Fi* > select and hold on the wireless network that is not wanted > *Forget Network*.
- Whenever a question mark appears at the top of a mobile device, it means there are Wi-Fi networks in the area, and you need to select the one that you want to attach to. A lock next to a wireless network name means you need a password to access the wireless network.
- Slow or intermittent transmissions can be related to distance to the access point, external interference, other Wi-Fi networks and devices, and the number of devices attached to the same wireless access point.

FIGURE 10.76 Wireless signal strength

GPS Issues

GPS is not provided in all mobile devices. The geographic environment affects GPS reception and can cause intermittent connectivity. If GPS is installed but is not functioning properly, try turning off *Location Services* and then turning it back on. If that fails, restart the device. Some Android devices have assisted GPS, which uses GPS satellites, cell towers, and Wi-Fi networks to provide location services. The device might be in an area where connectivity is limited or missing. Ensure that *Use Wireless Networks* and *Use GPS Satellites* are enabled on an older phone. Some phones have a *High Accuracy* setting instead. Another problem is that the user might have denied a particular app the right to have access to location services, and the app might not be very useful without location services. Access the app settings to verify that location services are enabled. You can try uninstalling and reinstalling the app. Turn off any apps that are using GPS but are not needed.

Bluetooth Issues

If you have **no Bluetooth connectivity**, the suggestions are the same as for all other network connectivity issues: Turn the device off and back on again, move the device closer to the other Bluetooth device(s), and put the device in Airplane Mode and then turn off Airplane Mode to toggle off all radios and then re-enable them. Other troubleshooting hints are as follows:

- Check for interference from other devices, including wireless devices on the same frequency. Also look for Windows, Apple iOS, or Android configuration issues.
- If a Bluetooth device is not working in Windows, try the following: Select the Bluetooth icon ( ) in the notification area on the taskbar and select *Show Bluetooth Devices*. If the device is not listed there, select *Add a Device* and try to add it.
- Ensure that the Bluetooth device is charged, powered on, and in the appropriate mode to pair with another Bluetooth device, such as a computing device or car with Bluetooth capability.
- Ensure that other wireless devices, such as wireless networks, automatic lighting and remote controls, cell phones and other portable phones, and microwave ovens, are not interfering with the device.
- Remove unused USB devices.
- If passkeys (PINs) are used, ensure that the keys match on both devices.
- If a Bluetooth transceiver is used, move the transceiver to another USB port.
- Remove all other Bluetooth devices to aid in troubleshooting the problematic device.

- In Windows, ensure that Bluetooth services are enabled. See Chapter 16, "Advanced Windows," for more information on Windows services.
- In Windows, ensure that Device Manager shows no issues with the Bluetooth transceiver driver (under the *Bluetooth Radios* section) or the Bluetooth device (sometimes shown under the *Other Devices* category). The Bluetooth driver for the host computer may need to be updated for a newer device.
- Use similar steps with Apple iOS and Android devices: Ensure that the device is powered, ensure that Bluetooth is enabled, and ensure that no other wireless networks/devices are nearby (by moving to another location to see if they appear).
- A common method used with Bluetooth devices is to restart the pairing mode on the Bluetooth device or rescan for a device from the iOS/Android computing device.
- If a mobile device unintentionally pairs with another Bluetooth device, turn off Bluetooth—and keep it off except when you are using it. Move the mobile device closer to the Bluetooth device.
- USB-to-RJ45, USB-to-Bluetooth, and USB-to-Wi-Fi adapters/dongles can be used when a network port fails.

NFC Connectivity Issues

The most common cause of NFC not working is that it is turned off/disabled. If you recently did a restart of the mobile device, it may have disabled NFC. Check the battery level. Some devices do not allow NFC to be used if the battery does not have a specific (high) battery charge level. Sometimes a specific style of case may interfere with NFC operations. Check to ensure the device is not in Airplane Mode. Try restarting the device or powering off and back on.

SOFT SKILLS: A WORD ABOUT APPEARANCE

Whether you like it or not, you are sometimes judged on your personal appearance. Why does appearance matter so much? Research shows that we form opinions about each other within mere seconds of meeting. And some people decide whether you are trustworthy in less than a second! Look at Figure 10.77 and imagine that each of these people is a technician coming in to fix your computer. What would be your impression of each person, based only on their attire?

FIGURE 10.77 Professional attire options

To make good impressions on your boss and your customers, strive to project a competent and professional appearance and demeanor. A good rule of thumb is to dress to the level of the client. For example, you would probably dress more professionally for a job in a law office or doctor's office than you would for a job at Joe the plumber's business. If you knew you were going to be working on laser printers, you probably wouldn't want to wear your best clothes, or you might wear a lab coat to protect your clothes.

Be aware of generational bias. In the United States today, four generations have different values. The Traditionalists, or silent generation, born 1925–1945, value suits, coats, and ties for men and dresses for women. Most of these people are now age 75+, so there are few of them left in workplaces. The Baby Boomers, 1946–1964, are a little more relaxed about dress codes but still believe in good appearance (think business casual). Now aged in their 60s to 70s, they are likely to be bosses and senior managers. Next come the GenXers, generally born 1965–1980, who value flexibility and freedom and are even more relaxed—even casual. Finally, GenYers, or Millennials—born between 1981 and 1996—value change, diversity, and individual freedom. These are the workers most likely to express themselves with tattoos, piercings, extreme grooming, and so on. To Millennials, dress codes are much less important than they are to members of the other generations.

The following are some common-sense guidelines:

- Avoid wearing tattered jeans, sneakers, and t-shirts, as you could run the risk of looking too scruffy to be taken seriously.
- If your job involves dirty work, such as pulling fiber-optic cables through the overhead space or working on laser printers, jeans and button-down shirts are acceptable. Or consider wearing a lab coat. It doesn't hurt to let the client know upon checking in that you are dressed for a dirty job.
- Watch your haircut and facial hair. Don't forget to groom your hands and nails, which will be noticed (either consciously or unconsciously) by your boss and customers.
- Women are more likely to be better liked and trusted if they use moderate makeup and little to no perfume.

Table 10.14 lists recommendations for attire according to the environment.

TABLE 10.14 Attire in specific environments

Environment	Recommended attire
Business dress or formal	Men: Coat and tie. Women: Dress, skirt, pant suit.
Business casual	Men: Dress shirt (tie optional). Women: Dress, skirt/blouse, pants/shirt
Casual	Men: Collared shirt, polo shirt, nice pants, slacks. Women: Pants, polo shirt

TECH TIP

The colors you wear send subliminal messages

Colors can profoundly affect how other people view you. Here are some of the main ones to bear in mind:

- **Black or dark gray:** Represents authority and confidence
- **Blue:** Suggests trust and traditional values
- **Green:** Portrays empathy and tranquility
- **Red:** Conveys that you are passionate and likely to be an extrovert
- **Brown:** Says that you are loyal and reliable

It is usually the subconscious mind that notices how others look. So even if you don't consider appearances to be very important, keep in mind that, without your realizing it, appearances have helped you form an opinion of just about everyone you have ever met. Don't underestimate the importance of dressing appropriately on the job but don't let your wardrobe impede your ability to do the job.

Chapter Summary

- Mobile devices are used for different purposes and therefore come in a variety of types, including laptops, tablets, drawing pads, smartphones, wearable technology, e-readers, and cameras.
- Mobile devices have the following common hardware parts: display, flash memory, battery, DC jack, speaker, microphone, speaker, wireless antenna, system board, processor, and expansion options. Other parts that may be more for laptops or tablets include SODIMMs; storage that could be mechanical, SSD, and/or hybrid; ports and adapters; keyboards; miniPCIe cards; touchpads; and touch screens.
- Mobile devices have various methods of expansion and connectivity, including the following: NFC, proprietary, serial, hot spot, USB, miniUSB, microUSB, Lightning, infrared, tethering, Bluetooth, GPS, cellular, satellite, Wi-Fi, miniPCI/PCIe, docking stations, and port replicators.
- Mobile devices commonly have accessories that need to be installed and/or attached, including headsets, touchpads, webcam, speakers, game pads, battery packs/chargers, and memory.
- Mobile device operating systems include the open source Android, closed source Apple iOS and iPadOS, Chrome OS, and various Microsoft Windows-based mobile operating systems.
- Laptops use Fn keys to control specific functions, such as Wi-Fi, Bluetooth, speakers, display output, and keyboard backlighting.
- Mobile devices need to have their operating system and data backed up. Two common methods to do this are to back them up to another device or use storage in the cloud.
- Mobile devices need security. All mobile devices need operating system security, personal file and identity security, anti-malware, and antivirus. Remote data wiping can be configured to protect the data on devices that are compromised or stolen.

- A plastic scribe helps with prying off plastic parts and covers. Laptops frequently have cables that run along the back or sides of the device. Keep screws separated and take notes and photos for any parts that are removed.
- Conserve mobile device power by adding more RAM, turning off wireless/Bluetooth, turning off unnecessary apps, configuring power options, reducing screen brightness, and avoiding temperature extremes.
- Li-ion batteries are used with mobile devices. If a device must be attached to AC power or a USB port in order to work, replace the battery with the correct DC power jack, appropriate DC voltage level, and current (amperage) equal to or higher than the original power brick.
- Before removing or installing memory, disconnect the power cord and remove the battery on a mobile device.
- Laptops can sometimes be upgraded with SODIMMs. Tablets and smartphones can sometimes be upgraded and gain additional storage through flash memory cards.
- AC power goes into the power supply or mobile device power brick. DC power is provided to all internal parts of a computing device.
- Secure a mobile device with a PIN, facial recognition, a password, or a passcode/pattern.
- When replacing a laptop motherboard, additional components may have to be removed.
- Troubleshooting mobile devices commonly includes a soft reset or a restart or a hard reset, which is another name for a factory reset. Android and iOS devices use *Settings* to manage most configurations. Windows uses either various Control Panels or *Settings*.
- Troubleshooting commonly involves disabling apps, connectivity, and features.
- Troubleshooting sometimes involves removing AC power and the battery from a mobile device.
- Mobile device repairs commonly require different tools, including scribes, antistatic gloves, and smaller tools.

A+ CERTIFICATION EXAM TIPS

- ✓ Be able to explain the difference between Android, Chrome OS, iOS, and iPadOS on mobile devices.
- ✓ Be able to identify, describe the purpose of, and replace/install and configure hardware components including batteries, keyboards or keys, RAM, hard drives, SSD, styli, headsets, speakers, webcams, trackpads, drawing pads, and wireless cards, as well as security components such as biometric and NFC devices.
- ✓ Know that each app has configurable settings that might need to be adjusted. Be able to configure business apps that deal with email and cloud storage. Be able to synchronize data specifically for the calendar and contacts.
- ✓ Know the difference between a docking station and a port replicator.
- ✓ Watch a few videos on laptop disassembly and digitizer replacement.
- ✓ Be able to describe the difference between the inverter and digitizer. Go back to Chapter 8 to review the different types of displays and attributes, including LCD, OLED, TN, IPS, and VA. Know how to replace the Wi-Fi antenna, webcam, and microphone.
- ✓ Study how to configure and connect via USB, Lightning, NFC, hotspot/tethering, Bluetooth, GPS, cellular (3G, 4G, 5G), and Wi-Fi. Know what information is needed for corporate email configuration, two-factor authentication, and corporate apps. Be able to sync Microsoft 365, ActiveSync, calendar, contacts, and any other commercial mail app. Know that Airplane Mode disables Bluetooth, cellular, and Wi-Fi communications and also preserves battery life. Right before taking the exams, use an Android simulator or practice on Android, iOS, and Windows device configurations. Know that bandwidth throttling might be implemented on wireless networks and may affect those who are streaming video, creating a hotspot, or using tethering.
- ✓ A cell phone requires an NFC chip in order to use the mobile pay feature. Be able to recognize and repair NFC issues.

- ✓ Realize that quick battery drain could signal more than just a battery that needs to be replaced. Check for running apps, brightness levels, and open communications (Bluetooth, cellular, Wi-Fi, GPS, and so on).
- ✓ Review the types of things you might control with function keys. Know that you might use these keys to solve problems such as erratic mouse (or touchpad) actions and display output.
- ✓ Review corporate and BYOD device configurations, MDM, policy enforcement, and how corporate apps are handled.
- ✓ Know the difference between a SIM and eSIM and how to install one.
- ✓ If you can't easily reattach a cell phone back, check for a swollen battery.
- ✓ Know that Android devices synchronize to the cloud by default. Know that iTunes can be used to back up/restore an iOS device. Know that OneDrive is used to access saved attachments from Microsoft Outlook. Configuring a mobile device to use an email account enables synchronization of associated data, such as calendars and contacts.
- ✓ Know the purpose of mobile device security measures, including screen locks (facial recognition, PIN, fingerprint, pattern, swipe), remote wipe, locator app, OS update, encryption, remote backup, and antivirus/anti-malware.
- ✓ Be able to configure security settings on Android, iOS, and Windows devices.
- ✓ If you cannot connect to a wireless network, see if there are multiple networks in the area and select one. Note that a wireless network might need to be "forgotten" so that you can reattach with an updated password or just reassociate if internet connectivity is unavailable.
- ✓ Review how to troubleshoot security situations including APK, developer mode, root access/jailbreaking, unauthorized or malicious apps, and app spoofing. Also know that symptoms of security issues include an increase in network traffic, slow response times, data usage alerts, limited internet connectivity, a lot of ads, fake security warnings, unusual app behavior, and leaked files or data.
- ✓ Be able to troubleshoot connectivity, liquid damage, overheating, digitizer and screen issues, ports, malware, cursor drift, and touch calibration.
- ✓ Read and reread all the troubleshooting scenarios in the chapter. Troubleshooting mobile devices is a part of both the CompTIA A+ 220-1201 and 220-1202 exams.

Key Terms

2.4 GHz, 3G/4G/5G, 5 GHz, 6 GHz, 802.11a, 802.11b, 802.11g, 802.11n, 802.11ac (Wi-Fi 5), 802.11ax (Wi-Fi 6), 802.11be (Wi-Fi 7), Airplane Mode, Android, app fails to close, app fails to install, app fails to launch, application spoofing, application update, authenticator app, backlight, battery not charging, biometric, Bluetooth, broken screen, BYOD, calendar, CCFL, cellular card, cellular location service, Chrome OS, cloud storage, configuration profile, contacts, cursor drift, data cap, DC jack, degraded performance, degraded response time, developer mode, device encryption, digitizer, dim display, docking station, does not autorotate, drawing pad, eSIM, facial recognition lock, factory reset, fake security warning, fingerprint lock, flash memory, GPS, hard reset, headset, high network traffic, high number of ads, hotspot, IMAP, improper charging, intermittent wireless, inverter, iOS, iPadOS, IR, jailbreak, laptop docking station, laptop RAM, Lightning port, limited connectivity, liquid damage, locator application, LPCAMM, LTE, M.2, malicious app, malware, memory card reader, MDM, microphone, microUSB, miniPCIe, miniUSB, mobile docking station, mobile motherboard, mSATA, NFC, no Bluetooth connectivity, no display, no internet connectivity, no wireless connectivity, NVMe, OneDrive, OS fails to update, OS update (mobile), overheating, physically damaged port, PIN code, policy enforcement, poor battery health, POP3, port replicator, random reboot, remote backup, remote wipe, root access, screen lock, scribe, SD, security pattern, SIM, SODIMM, speaker, special function key, SSD, stylus, stylus does not work, swipe lock, swollen battery, system lockout, tethering, touch calibration, touch screen non-responsive, track pad, track point, unauthorized app, unexpected app behavior, USB-C, webcam, Wi-Fi analyzer, Wi-Fi antenna, Wi-Fi antenna connector, Wi-Fi calling, wireless card

Review Questions

1. How can you control sending display output to an external monitor on a laptop?

   _____

2. Which type of mobile device would most likely have a digitizer?

   [work laptop | device that has a touch screen | gaming laptop | credit card reader]

3. In which of the following situations would Bluetooth most likely be used?

   a. to connect to a corporate wireless network

   b. to attach a keyboard to a PC

   c. to connect a PC to a phone line

   d. to connect a flash drive to a camera

4. Which operating system is used with an Apple iPad?

   a. iOS

   b. Chrome

   c. iPadOS

   d. Android

5. List three recommendations for saving power on a laptop.

   _____

   _____

   _____

   Consider the following memory advertisements for laptop memory used in Question 6.

   a. 16 GB (2x8GB) 204-pin DDR3 SODIMM DDR3L 1600 (PC3L 12800) 1.35 V unbuffered

   b. 4 GB (2x2GB) 1,333 MHz DDR3 unbuffered DIMM

   c. 8 GB 260-pin DDR4 SODIMM 2400 (PC4 19200)

   d. 8 GB DDR3 204-pin SODIMM PC3-12800 memory

6. In these advertisements, which memory module(s) would work as an upgrade for a laptop, given the following specifications:

   Maximum of 16 GB. Configured with 4 GB DDR4 1 main memory slot (which is occupied).

   _____

7. Which solution would help a company manage the corporate apps deployed on employees' personal mobile devices?

   [MAM | iCloud | ActiveSync | PRL]

8. Which of the following are used to back up an iOS device? (Choose two.)

   [iBooks | iTunes | Tips | iCloud | iBackup | Backup]

9. Which type of laptop hard drive would provide the best performance?

   [mechanical | SSD | hybrid | stock]

10. What is a drawback of SSDs?

    [installation time | MTBF | maintenance requirements | cost | speed | reliability]

11. [T | F] A technician is sometimes judged and assumed to be competent or not competent based on what he or she is wearing.

12. Which icon would be used on a laptop to turn off Wi-Fi?

a.

b.

c.

d.

13. A laptop display is not showing anything, but the technician can hear the hard drive working. The technician connects an external monitor, and the monitor works. What should the technician try next?

a. Replace the laptop display.

b. Try connecting another external monitor.

c. Replace the laptop display connector.

d. Use the appropriate key to retest the output to the display.

14. What is the purpose of a laptop inverter?

a. to convert DC to AC for the CCFL backlight

b. to attach the keypad to the keyboard

c. to allow specific keys to be used as a numeric keypad, when enabled

d. to allow the display to be flipped backward

15. List three recommendations for laptop security.

_____

_____

_____

16. A hybrid drive is:

a. a mechanical hard drive.

b. an SSD.

c. a combination of an SSD part and a mechanical drive in the same case.

d. an upgraded flash drive.

17. Which of the following should be tried first if a mobile device is frozen?

a. factory reset

b. soft reset

c. hard reset

d. recovery

18. A user complains that he has slow data speeds on his mobile device. List three things you will check.

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

19. A mobile device continuously attaches to a nearby Bluetooth-enabled computer that is not the computer the user wants to attach to. What should be done?

    a. Disconnect the Bluetooth adapter from the nearby computer.

    b. Move the Bluetooth device closer to the desired computer.

    c. Power off the nearby computer.

    d. Put the mobile device in Airplane Mode.

20. A technician suspects that a mobile device has a security issue due to a rogue APK source because the user admits to just having updated the OS. Which type of mobile device is the technician working on?

    [Windows laptop | iPad | Apple laptop | Android device]

Exercises

Exercise 10.1 Identifying Laptop Parts

Objective: To identify various laptop parts correctly

Procedure: Identify each part in Figure 10.78 by matching the component name to the identified part in the photo.

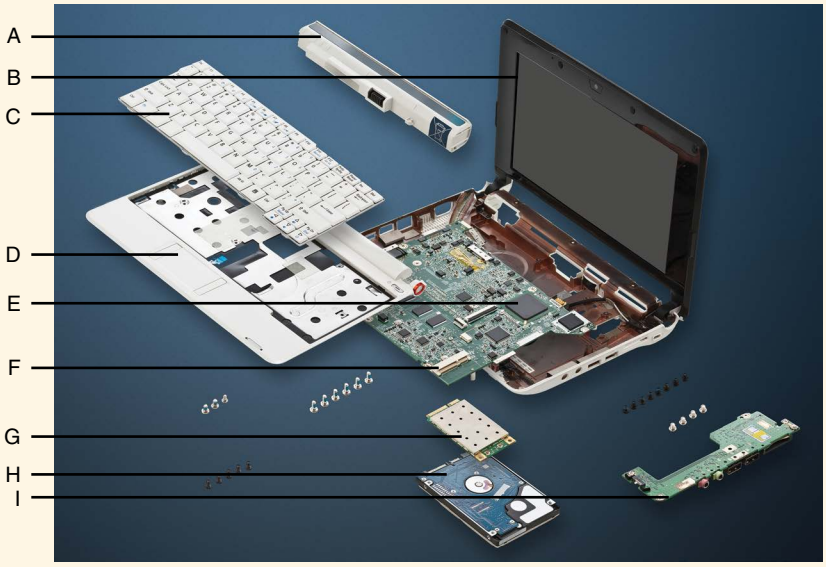


FIGURE 10.78 Laptop part identification photo

Components

LCD	Keyboard
Ports assembly	System board
Mounting bracket for touchpad	Processor
Hard drive	Palm rest assembly
Battery	

A. _____ **F.** _____

B. _____ **G.** _____

C. _____ **H.** _____

D. _____ **I.** _____

E. _____

Exercise 10.2 Common Laptop Keys

Objective: To identify various keys used on a laptop

Procedure: Match each laptop function key in Figure 10.79 to the description in Table 10.15.

FIGURE 10.79 Laptop function key identification photo

TABLE 10.15 Keyboard function key usage

a.	Increase volume	**g.**	Mute
b.	Decrease display brightness	**h.**	Increase display brightness
c.	Enable keyboard backlight	**i.**	Display mode
d.	Enable Bluetooth radio	**j.**	Enable touchpad
e.	Disable webcam	**k.**	Decrease volume
f.	Put in sleep mode	**l.**	Disable touchpad

F1	_____	F4	_____	F7	_____	F10	_____
F2	_____	F5	_____	F8	_____	F11	_____
F3	_____	F6	_____	F9	_____	F12	_____

Exercise 10.3 Where's the Part?

Objective: To determine the main locations of important laptop parts

Procedure: Identify each part as being located on the motherboard or in the display. Write your answers in Table 10.16.

Parts

CCFL	CPU	Digitizer
Inverter	M.2 SSD	mSATA
SODIMM	Webcam	Wi-Fi antenna

TABLE 10.16 Mobile device parts

On the motherboard	Within the display

Activities

Internet Discovery

Objective: To obtain specific information from the internet regarding a computer or its associated parts

Parts: Computer with internet access

Procedure: Complete the following procedure and answer the accompanying questions.

1. Watch the laptop SSD replacement video at the following URL to answer Questions 1–5: https://www.youtube.com/watch?v=E_sF9fRwyU4. (If this link does not work, find a video that shows a laptop hard drive replacement.)

   List one piece of software mentioned in the video that might be used to clone the operating system.

   _____

2. Use the internet to find an alternative cloning software that could be used. Detail why you think this software would be appropriate and why you chose it.

   _____

   _____

3. In the video, what did the technician do before removing the original drive in the laptop, and why did he say he did this?

   _____

4. What type of drive was the original one?

   _____

5. Where was the heat plate located?

   _____

   A customer owns a Toshiba Satellite R845-ST6N02 laptop. Use the Toshiba troubleshooting assistant program to help with a battery problem. Use information from this program to answer Questions 6–9.

6. What output values should be on the AC adapter?

   _____

7. Assume that the values on the AC power brick match those required on the computer. How long should the power button be held down after the external power and battery have been removed from the computer?

   _____

8. Which two colors can be used for the power indicator light, if it is working?

   _____

9. Assume that you have power, and you shut down the computer and remove the AC adapter. What might you do before assuming that the battery is dead?

   _____

10. A student has a ROG gaming laptop, and the function keys are not working. Use the internet to find what some people have done. List one or two solutions.

    _____

    _____

Soft Skills

Objective: To enhance and fine-tune a future technician's ability to listen, communicate in both written and oral forms, and support people who use computers and mobile devices in a professional manner

Activities:

1. In groups of three, each person finds a video that shows a particular model of laptop being taken apart. Share your findings with the others. Each team selects the best video to share with the class or submits the web link to the teacher.
2. Record yourself describing a mobile device problem and what you did to fix it, in three minutes or less. If you have never had a mobile device problem, use the internet to find someone else's problem and then describe it in your own words. No reading aloud. Tell the story.
3. In groups of six, three people must each find a cartoon or story that describes a funny mobile device situation. The other three people should find a cartoon or story that illustrates the need to dress professionally in the IT field. Each person must share findings with the group. Have a category for mobile and a category for appearance. Each person rates each cartoon or story. Summarize your findings in electronic format or verbally.
4. Each group is assigned one of the following laptop parts: (1) processor and heat solution; (2) mechanical, SSD, or hybrid storage device; (3) display; (4) system board; (5) inverter; or (6) backlight. Work in teams to outline in words and illustrations how to replace the part and issues related to the replacement. Present your group's work to the class.
5. Find a graphic or photograph that shows how you think a computer or mobile device technician might appear when professionally dressed. Then find another one that shows inappropriate attire.

Critical Thinking Skills

Objective: To analyze and evaluate information as well as apply learned information to new or different situations

Procedure:

1. Locate two laptop manuals from two different manufacturers. They cannot just be two models from the same manufacturer. Compare and contrast how the CPU is replaced in each one.

   _____

2. Select a laptop that has a mechanical hard drive and pretend it is yours and has been yours for at least a year. Now pretend that you are upgrading to an SSD or a hybrid drive. Select what hardware and software you might need and price it all out. Develop a step-by-step plan of action of how you are going to do this.
3. On a separate piece of paper, describe why Wi-Fi networks are so important to cell phone users. Are there any drawbacks to using them?

   _____

   _____

   _____

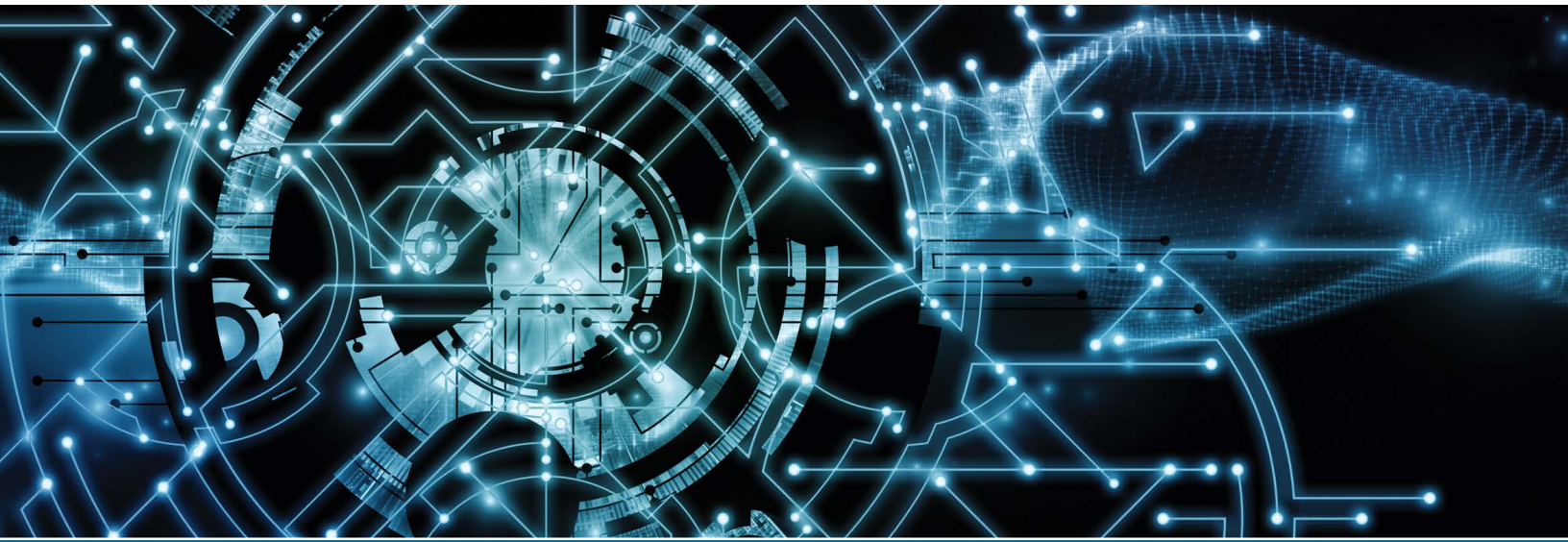
   _____

   _____

4. Find a technical job at monster.com, dice.com, or indeed.com. Then look online for at least three graphics or photos showing clothes you think someone would wear to the interview for this job. Find another three graphics or photos that depict what someone would wear on a daily basis for the job.

This page intentionally left blank

11 Computer Design and Troubleshooting Review



In this chapter you will learn:

- To select computer components based on the customer's needs
- The components best suited for a particular computing environment
- How to design for specific computer subsystems, such as the video or storage subsystem
- How to perform basic troubleshooting procedures
- How BIOS/UEFI controls the boot sequence and how that helps when troubleshooting
- The purpose of POST error codes
- How to deal with difficult customers or situations

CompTIA Exam Objectives:

- ✓ 1201-2.8 Explain networking tools and their purposes.
- ✓ 1201-4.1 Explain virtualization concepts.
- ✓ 1201-5.1 Given a scenario, troubleshoot motherboards, RAM, CPUs, and power.
- ✓ 1202-4.7 Given a scenario, use proper communication techniques and professionalism.

Design Overview

Why would employers want technicians to be able to design computers? If you needed a car repaired, wouldn't it be nice to have a person who could design cars to advise you? A designer would know the best engines, the most fuel-efficient body design, what parts might not work well with other parts, and so on. A designer would know a lot about all parts of the car. Similarly, those who can design computers know a lot about computer parts and how those parts interact with one another.

When you first learn about computers, you learn the language, or lingo. You learn terms such as *RAM* and *processor*. Later, when you hear these words, you form images in your mind. You do more than just recognize the words; you actually know what different parts look like. You can explain to someone else what a part does. You continue to grow in a particular area. Designing something is right up there with troubleshooting something well: It requires knowing what you are talking about.

Benjamin Bloom chaired a committee that created a classification of learning objectives that was named Bloom's Taxonomy. Look at Figure 11.1 to see how people normally progress through the learning process from the bottom to the top. Notice that creating is at the top. Of course, employers want people who can design: They are the folks who know all the things it takes to be able to design.

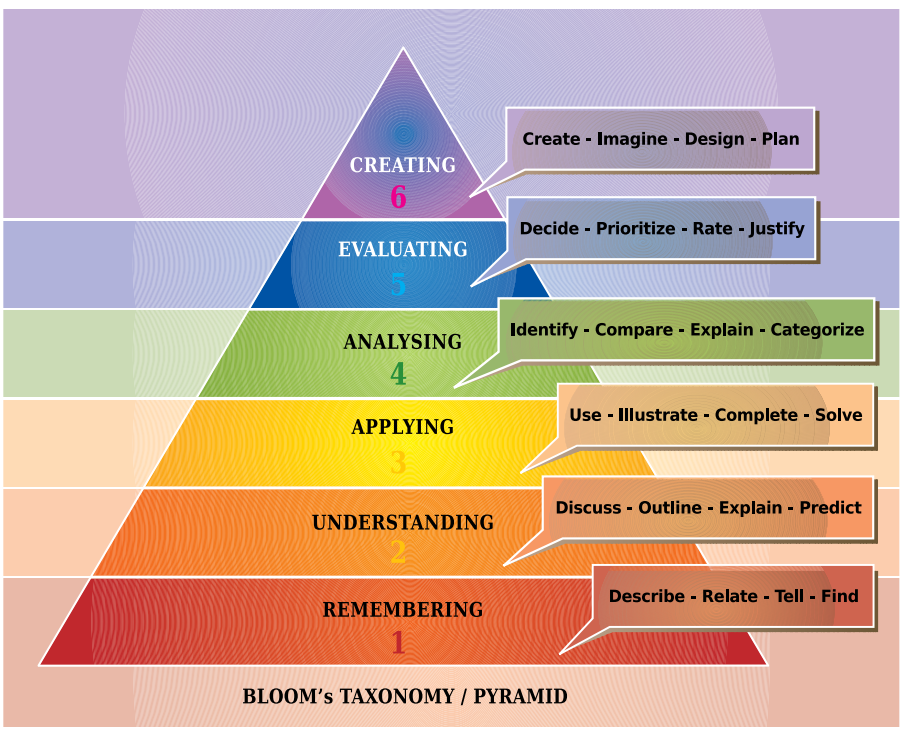


FIGURE 11.1 Bloom's Taxonomy

This chapter helps you learn how to select components within subsystems, such as video or audio, and the components needed for complete computer builds, based on the type of customer and the customer's needs. Even if you are designing just a subset of a computer, such as the video subsystem or a data storage subsystem, you must know how that subset interacts with other components that might need to be upgraded as well. Be sure to check out the exercises at the end of the chapter, which help put all this together. Practice is one of the best teachers.

Computer System Design

Computer users need different types of computer systems. What a user does with a computer dictates the components and peripherals needed. Looking at computer systems by purpose is a good place to start with design.

Graphic/CAD/CAM Design Workstations

Engineers and design engineers use computer-aided design (CAD) and computer-aided manufacturing (CAM) systems in manufacturing plants to create things. Graphic design personnel also use a similar type of system (see Figure 11.2). A **graphic/CAD/CAM design workstation** needs the following key components:

- Powerful multicore processor(s)
- Maximum system RAM
- Solid-state drive (SSD)
- High-end video card(s) with maximum video RAM and graphics a processing unit (GPU)
- Large display or dual displays
- Large-capacity hard drive(s)
- Optional peripherals such as digital tablets, scanners, plotters, and 3-D printers
- Good-quality mouse or other input device

FIGURE 11.2 CAD/CAM design workstation

Gaming PCs

A gaming computer is a unique type of PC. Gamers frequently build their own systems, but some computer manufacturers make gaming PCs. A **gaming PC** (see Figure 11.3) tends to have the following key components:

- Powerful multicore processor(s)
- High-end video cards (with maximum video RAM and specialized GPU)
- High-definition sound card and speakers
- High-end system cooling
- SSD
- Large amount of RAM
- Large display or dual displays

- Quality mouse
- Optional gaming console
- Headphone with microphone
- Optional 3-D glasses (if supported by the video card and monitor)

FIGURE 11.3 Gaming PC

Audio/Video Editing Workstations

An **audio/video editing workstation** (see Figure 11.4) is used to manipulate sounds (shorten, add, overlay, and so on) or video. This type of system requires a lot of hard drive space and RAM. These are the most common configuration elements for such a computer:

- Specialized video card with maximum video RAM and GPU
- Sound card and speakers
- Fast and large-capacity hard drive
- Dual monitors
- Powerful multicore processor(s)
- Large amount of system RAM
- Quality mouse
- Possible digital tablet or scanner

FIGURE 11.4 Audio/video editing workstation

Network-Attached Storage (NAS) Devices

A network-attached storage (**NAS**) device can be a single box that contains multiple hard drives used for storing photos, movies, and files from multiple computers in a home or small office environment (see Figure 11.5). It is commonly used for media streaming of videos and music and file sharing in the home environment. A diskless NAS is a storage container that comes without disks so you can add your own mechanical drives or SSDs.

FIGURE 11.5 Home or small business NAS

In a corporate environment, a NAS can also be rows of hard drives in a larger company environment (see Figure 11.6). These drives provide storage for multiple servers and users and are commonly configured in a RAID array for data recovery in case one drive fails.

FIGURE 11.6 Corporate NAS

Virtualization Workstations

A **virtualization workstation** has at least one operating system, in its own **virtual machine** that is separate from the host operating system (see Figure 11.7). Keep in mind that because each virtual machine has its own operating system, each one needs to have its own applications and security installed. Note that a controlled virtualized workstation in a business environment is

known as a virtual desktop, as discussed in Chapter 12, "Internet Connectivity, Virtualization, and Cloud Technologies."

A virtualization workstation has the following components:

- Maximum CPU cores
- Maximum RAM
- Multiple fast, large-capacity hard drives
- Possible SSDs
- Possible network-attached storage for increased storage space that can be shared with other devices

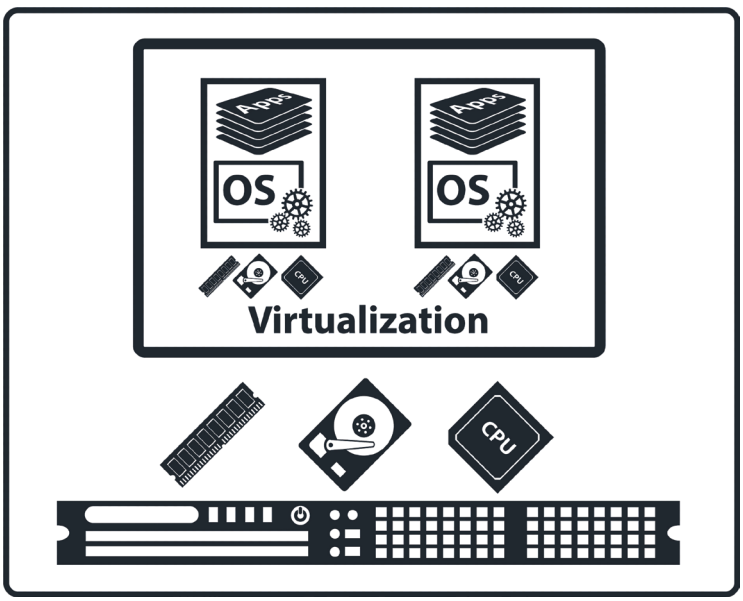


FIGURE 11.7 Virtualization workstation concepts

Thin Client Workstations

A **thin client** workstation is a desktop or laptop that has a display, mouse, keyboard, and network connectivity and runs applications from a server. There is very little software added to the computer. Thin client computers provide security to critical data and applications and are commonly used in airports, hotels, and corporate areas where the information accessed or software used is centralized.

Thin client computers are less expensive than normal workstations; however, the network infrastructure (for example, servers, software, storage area network [SAN]) to support thin clients costs money. Storage tends to be cloud based or on remote storage media. Both the hardware and software environments can be virtualized (commonly referred to as desktop virtualization) in order to provide a controlled environment. Corporations, medical offices, and call centers commonly use thin clients (see Figure 11.8).

Characteristics to look for in a thin client computer include the following:

- Meets minimum requirements for the selected operating system
- Network connectivity (1 Gb/s preferred)
- Only used for basic applications, such as word processing, spreadsheet manipulation, and web-based apps
- Optional display privacy screen

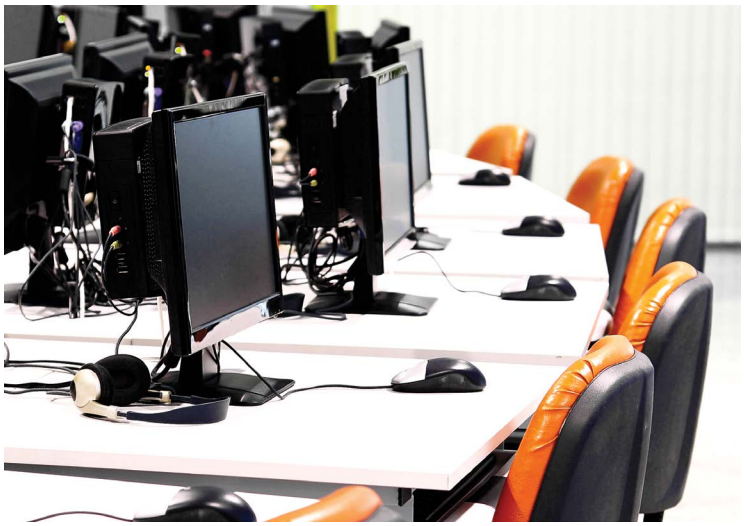


FIGURE 11.8 Thin client workstations

Standard Thick Client Workstations

A **thick client** computer is the most common type of desktop or laptop in the work environment. Applications are installed and documents are commonly stored on the local hard drive. An all-in-one computer could be a thick client computer. Computers in small businesses tend to be thick client workstations. A thick client computer has the following characteristics:

- Meets minimum hardware requirements for the selected operating system
- Desktop applications (each one meeting recommended hardware and software requirements)
- Optional display privacy screen
- Optional dual displays

Home Servers

A **home server** computer is used to store data; function as a web server, print server, or file server; control media streaming; be accessible from outside the home; control devices; and manage backups of other computers. Notice in Figure 11.9 that the home server in the top-right corner can be used to back up files from other home devices, such as a laptop. Servers and networks are discussed in Chapter 13, "Networking." Typical components in a home server include the following:

- Multiple hard drives in a RAID array configuration
- 1 Gb/s (1000 Mb/s) NIC
- Medium to large case
- Multiple processors or multiple cores in the processor
- 8 GB or more RAM
- Server applications, including media streaming, file sharing, and print sharing applications
- Optional NAS
- Optional KVM switch

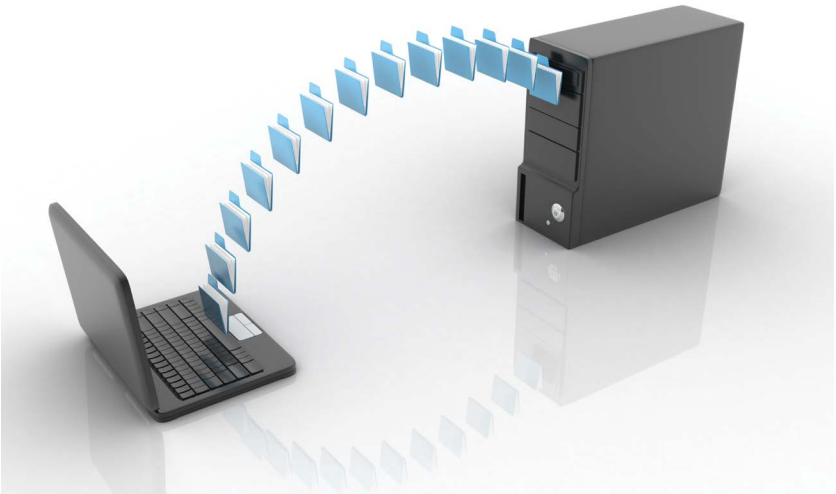


FIGURE 11.9 Home server

Go Green

Keep in mind that there are many ways to go green and conserve energy in computer design. The company requesting a design may require green specifications. Cases, motherboards, processors, power supplies, printers, displays, and other computing devices can be designed with energy conservation in mind. The Electronic Product Environmental Assessment Tool (EPEAT) can help with that.

The **EPEAT rating system** was designed to work with the EPA in identifying products that have a green (and clean) design. **ENERGY STAR** is another program that requires strict energy efficiency. Products that earn the ENERGY STAR rating today have low total energy requirements, low-power modes, and efficient power supplies.

Another aspect of being green is recycling old components. Check the local disposal regulations and requirements and find places that can recycle your old electronics (see Figure 11.10).

You can also be conscientious of energy requirements when designing a subsystem. Upgrade requests might be for a computer subsystem. In such a case, the best practice is to look at the subsystem as a unit. The following sections examine the various computer subsystems.

FIGURE 11.10 Computer parts recycling

Motherboard and Associated Component Design

The motherboard, chipset, and CPU are all directly related to one another and should be designed in conjunction with one another. If you buy an Intel motherboard, then you have to get an Intel processor; alternatively, you can use an AMD motherboard and processor. Newer technologies may influence your choices.

TECH TIP

Don't forget the cooling

If you select a high-end CPU, you must have appropriate cooling for it.

Memory ties into processor technology because the type of motherboard/chipset dictates the type of memory supported, the maximum amount of memory the motherboard manufacturer might consider putting on the motherboard, and the maximum memory speed that can be used. Whenever a technician is upgrading or replacing a motherboard, compatibility with existing components is a requirement.

The most important design consideration for memory is to take advantage of dual-, triple-, and quad-channeling, when possible. Ensure that the memory modules are purchased together and installed according to the recommendations set forth in the motherboard/computer manual. Encourage an end user to buy as much RAM as they can initially afford. Memory is one of the most influential considerations on the user's computing experience. Beef up this subsystem component as much as possible.

When dealing with the motherboard, consider the form factor, chipset, whether the CPU is included, CPU size, motherboard socket size, nanotechnology used with the processor and/or chipset (14 nm, 22 nm, 32 nm, 45 nm, and so on), CPU cooling, RAM, and the number and type of memory slots/CPU sockets.

Power Supply and Case Design

When selecting a power supply, the main concerns are size (form factor), total wattage for specific voltage levels, number of connectors, and power efficiency. One issue you must consider is how many connectors connect to the same cable. When you have several high-powered devices, you want to be able to connect them with separate power cables, if possible, instead of using two connectors along the same cable. Also, be careful with cables that do not have at least four wires. These are peripheral cables to power 12-volt fans and are normally labeled as fan connectors. Some power supplies have detachable cables that connect between a power supply connector and a device connector. You attach the number and type of cables you need. Buy additional cables of a specific type, as needed. Figure 11.11 shows detachable cables.

When replacing, upgrading, or purchasing a power supply, considerations include the number of power cables needed for video cards, number and type of power cables, form factor, wattage for the 12-volt line, total wattage (determined using an online power-use calculator), quietness, mean time between failures (MTBFs), overvoltage, overcurrent, undervoltage and short-circuit protection, and warranty period.

The power supply, case, and motherboard have to be the same form factor. Some cases accept multiple motherboard form factors. Most cases have at least two locations for fans: one fan at the front of the case and one at the rear. Fans tend to come in 40, 60, 80, 90, 92, 120, or 140 mm sizes. Look for the following key features in a new case: size, type (desktop or tower), number and type of front panel ports, number and placement of fans, cable management, expansion slots, drive bays, and ease of cover removal.

FIGURE 11.11 Detachable cables for some power supplies

Table 11.1 lists recommendations for cases and power supplies for different types of users.

TABLE 11.1 Power supply and case design

Use	Design considerations
Graphic/CAD/CAM, gaming PC, home server PC, audio/video editing computer, or virtualization computer	500W or higher power supply ATX mid- or full-sized tower Two or more case cooling fans
Thin client	300W or higher power supply Mini-ATX or microATX tower
Standard thick client or normal user	300W or higher power supply ATX, mini-ATX, microATX, or mid-sized ATX tower

Figure 11.12 shows a computer case that has removable drive trays for internal hard drives.

FIGURE 11.12 Case with removable internal hard drive trays

Storage Subsystem Design

The storage subsystem consists of magnetic or flash technologies for internal or external hard drives, flash storage (including SSDs), or optical drives. When adding, replacing, or building a storage subsystem, you must take into account the customer's needs, how long the customer plans on storing the data, and how long the customer thinks the storage subsystem will be in use before being upgraded or replaced. Table 11.2 helps with the storage device options.

TABLE 11.2 Storage subsystem design considerations

Feature	Design considerations
Internal connectivity	SATA or M.2
Internal power	Molex or SATA power connector
Internal physical size	1.8, 2.5, 3.5, or 5.25 inches, with an available expansion slot in the case
External connectivity	USB, IEEE 1394 (FireWire), eSATA, or eSATAp port NIC, if required, for cloud (internet) storage Media reader for flash media, if needed
External power	Either external power cord or power provided by the USB, IEEE 1394, or eSATAp port
Storage technology	Magnetic (hard drive or optical drive); SATA 1.5, 3, or 6 Gb/s (SATA1, SATA2, or SATA3), M.2, flash memory (SSD, flash drives, and flash media), or hybrid (magnetic and SSD)
Special storage considerations	Multiple drives, if RAID is used NAS to share storage with other computers
Storage device speed	5,400, 5,900, 7,200, 10,000, or 15,000 RPM for magnetic drives Transfer rate for SSDs Input/output operations per second (**IOPS**) for both magnetic drives and SSDs, which is a measurement that takes into account sequential reads/writes as well as random reads/writes
Optical drive features	Read-only or read/write; red-violet and/or blue laser(s)
Drive buffers	Extra memory in storage drives that can increase data transfer rates

Audio Subsystem Design

The audio subsystem consists of the audio ports and speakers. When upgrading or building an audio subsystem, let the customer listen to the speakers, if possible. Table 11.3 lists audio design considerations.

TABLE 11.3 Audio subsystem design considerations

Feature	Design considerations
Number of speakers	Two for a casual user or gamer; three to seven for a music, video, or gaming enthusiast 5.1 surround-sound system: center channel speaker, two front channel speakers for left/right audio, two rear channel speakers for left/right audio, and a subwoofer for low-frequency (bass) sound effects 7.1 surround-sound system: the same speakers as 5.1, with two additional center channel speakers for left/right audio

Feature	Design considerations
Microphone	Integrated into the display, headset, or external, with a headset being best for conference calls
2.0 or 2.1	2.0 audio subsystem: two channels (left and right), with an amplifier within one of the two speakers 2.1 audio subsystem: two speakers and a subwoofer for lower-frequency sounds
Port connectivity	3.5 mm mini-plug, S/PDIF TOSLINK, S/PDIF fiber, or wireless
Sound card	PCI, PCIe, or integrated into the motherboard Number and type of sound ports matching the speaker connectivity
Logistics	Elimination of trip hazards Shelving, wall plates, wall inserts, wall hangers Speaker location planning

Display Subsystem Design

Displays are important to the computing experience. With respect to replacing, upgrading, and installing displays, design specifications are important. Multiple displays are the norm in many work environments. Some jobs require many displays (see Figure 11.13).

FIGURE 11.13 Multiple displays

Table 11.4 lists some design considerations for displays.

TABLE 11.4 Display subsystem design considerations

Feature	Design considerations
Size/aspect ratio	Common determining factors include physical location, available space, and cost Common aspect ratios: 4:3, 16:9, 16:10, and 1.9:1
Number of displays	Two displays or a single widescreen display
Type of display	Plasma, LCD with CCFL backlight, LCD with LED backlight (LED), or OLED Touch screen

Feature	Design considerations
Display conferencing features	Integrated microphone or webcam
Contrast ratio	A higher number is better and keep in mind that not all vendors give true numbers
Video adapter	Number and type of ports Number of cards and support for sharing of resources (for example, SLI, CrossFire) Memory GPU Power and cooling requirements Power connectivity requirements

Troubleshooting Overview

When a computer does not work properly, a technician must exhibit one essential trait: the will to succeed. The main objective is to return a computer or peripheral to service as quickly and economically as possible. When a computer is down, a business loses revenue and productivity. Therefore, a technician must have a good attitude and great perseverance and drive to resolve the problem at hand quickly, efficiently, and in a professional, helpful manner.

TECH TIP

Back up data

Before any changes are made to a system, ensure that its data is backed up, if possible.

A technician must use all available resources, including documentation for a particular peripheral, motherboard, or computer; the internet; their five senses; other technicians; corporate documentation; textbooks; experience with similar problems; training materials; previous service history on a particular customer/computer; information from users or those around them (see Figure 11.14); and online databases provided by companies or partners. Technicians can be tenacious, but they keep in mind that time is money, and solving a problem quickly with the least downtime to the customer is a critical component of a computer support job.

FIGURE 11.14 Technician gathering information from a computer user

TECH TIP

Before making changes…

Consider corporate policies, procedures, and impacts before implementing changes.

Evaluating and solving a technology problem is a high-level objective in Bloom's Taxonomy, as shown earlier in the chapter (refer to Figure 11.1). Teaching someone to troubleshoot is challenging. Not every problem can be described in a step-by-step fashion. Troubleshooting is easier if a technician uses reasoning and takes logical steps. Logical troubleshooting can be broken down into six simple steps:

Step 1. Identify the problem.

Step 2. Establish a theory of probable cause. (Question the obvious.)

Step 3. Test the theory to determine the cause.

Step 4. Establish a plan of action in order to resolve the problem and implement the proposed solution.

Step 5. Verify full system functionality and, if applicable, implement preventive measures.

Step 6. Document the findings, actions, and outcomes.

When following these steps, do not forget to consider company policies, procedures, and how any changes may impact company functions.

Step 1. Identify the Problem

Computer problems come in all shapes and sizes. As part of step 1, you gather information from the user and see if the user has changed anything. Many problems relate to the people who operate computers—the users. Users may fail to choose the correct printer, press the wrong key for a specific function, or issue an incorrect command.

Have the user demonstrate or re-create the problem. Because the user is often the problem, you can save a great deal of time by taking this step. Do not assume anything! A user may complain that "my hard drive does not work" when, in fact, there is no power to the computer. Often users repeat computer terms they have heard or read, but they do not use them correctly or in the right context. By asking a user to re-create a problem, a technician has a chance to see the problem as the client sees it. This should be done even during a phone consultation. Whether diagnosing a problem on the phone or in person, be sure to follow these guidelines:

- Do not assume anything; ask the user to re-create the problem step-by-step.
- Question the user. Ask the user if anything has been changed. Do not be threatening; you want the user to be forthright and honest. Ask open-ended questions to get an idea of what is wrong. Use closed-ended questions (those that require a yes or no answer) to narrow the problem. Refer to Figure 1.2 in Chapter 1, "Introduction to the World of IT," to see examples of these techniques.
- Inquire about any environmental or infrastructure changes in the work environment. Has anything been added to the computer or network recently? Has any maintenance work been done in the area?
- Verify obvious conditions, such as power to the monitor or speakers muted through the settings.
- Do not assume that there is not a problem if the user cannot re-create it. Some problems occur intermittently.
- Use all your senses. Listen for noises such as from the power supply, case/CPU fans, speaker feedback, hard drive, or optical drive. Power off if you detect a burning smell.
- **Back up data**, if possible, before making changes (see Figure 11.15).

FIGURE 11.15 Back up user data before making changes

Step 2. Establish a Theory of Probable Cause (Question the Obvious)

In order to establish a theory of probable cause, you have to have heard or seen the problem as explained by the user. A lot of times, you establish a theory based on analyzing the problem and determining whether the problem is hardware or software related (or both) by using your senses. Sight, hearing, and smell can reveal a great deal. Smell for burning components. Watch the computer boot, look for lights, listen for beeps, and take notes.

Review system and application logs. Operating system logs document what occurs during normal and abnormal conditions. Applications also log issues. For hardware issues such as those related to motherboards, RAM, CPU, or power, make sure you examine log entries and error messages displayed. Use the Windows *System Configuration* window > *Boot* tab and enable the *Boot log* checkbox > *Apply* > *OK* > *Restart*. Within the Options window, select *Enable Boot Logging* > *Reboot* > and examine the logging file `ntbtlog.txt` (by opening the *Run* option and searching for `C:\Windows\nbtlog.txt`)

Finally, use internal resources such as coworkers or your boss. Use external resources including the internet to research symptoms. Do not forget to question the obvious.

The Boot Process

One thing that might help you establish a theory of probable cause is to examine the boot process. Frequently, a hardware problem is detected during the power-on self-test (POST) executed by the BIOS/UEFI when the computer is first powered on. Remember that the traditional BIOS is looking for the boot loader (a small bit of code on a drive). The computer is configured with a specific device boot order. Knowing the steps taken during the boot process can help you troubleshoot an older machine that has a traditional BIOS:

Step 1. The power supply sends a power good signal.

Step 2. The CPU looks in BIOS for software.

Step 3. The CPU executes POST from BIOS. Note that any errors are usually audio or motherboard LEDs or codes at this point.

Step 4. System resources (I/O address, memory addresses, and interrupts) are retrieved from nonvolatile RAM (NVRAM, which is RAM that can be changed but where data is not lost when power is removed) and assigned to ports, devices, and adapters.

Step 5. Video is initialized, and a cursor appears.

Step 6. POST continues to check hardware and error messages, and codes can now appear on the display.

Step 7. Based on the boot order configuration in System Setup, the system checks for an operating system from the specified devices.

Step 8. The computer loads an operating system found from the first device that contains an operating system or displays an error.

On a newer computer that has a UEFI BIOS, things can be a bit different. A UEFI BIOS can optionally have a BIOS compatibility mode in which the computer behaves as previously described. However, if the system is natively booting using UEFI, the UEFI standards require a common format for executable code. This allows much more flexibility in the boot process, as UEFI has to be able to interpret (not just recognize) globally unique identifier (GUID) partition table (GPT) partitions and the traditional master* boot record (MBR). UEFI supports larger drives and partitions.

UEFI has a boot manager. This boot manager can load UEFI drivers and applications and is customizable. These are not operating system drivers. This means that if the operating system has issues, you can still use your mouse and other devices that have UEFI drivers within the UEFI environment and with UEFI applications that could help with troubleshooting. Refer to Chapter 4, "Introduction to Configuration," for a refresher on the UEFI BIOS. Figure 11.16 shows the boot sequence for a UEFI-based device.

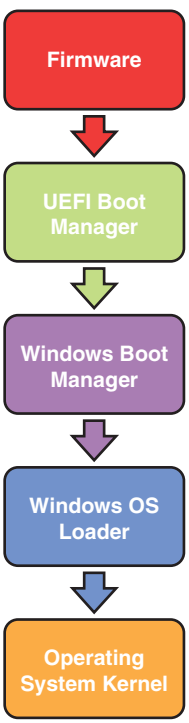


FIGURE 11.16 UEFI boot order

* **NOTE** Use of the term *master* is ONLY in association with the official terminology used in industry specifications and standards and in no way diminishes Pearson's commitment to promoting diversity, equity, and inclusion and challenging, countering, and/or combating bias and stereotyping in the global population of the learners we serve.

POST Codes and Error Messages

During the firmware phase—whether UEFI or BIOS is used—POST checks out the hardware in a sequential order, and if it finds an error, the BIOS/UEFI issues a beep, displays a numeric error code, or displays an **error message**. Make note of any error codes, beeps, or messages. The number or duration of beeps, the meaning of numeric error codes, and the type of error messages that appear are different for different computers.

TECH TIP

Audio POST code: Checking video and RAM first

Have you ever been working on a computer and gotten a POST code that you didn't want to take the time to look up? Audio codes are frequently related to video and memory. Check connections and reset the card or module.

The secret is knowing the BIOS/UEFI chip manufacturer. The computer or motherboard documentation sometimes contains a list of codes or beeps used for troubleshooting. A single beep is a common tone heard on successful completion of POST, when hardware errors were not detected. Listening is an important part of troubleshooting.

Table 11.5 lists the audio beeps heard on Dell computers. Table 11.6 lists audio beeps for computers that have an AMI BIOS/UEFI chip installed. Table 11.7 lists the audio beeps heard on a computer with a Phoenix BIOS/UEFI chip installed. When you see a series of codes like 1-1-2, it means the computer beeps once, pauses, beeps again, pauses, and then beeps two times.

TABLE 11.5 Dell computer POST audio beeps

Beeps	Description of problem
1	Motherboard/UEFI BIOS
2	RAM
3	Motherboard or chipset
4	RAM
5	Real time clock power failure
6	Video BIOS
7	CPU

TECH TIP

Troubleshoot the first POST code heard or seen

If multiple POST errors occur, start by troubleshooting the first one heard or seen.

TABLE 11.6 AMI BIOS/UEFI audio beeps

Beeps	Description of problem
1 short	RAM
2 short	RAM
4 short	Motherboard timer
6 short	8042 Gate A20 test error
8 short	Display RAM
9 short	ROM checksum error

TABLE 11.7 Phoenix audio beep codes

Beeps	Description
1	Normal POST
1 short 1 long	RAM
1 long 2 short	Motherboard
1-1-2	CPU
1-1-3	Real time clock/CMOS
1-1-4	BIOS checksum
1-1-1-1 or 1-3-4-1	RAM

Don't get frustrated when error messages appear on the screen. Error messages are good things in that they assist you in troubleshooting. Table 11.8 lists the POST error messages that sometimes appear.

TABLE 11.8 BIOS/UEFI POST error messages

Message	Description
BIOS ROM checksum error—System halted	The BIOS/UEFI has a problem and needs to be replaced.
CMOS battery failed/error	Replace the motherboard battery.
CMOS checksum error—Defaults loaded	CMOS has detected a problem. Check the motherboard battery.
CMOS timer error	The system date/time has not been set. Check/replace the motherboard battery if this is not the first time this computer has been powered on.
Hard disk install failure	The BIOS/UEFI could not find or initialize the hard drive. Check the hard drive connectivity and power.
Intruder detection error	The computer chassis has been opened.
Keyboard error or no keyboard present	The keyboard could not be found. Check the cabling.
Keyboard is locked out—Unlock the key	Ensure that nothing rests on the keys during the POST.

Message	Description
Memory test fail	A RAM error occurred. Swap the memory modules.
Memory size decrease error	The amount of system RAM has decreased. Check to see whether RAM has been stolen, needs to be reseated, or needs to be replaced.
Memory optimal error	The amount of memory in channel A is not equal to channel B. For optimal memory performance, the channels should have equal memory. See Chapter 6, "Memory," for more details.
Override enabled—Defaults loaded	The current settings in CMOS could not be loaded, and the BIOS/UEFI defaults are used. Check the battery and CMOS settings.

A BIOS/UEFI can be sold to various computer manufacturers that are then allowed to create their own error codes and messages. Look in the motherboard/computer manual or on the manufacturer's website for a list of exact error messages.

TECH TIP

Check motherboard manual or website for the latest error codes

Manufacturers constantly produce BIOS/UEFI upgrades, and you can use the internet to verify POST errors that occur and the recommended actions to take.

In addition to generating audio tones or numeric error codes or written messages, the motherboard might provide additional troubleshooting information, such as the following:

> You might see a **proprietary crash screen** or a screen showing something that is unique to a specific manufacturer.

> In Windows, you might see a blue screen of death (**BSOD**) with a numeric code and/or a message. You might also see the system display a message saying a particular application is not responding or nothing is happening at all. Use *Task Manager* to stop the application or give the application more time to complete the task. Close other open applications. See Chapter 16, "Advanced Windows," for more Windows troubleshooting.

> On macOS or Linux operating systems, you might see a colored **pinwheel** that appears to turn forever. Use *Activity Monitor* to check for processor and RAM performance and free disk space and/or to stop the problematic application. See Chapter 17, "macOS and Linux Operating Systems," for more tips for troubleshooting Mac and Linux systems.

When a numeric code appears or when certain lights illuminate, you have to use the internet or motherboard/computer manual to determine the issue. Some motherboards have a numeric display or colored indicators that display as part of the POST. The meaning of the visual clues can be found in the motherboard or computer manual.

Other Diagnostics

Some technicians carry a POST card as part of their toolkit. A **POST card** is a PCI/PCIe adapter or USB-attached card that performs hardware diagnostics and displays the results as a series of codes on an LED display or LED light(s). These are not as popular today as they once were because many UEFI-based motherboards include powerful diagnostics that can be downloaded from the computer manufacturer's website. However, a POST card is useful if a system does not boot and no other symptoms appear.

TABLE 11.9 UEFI diagnostic types

Diagnostic	Description
Express, start, or system test	Similar to POST, checks the main hardware components needed to load the operating system.
Component test	Allows selection of individual parts to test.
Hard drive test	Checks the drive for bad areas and has the capability to mark an area and not use it in the future.
Memory test	Performs multiple reads/writes to memory locations.
Battery test	Checks the battery's power level.

Some motherboard LEDs are used in conjunction with switches that can be pressed to test components. Figure 11.17 shows a motherboard LED, and Figure 11.18 shows some common uses of motherboard LEDs.

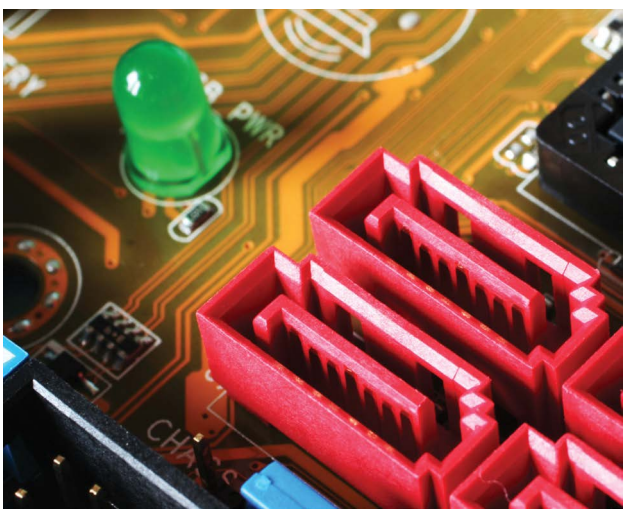


FIGURE 11.17 Motherboard LED

Examples of Motherboard Switches and LEDs

Switch	LED	Explanation
MemOK!	MemOK	Depress the MemOK switch to determine if the RAM modules are compatible. The MemOK LED illuminates if so.
EPU	EPU	Enable the EPU switch or enable through BIOS to allow the motherboard to moderate power consumption. When enabled, the EPU LED is lit.
	RAM	The RAM LED illuminates for a memory error.
	Power	The power LED commonly illuminates when power is applied, or if the computer is in either the sleep or soft off power mode.

FIGURE 11.18 Motherboard switches and LED usage

Hardware Errors

Hardware errors sometimes occur. For example, a display might suddenly go black, an optical drive's access light might not go on when the drive attempts to access the optical disc, or a printer might repeatedly flash an error code. If you suspect a physical port problem, you can use a loopback plug to test the port. A **loopback plug** sends a signal out one or more electrical pins and allows the signal to come back in on one or more different pins. Uses for a loopback plug are to test a communication circuit port like the internet or fiber connection or an RJ45 loopback plug to test network port functionality.

TECH TIP

What to do if you smell smoke coming from a computer

Unplug the device if you can. Pull the fire alarm. Call 911. If you see smoke, get a fire extinguisher and PASS (pull the pin, aim at the base of the fire, squeeze the trigger, and sweep slowly side to side).

Hardware errors are usually obvious because of POST error codes or errors that occur when accessing a particular device. Also, some peripherals, such as hard drives and printers, include diagnostics as part of the software that is loaded when the device is installed. These diagnostics are frequently accessed through the device's *Properties* window.

Random Device Failure

Sometimes, none of the hardware troubleshooting actions described so far work. In such a case, a grounding problem might be the issue. Symptoms of a grounding problem include intermittent or unexplained shutdowns.

To troubleshoot a **random device failure**, build the computer outside the computer case on an antistatic mat, if possible. Start with only the power supply, motherboard, and speaker connected. Even though it will normally produce a POST audio error, verify that the power supply fan turns. Most power supplies issue a click before the audio POST beeps. Next, verify the voltages from the power supply. If the fan turns and the voltages are correct, power down the machine and add a video adapter and monitor to the system. If the machine does not work, put the video adapter in a different expansion slot and try again. If placing the video adapter in a different expansion slot does not work, swap out the video adapter.

If the video adapter works, continue adding devices one by one and checking the voltages. Just as any one device can prevent a system from operating properly, so can any adapter. If one particular adapter causes a system to malfunction, try a different expansion slot before trying a different adapter. If the expansion slot proves to be a problem, check the slot for foreign objects. If none are found, but the problem still occurs, place a note on the expansion slot so that no one will use it.

An intermittent device failure is one of the hardest things to troubleshoot. Devices commonly associated with intermittent device failure are the motherboard, RAM, processor, and power supply; however, a failing hard drive can also present as an intermittent device failure if the drive is starting to have problems.

Of the motherboard, RAM, processor, and power supply, RAM is the easiest to troubleshoot, even if there are multiple memory modules installed. Before trying anything else, remove power to the system and push firmly on the memory modules. They can creep up a bit even with the side locking levers in place. Power on and see if the problem reappears. If it doesn't, swap the modules to see whether symptoms change or remove one of the modules. If the system remains stable, reinsert the module and see whether the intermittent failure returns.

For intermittent power issues, first check the power output with a power supply tester. Also check the power supply wattage and ensure that it is adequate for the number of installed devices. Inspect power connectors to ensure that they have not gotten caught or crimped in the cover.

Determining whether a problem is a motherboard or a processor is tough. The easiest thing to do is check the processor on a different (compatible) motherboard. You might see whether you can use a particular UEFI diagnostic to do an extended test on the motherboard and processor.

Software Errors

Software errors occur when a computer user accesses a particular application or file or when the system boots. Applications sometimes present error messages like POST does, but they are application specific. Sometimes an application restarts itself or needs to be manually stopped through Task Manager. Then you can open the application again.

Some software errors relate to hardware, such as a USB-to-serial adapter. If the application being used with such an adapter locks, unplugging the USB cable and reinserting may cause the hardware and software to start working again.

Sometimes a software problem can be resolved with a **warm boot**. Warm booting causes any changes that have been made to take effect without putting as much strain on the computer as a cold boot does. A warm boot can be performed in various ways, but one way is through the *Start* button > *Power* icon > *Restart*.

Files that affect the booting process, such as files in the Startup folder, are dependent on the operating system. If in doubt as to whether a problem is hardware or software related, use Windows *Device Manager* to test the hardware to eliminate that possibility. Every software program has problems (bugs). Software manufacturers typically offer software **patches** or **service releases** to fix known problems. Patches or service releases are usually available on the internet from the software manufacturer. It is important to keep applications and the operating system patched. A **service pack** usually contains multiple patches and installs them at the same time rather than in multiple downloads.

Take your time with this step, gathering all the details you can to come up with as to what the problem could be. Figure 11.19 shows some problem-solving strategies you could use during this part of the troubleshooting process.

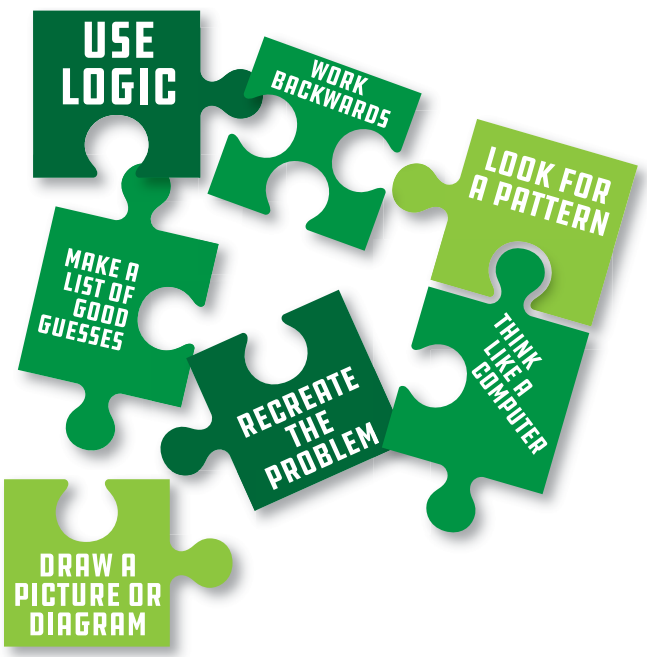


FIGURE 11.19 Problem-solving strategies

Step 3. Test the Theory to Determine the Cause

Once you have a theory or suspect a general area and your theory is confirmed, you need to determine the next steps needed to resolve the problem. If you go through a series of steps and the problem is unresolved, you might have to step back and re-evaluate the problem. From there, you can establish a new theory or, if needed, escalate the problem to a more senior technician.

Divide the problem into logical areas and continue subdividing the problem until you have isolated it. For example, if an error appears each time the computer user tries to write data to a flash drive, the logical places to look are the user's flash drive, the port that it connects to, potentially a cable that connects the port to the motherboard, the motherboard circuits that control that port, the BIOS/UEFI settings where the port could be disabled, and the software program that is currently being used. Any of these may be the cause of the problem.

Ernie Friend, a technician of many years, advises students to divide a problem in half, and then divide it in half again, and then continue to divide it until the problem is manageable. This way of thinking carries a technician a long way. Also, keep in mind that you will eventually beat the problem at hand! You are smarter than any problem!

TECH TIP

Reinstall the original part if a replacement part does not fix the problem

Reinstall the original part if the symptoms do not change after changing out that part. Then continue troubleshooting.

Here's how you could use Ernie's philosophy with a flash drive problem: Divide the problem in half by determining whether the problem is hardware or software related. To determine whether the software application is causing the problem, try saving a file to the flash drive from another application. If the second application works, then the problem is in the first application. If both applications have problems, the problem is most likely in the hardware or the BIOS/UEFI. The next easiest thing to eliminate as a suspect is the flash drive. Try a different flash drive. If a different flash drive works, then the first flash drive was the problem. If neither drive accepts data, the problem is the port, cable, motherboard, or BIOS/UEFI settings. Try a different port. If that works, then something is wrong with the port or the cable that goes from a front panel port to the motherboard, the port is disabled in Device Manager, or the port is disabled in the BIOS/UEFI settings.

If a hardware problem is evident after a POST error or peripheral access/usage error occurs, consider the problem a subunit of the entire computer. For example, if a POST error occurs for the optical drive, the subunit is the optical drive subsystem, which consists of the drive, the cable, and the controlling circuits that may be on an adapter or the motherboard.

If a problem is software related, narrow it to a specific area. For example, determine whether the problem is related to printing, saving, or retrieving a file. This may give you a clue about what section of the application is having a problem or may lead you back to considering other hardware components as the cause of the problem.

TECH TIP

Change or check the easy stuff first

When isolating a problem to a specific area, be practical: Change or check the easy stuff first (see Figure 11.20). Time is money—to the company or person whose computer is down and to the company that employs the technician.

FIGURE 11.20 Check the easy stuff first

When multiple things could cause a problem, make a list of possibilities and eliminate the potential problems one by one. If a display is faulty, swap the display with another one before opening the computer and replacing the video adapter.

Also, check with the computer user to see whether anything about the computer has changed recently. For example, ask if anyone installed or removed something from the computer or if new software was loaded before or has been loaded since the problem started. If the problem is hardware related, you can use the Device Manager and Windows troubleshooting wizards to narrow it down to a subunit.

If you do not hear any unusual audio beeps or see any POST error codes and you suspect a software error, reboot the computer. Before Windows starts, press the F8 key to bring up the *Advanced Boot Options* menu. Select a menu option, such as *Repair Your Computer*, *Safe Mode*, or *Last Known Good Configuration*. On newer computers, it is not always easy to press the F8 key fast enough during startup to get to the Advanced Startup options. In Windows 10 or 11, access *Settings* > *Update & Security* > *Recovery* > locate the *Advanced Startup* section > click the *Restart Now* button.

Swapping a part, checking hardware settings, and referring to documentation are necessary steps in troubleshooting. Noting error or beep codes is just one element in the diagnostic routine. Determining what the problem is usually takes longer than fixing it. Software problems frequently involve reloading software applications and software drivers or getting software updates and patches from the appropriate vendor. The internet is an excellent resource for these files and vendor recommendations. Hardware problem resolution simply involves swapping the damaged part. Sometimes it is necessary to remove or disable unnecessary components and peripherals, especially in notebook computers.

If swapping a part or reloading the software does not solve the problem, go back to logical troubleshooting. Step 2 reminds you to divide the problem into hardware- and software-related issues. Go back to that step, if necessary.

Step 4. Establish a Plan of Action to Resolve the Problem and Implement the Proposed Solution

Every repair should involve a plan of action. Having a plan helps you through the problem-resolution process. The plan of action should take you through resolving the problem and implementing the solution. Refer to the vendor's support site and instructions for guidance on how to proceed.

Some repairs take multiple steps. You might have to apply a BIOS/UEFI update before installing a new adapter. You might have to update the operating system or remove a virus before reinstalling or upgrading an application. Having a plan instead of just doing things in a random order saves time—and time is money!

Step 5. Verify Full System Functionality and, If Applicable, Implement Preventive Measures

Do not assume that a single hardware component or software repair fixes a computer. The computer could have multiple problems, or one repair might not offer a complete solution. Verify full system functionality and have the user test the computer in normal conditions to ensure that the problem is indeed solved. You may need to implement preventive measures, such as cleaning the computer or device or installing a legal copy of antivirus/anti-malware software and making sure that software is updated. Preventive measures also include using disk maintenance utilities to clean up the hard drive, cleaning the optical drive laser lens, scheduling disk maintenance, and creating a recovery image.

Step 6. Document the Findings, Actions, and Outcomes

Many technicians feel that their work is done once a problem is solved, but it is not. It is important to document the steps taken to resolve a problem in a clear, concise manner. A lot of times, this documentation is put in a customer's record, or an invoice is generated as a result of a repair. Having easy-to-read and easy-to-understand documentation is important for nontechnical users who see this documentation as well as for any follow-up repairs that you or another technician must do. The old adage that a job is not done until the paperwork is done is still true, even though the paperwork is now usually electronic documentation (see Figure 11.21). Documentation remains an important last step.

The best computer technicians can repair problems, build trust with users, and explain problems in a way customers can understand. A repair is not finished until the user is informed. Technical training on new equipment or a procedure/process may be necessary. Realize that computer users are intelligent even if they are not proficient in technical terminology.

A good recommendation is to follow up with a customer a week after a repair to make sure the customer is satisfied and verify that the problem is solved. If the customer is unhappy, jump at the chance to redo the repair. The best advertising is good referrals from satisfied customers. Keep in mind that the general rule of thumb is that if a customer is satisfied, they will tell 1 or 2 other people about the service, but if a customer is dissatisfied, they will tell 10 other people about the problem.

Each computer repair is a different scenario because of the plethora of vendors, products, and standards in the marketplace. But this is part of what makes a technician's job so interesting and challenging. Break down each problem into manageable tasks, isolate the specific issue, and use all available resources—including other technicians, documentation, and the internet—to solve a problem. Maintain a "can do" attitude with intermittent problems, which are the most difficult-to-solve types of problems. Don't forget to tell the user what was done to solve a problem.

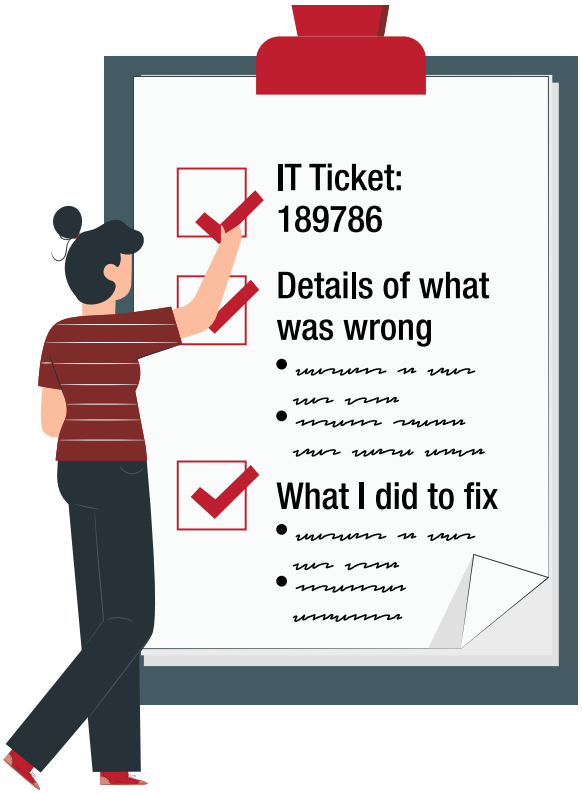


FIGURE 11.21 Document the findings, actions, and outcomes

Sample Troubleshooting Flowcharts

Technical documentation commonly includes troubleshooting flowcharts. Learning how to read and use them is helpful. Figure 11.22 shows a flowchart that does not have any words in it. The symbols in the sample flowchart are as follows:

- The powder blue and dark orange rectangles with rounded edges are terminal blocks that show where to start or where to end. Not all flowcharts have these blocks.
- The lime green parallelogram shows input or output, which could be generating a report or receiving some type of diagnostic data.
- The yellow rectangle is the most common shape you will see in a flowchart. It shows an action to take, a task to do, or an operation to perform.
- The purple diamond is a decision box. Which direction you take out of the decision box depends on what happens. Notice in Figure 11.22 that there are three results that could occur from the decision box. If they were Yes, No, and Not applicable, and whatever you did resulted in the question posed in the purple box having an answer of yes, the left output from the purple decision box could lead to another action box, labeled Yes. If the answer were not applicable and the bottom of the purple decision box were labeled N/A, then you would terminate and be done (drop to the orange terminal block). If the answer out of the purple decision box were no and the right side of the decision box were labeled No, you would do the action listed in the blue action box on the right

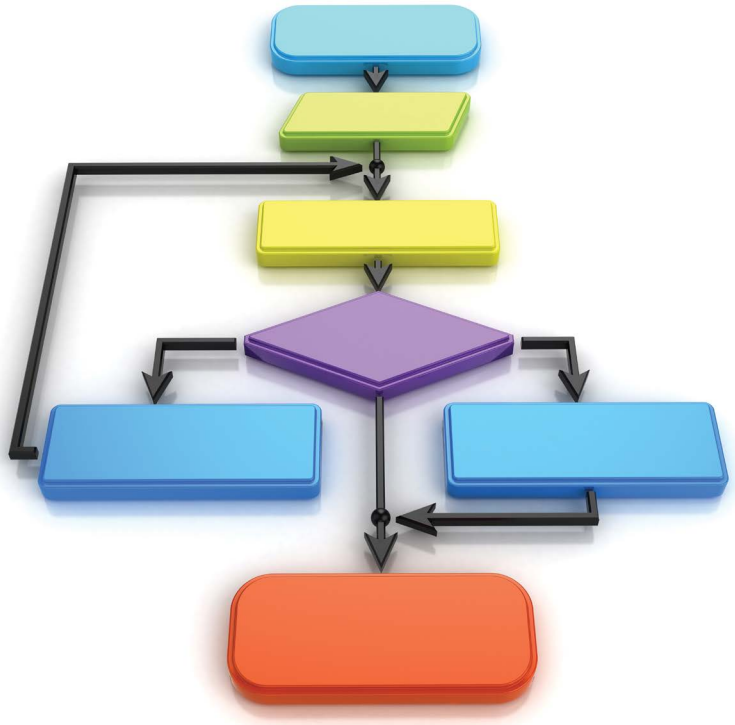


FIGURE 11.22 Sample flowchart

Figure 11.23 shows a simple troubleshooting flowchart, and Figure 11.24 shows a USB troubleshooting flowchart.

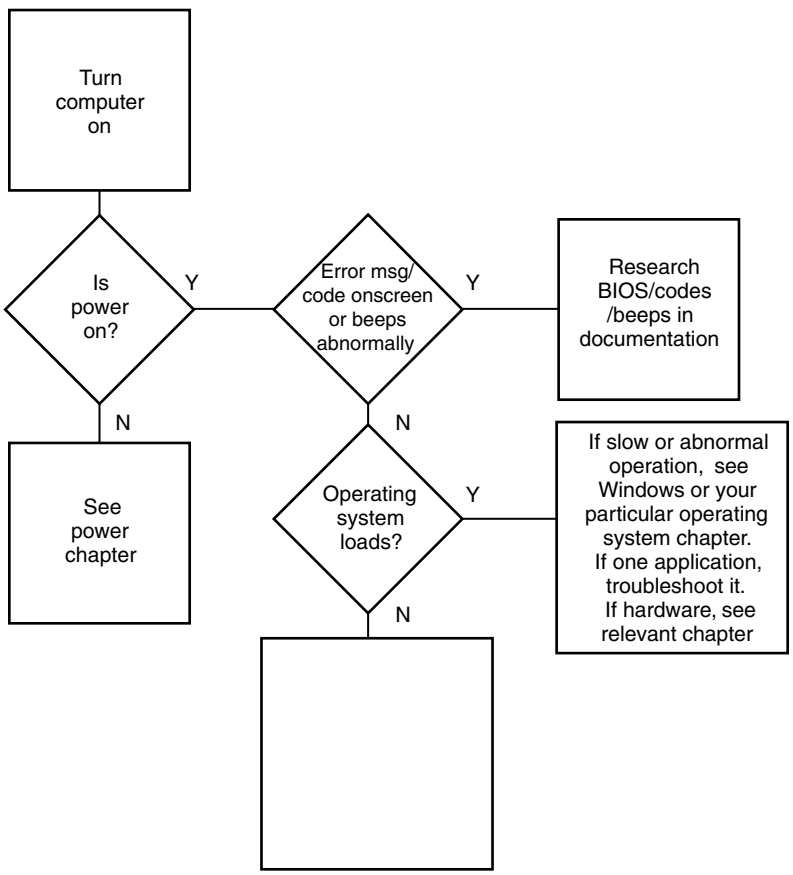


FIGURE 11.23 Basic troubleshooting flowchart

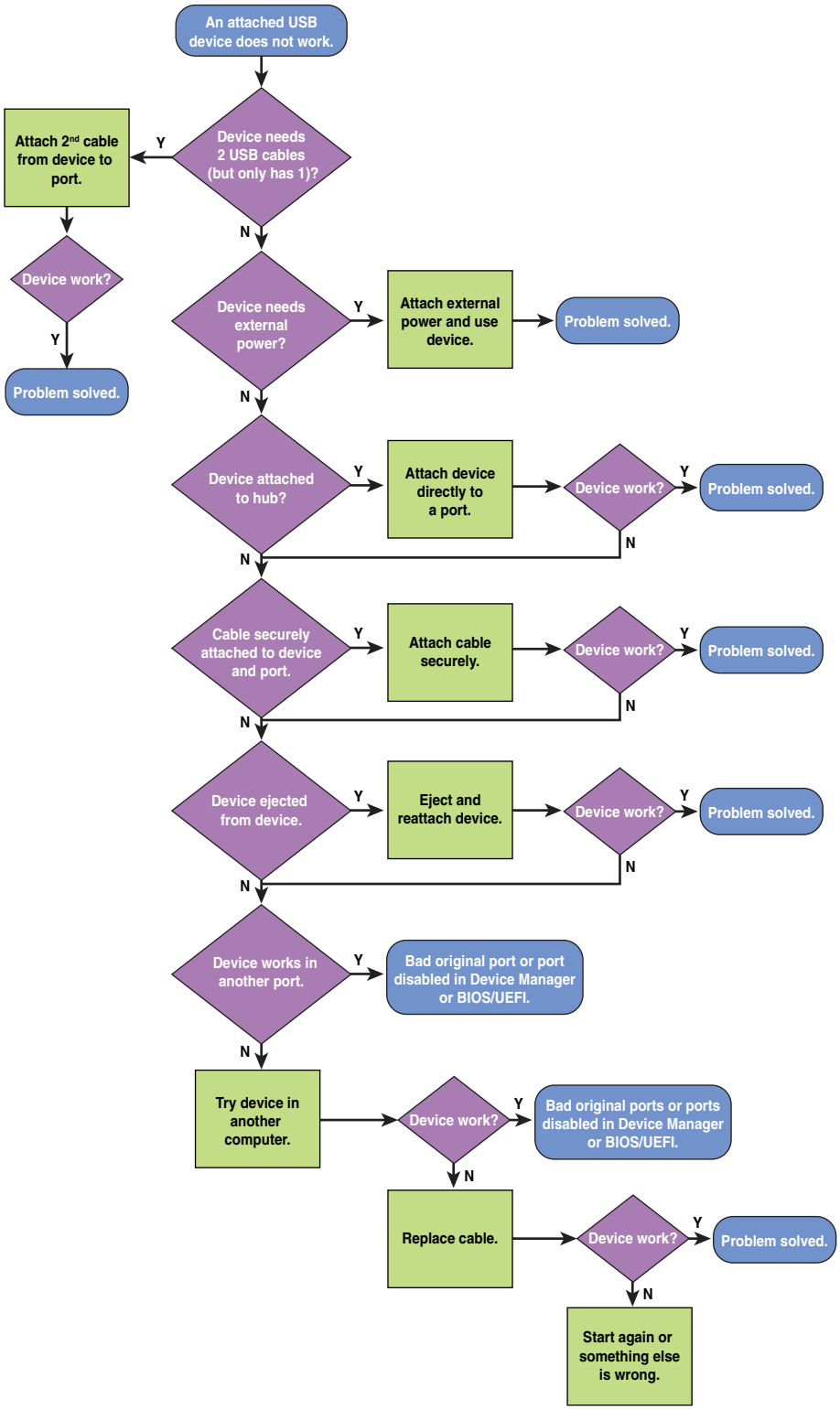


FIGURE 11.24 USB troubleshooting flowchart

Keep in mind that each chapter of this book has one or more troubleshooting sections to help with problems. In addition, the chapters toward the end of this book address problems related to operating systems. Review the troubleshooting sections of the CompTIA A+ 220-1201 certification exam objectives and review each chapter's troubleshooting sections before taking the exam.

SOFT SKILLS: DEALING WITH DIFFICULT CUSTOMERS

One of the most difficult tasks a technician faces is dealing with people who are angry, upset, or frustrated. This is a common issue for those who come to help or try to troubleshoot a problem over the phone. Dealing with irate customers is a skill that you can fine-tune. Listening to peer technicians tell how they have successfully (or unsuccessfully) dealt with difficult customers can also help. Realize that not only do customers want their computer problems fixed, they sometimes need to vent and be heard. Because a technician is the person with the knowledge for at least the start of the resolution and the technician is in front of or on the phone with the person who is not able to do something on the computer, the technician may be a scapegoat and must try to listen to the irritated customer. Some key tips for dealing with customers are shown in Figure 11.25.

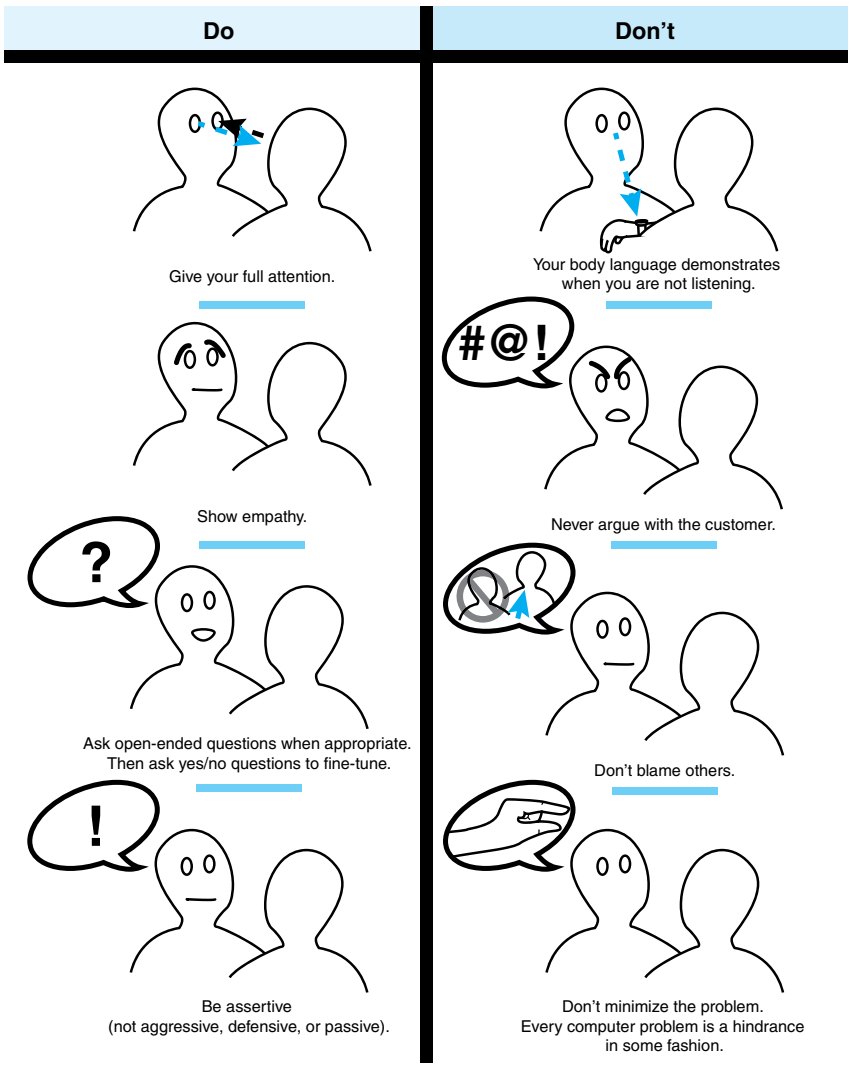


FIGURE 11.25 Dealing with irate customers

The last suggestion in Figure 11.25 about being assertive is one that many people do not understand. Aggression involves dominating a conversation or situation by threatening, bullying, being sarcastic, or showing belittling behavior and/or actions. Some technicians consistently demonstrate aggressive behavior. This reflects poorly on the technician and the company that the technician represents. Passive behavior involves letting others dominate you and expressing yourself apologetically. Technicians who are passive frequently apologize while the customer is trying to explain the problem. Assertive

behavior involves being respectful of another person but not allowing them to take advantage or dominate the situation. This is the middle ground you want to strive for when dealing with customers. It would be appropriate to raise a hand to indicate that you want an irate customer to stop what they are doing (see Figure 11.26). This would be an assertive way to show that their current behavior is inappropriate.

FIGURE 11.26 Being assertive with an irate customer

When dealing with an irate customer, you want to stay calm and maintain your professionalism. Once the customer has calmed down a bit, you can glean more information about the problem with less anger mixed into the conversation. Dealing with angry customers is an important part of a technician's job, as it is for anyone else who works in a service industry. Consider customers' points of view and don't forget that they are the ones who must use the devices that you repair.

Chapter Summary

- A graphic/CAD/CAM design workstation needs multiple powerful multicore processors, maximum RAM, a high-end video card with maximum RAM and GPU, a large display/multiple displays, a large-capacity hard drive(s), an SSD, and a good input device(s).
- A gaming PC needs an SSD, a large amount of RAM, a high-definition sound card and speakers, additional system (high-end) cooling, a large display and/or multiple displays, high-end video/specialized GPU, and good input/output devices.
- An audio- or video-editing workstation needs powerful multicore processors, maximum RAM, a good video card with maximum RAM and GPU, a specialized sound card, a fast and large-capacity hard drive, dual monitors, and good input device(s).
- A virtualization workstation needs maximum multicore processors, maximum RAM, multiple fast hard drives, an SSD, and at least a 1 Gb/s NIC.
- A thick client computer supports desktop applications and meets recommended requirements for the selected OS.
- A thin client computer supports basic applications and meets minimum requirements for the selected OS. A thin client must also have network connectivity.
- A network-attached storage (NAS) device can be used for media streaming and file sharing. It should include a gigabit NIC, a RAID array, and a large hard drive.
- A home server PC has a medium to large case, multiple powerful multicore processors, lots of RAM, RAID, a 1 Gb/s NIC, and server applications such as media streaming, file sharing, and print sharing applications.
- When designing a motherboard, the CPU size and motherboard CPU socket must match.
- The power supply, motherboard, and case form factors must match.

- A power supply must have the correct wattage for a specific power level and an appropriate number/type of power cables.
- Display design should include considerations about physical space; type of display; features that might be integrated into the display (such as a microphone or camera), video port, and memory; GPU; and additional power requirements.
- The six steps of troubleshooting are as follows: (1) identify the problem, (2) establish a theory, (3) test the theory, (4) establish a plan of action, (5) verify full system functionality and, if applicable, implement preventive measures, and (6) document the findings, actions, and outcomes and provide feedback.
- The BIOS/UEFI controls the boot process. Knowing the traditional BIOS steps can help with the troubleshooting process.
- Like a traditional BIOS, the UEFI checks the hardware, but the UEFI boot manager can load drivers that allow devices such as the mouse and NIC to be used with UEFI applications.
- POST codes or motherboard LEDs give you clues in troubleshooting an issue.
- The BIOS/UEFI can contain advanced diagnostics.
- Reinstall parts if replacing them does not solve a problem.
- Document a problem as part of the troubleshooting process. Give the user the appropriate documentation. Be professional in your oral and written communication. Tell the user what was done to solve the problem.

A+ CERTIFICATION EXAM TIPS

- ✓ Know that to test a port or a connection such as connectivity to the internet, a fiber connection, or an RJ45 port, you could use a loopback plug.
- ✓ For troubleshooting motherboards, RAM, CPU, and power, know what to do when these symptoms appear: POST beeps, proprietary crash screens, blank screen, no power, sluggish performance, overheating, burning smell, random shutdown, application crashes, unusual noise, capacitor swelling, and inaccurate system date/time.
- ✓ Focus on display/projector, storage device, and RAID symptoms: incorrect input source, physical cabling issues, burnt-out bulb, fuzzy image, display burn-in, dead pixels, flashing screen, incorrect color, audio issues, dim image, intermittent projector shutdown, sizing issues, distorted image, LED status indicators, grinding noises, clicking sounds, bootable device not found, data loss/corruption, RAID failure, S.M.A.R.T. failure, extended read/write times, IOPS, missing drives in the OS, missing array, and audible alarms.
- ✓ If you know any technicians, ask them to tell you about the problems they have solved this week. Another idea is to get them to tell you about a problem and see if you can guess the top things that could cause that problem.
- ✓ Review the section "Soft Skills: Dealing with Irate Customers" for communication skills best practices. The communication questions can sometimes have answers that are very similar. Use the review questions at the end of the chapter to help practice with those types of questions.
- ✓ The 220-1202 exam focuses on very specific criteria for proper communication and professionalism, including difficult customers and situations. Avoid arguing with a customer and/or being defensive. Do not minimize the customer's problem. Avoid being judgmental. Clarify customer statements by asking open-ended questions (which allow the customer to freely explain the situation) to narrow the scope of the problem and by restating the issue or question to verify your understanding. Do not disclose work-related experiences via social media.

Key Terms

audio/video editing workstation, back up data, BSOD, ENERGY STAR, EPEAT rating system, error message, gaming PC, graphic/CAD/CAM design workstation, home server, IOPS, loopback plug, NAS, patch, pinwheel, POST card, proprietary crash screen, random device failure, service pack, service release, thick client, thin client, virtual machine, virtualization workstation, warm boot

Review Questions

1. _____ executes POST. [BIOS/UEFI | CMOS | NAS | RAM]

2. Which of these is most likely to require dual monitors as part of the configuration?

   [virtual computer | home server | audio/video editing workstation | NAS]

3. A person comes into a computer store wanting a custom-built computer. The customer will be using the computer to stream and save videos; to video chat with remote family; and for standard computer tasks such as using a word processing program, using spreadsheets, and browsing the internet. In addition, a child will use the computer to play games. Which computer component will the technician focus on to satisfy this customer?

   [500 GB hard drive | RAID array | multicore processor | 10G NIC]

4. Before making any changes to a computer that has a problem, what is the first thing you should do?

   a. Inform your supervisor of the steps you are taking.

   b. Back up any data that is stored locally on the computer that is not backed up elsewhere.

   c. Inform the user of any possibilities that might be causing the problem.

   d. Use a loopback plug to run diagnostics.

5. Which of the following would most likely be a design consideration for a gaming PC rather than for a computer used for virtualization?

   a. high amount of RAM

   b. NAS

   c. multiple fast, large-capacity hard drives

   d. additional system cooling

6. If a computer beeps once during POST, what does this commonly mean to a technician?

   a. There is not a problem.

   b. A CPU register test is occurring.

   c. A DRAM refresh is occurring.

   d. A video initialization error has occurred.

7. An adapter or a USB device that performs diagnostics and displays a code or illuminates LEDs is known as a _____.

   [DIGI card | probe | torx | POST card]

8–10. Group the following computer components into three design subsystems. In other words, group the components that need to be considered together when designing a subsystem of a computer. Each group must include at least two components. All components are used.

power supply	CPU	chipset
video card	case	CPU cooling
motherboard	display	RAM

Group 1 components: _____

Group 2 components: _____

Group 3 components: _____

_____

_____

_____

_____

11. A motherboard advertisement lists UEFI as one of the motherboard features. What is UEFI?
    - **a.** a port
    - **b.** a BIOS replacement
    - **c.** an internal interface
    - **d.** a type of storage device
12. Which design environments would have the largest display needs? (Choose three.)

    [CAD | gaming | audio/video editing | virtualization | thick client | home server]
13. Which type of computer design would be implemented if a workstation ran both Linux and Windows as operating systems?

    [CAD | home theater | virtualization | thin client | thick client]
14. When designing a tower computer, with what computer component would you consider physical space more than any other part?

    [hard drive | motherboard | display | CPU | power supply | air filter]
15. Which components could have an ATX form factor? (Choose two.)

    [hard drive | motherboard | display | CPU | power supply | air filter]
16. Place the six steps of troubleshooting in the order in which they occur.

    ____ Step 1 **a.** Test the theory to determine cause.

    ____ Step 2 **b.** Establish a theory of probable cause.

    ____ Step 3 **c.** Document and provide feedback.

    ____ Step 4 **d.** Identify the problem.

    ____ Step 5 **e.** Verify system functionality and, if applicable, implement preventive measures.

    ____ Step 6 **f.** Establish a plan of action to resolve the problem and implement the solution.
17. [T | F] During the *troubleshooting* phase in which you test the theory, you might be required to escalate the problem to a more experienced technician.
18. A _____ is used to test a communications circuit or RJ45 port.

    [multimeter | probe | torx | loopback plug]
19. Which computer design environment would have the most need for a digital tablet?

    [audio/video editing workstation | gaming | virtualization | mobile | home server]
20. [T | F] When dealing with an irate customer, it is best to listen to the customer vent.

Exercises

Exercise 11.1 Recommending Computer System Design

Objective: To be able to recommend a complete system based on the customer's needs or placement of the system

Parts: Computer with internet access

Procedure: Use the internet to research specific computers, based on each scenario.

1. A homebound elderly person has just had her hard drive fail. The drive was installed in a really old computer, and the person has decided to replace the computer rather than fix the broken one. The elderly person uses the computer to shop for family members, check email, play basic computer card games with others online, and view pictures on CDs or DVDs sent by family members. Internet access

is through a DSL modem that connects to the USB port and still works. Find a suitable computer on the internet. The customer would like to keep the cost around $700, including installation, if possible. Write the computer model, basic description, cost, and cost of installation.

_____

_____

_____

2. A graphic artist would like a second computer as a mobile solution and would like your assistance finding a suitable laptop. The artist does mostly video graphics creation but would like to be able to work while traveling. Find three possible solutions. Provide the computer model, basic description, and costs of the three laptops.

_____

_____

_____

_____

_____

_____

3. A sports complex wants to have a kiosk with a touch screen that holds a computer that runs specialized software to allow people to search for events and get detailed walking directions to the events and/or specific sports fields. No network connectivity is required. Locate a computer with an HDMI output for connectivity with the touch screen for this outdoor kiosk located in a year-round sports complex. List the model number, basic description, and your fee for installing this system.

_____

_____

4. A 10-person purchasing department is going to a thin client environment. Select one desktop thin client computer model and one mobile thin client model from different manufacturers that can be used in the department. The models need to support dual displays. Detail any model numbers, basic parts descriptions, and costs.

_____

_____

_____

_____

_____

_____

_____

_____

5. A small company is expanding and is hiring an administrative assistant for the sales manager. Select a computer, monitor, keyboard, and an inkjet all-in-one printer for this assistant, who will be using Microsoft Office–type applications. The boss has put a $1,300 limit (not counting shipping) on the entire purchase. Provide a detailed list, description, and costs of parts chosen.

_____

_____

_____

_____

_____

6. Select a CAD/CAM manufacturing design computer that uses 64-bit AutoCAD LT 2022 software. Research the AutoCAD LT application's video requirements. Provide a detailed list, description, and cost of parts chosen, including the video card and display. Assume that there is no price limit. (Note that AutoCAD LT requires a 1,920×1,080 display with True Color.)

_____

_____

_____

_____

_____

7. You have an unlimited budget to build the best gaming rig possible. Choose two PC manufacturer sites where you can select components, monitors, applications, and accessories for your new system.

_____

_____

_____

_____

8. You have an unlimited budget and need to build two systems from scratch. You will need cases, power supplies, motherboards, CPUs, RAM, hard drives, video cards, and more. List two websites where you can compare and buy all the components you need to build the two systems.

_____

_____

Exercise 11.2 Understanding Design Components

Objective: To be able to recognize the unique components for a specific computer design scenario

Procedure: Using the list of components, identify which components would be used in each of the scenarios. Note that any one component can be used multiple times.

Components

a. Multiple powerful processor cores
b. Maximum RAM
c. Lots of RAM
d. Multiple large-capacity hard drives
e. Large-capacity hard drive
f. RAID
g. Sound card and speakers
h. Powerful video card and RAM on the card
i. Multiple displays
j. Large display
k. DVR
l. TV tuner or cable card
m. 1 Gb/s NIC
n. Computer enclosure
o. KVM switch
p. SSD

Scenario 1

Identify the unique components from the provided list for a computer used for audio and video editing.

_____

_____

Scenario 2

You need to build a computer to test the Chrome operating system, along with your current Windows operating system. You have decided to do this in a virtual environment. Identify the unique components that would be in the computer.

_____

_____

Scenario 3

A customer wants to try out thin client workstations in one department. Identify one or more unique components that would be in one computer of this type.

_____

_____

_____

_____

_____

Scenario 4

A tire shop would like to have a computer in the lobby that displays information about the latest promotions and upcoming sales. The owner is concerned about theft. What unique component would be needed for this situation?

_____

Scenario 5

A computer programmer works from home but likes to work from several types of computers—a mobile tablet, a laptop, and a desktop—and wants to be able to work on any mobile device when traveling. The programmer has decided to create a server to store and access everything from anyplace. The programmer does not want to have to buy another keyboard, mouse, or display for the server but wants to share these components connected to the desktop computer with the server. What unique components would be part of this system?

_____

Exercise 11.3 Understanding Subsystem Design Components

Objective: To be able to design a subsystem of a computer, based on design requirements

Parts: Computer with internet access

Procedure: Use the internet to research specific computers for the scenarios.

Scenario 1

You have just ascertained that a customer's older microATX Core i3 motherboard in a home computer is bad. The customer wants a motherboard upgrade or replacement. The existing motherboard has a PCIe sound card and DVI port that the user would like to continue using. The RAM on the existing motherboard is 4 GB of DDR3 memory. The hard drive and optical drive use SATA for connectivity, and the customer would like to continue using these devices and the current operating system. The customer does light computer work but likes listening to broadcasts and music on the computer. Locate suitable replacement upgraded components. The budget is $250, including labor. Detail each item, item description, and cost.

_____

_____

_____

_____

_____

Scenario 2

A customer has been given a microATX motherboard, an Intel Core i5 quad-core processor, and RAM. The customer has two 3.5-inch SATA drives and would like to have an NVMe SSD in the future. The customer would like assistance getting a case and a power supply to handle all these devices. The customer does not have a lot of room but wants a tower case that provides good airflow through the computer. The customer has a budget of $200 for this. Locate a power supply and case for the customer. Detail the items, item descriptions, and costs.

_____

_____

_____

Scenario 3

A retired naval officer has just gotten into classical music and now wants surround-sound in his office. Select an appropriate sound subsystem. The budget is $250. The office system has both PCI and PCIe expansion slots available. List the components, a description of each component, and the cost.

_____

_____

_____

Scenario 4

A college graduate has started her own website design business. She wants a video card that supports two 20- to 24-inch displays. Recommend a video subsystem for her. The budget is $500 maximum. List the components, a description of each component, and the costs.

_____

_____

_____

_____

Scenario 5

Locate a motherboard, power supply, RAM, CPU, and midsized case that are compatible with one another for a work-from-home administrative assistant who does a small amount of gaming during off hours. The budget is $650. List the components, a description of the components (ensure that you list the type of RAM the motherboard supports), and the costs.

_____

_____

_____

_____

_____

_____

_____

_____

Exercise 11.4 Determining the Troubleshooting Process Step

Objective: To be able to determine which step of the troubleshooting process is occurring

Procedure: Match one of the six troubleshooting steps to the situation. Note that a particular step may be the answer for more than one situation.

Troubleshooting steps:

a. Identify the problem.

b. Establish a theory of probable cause.

c. Test the theory.

d. Establish a plan of action.

e. Verify full functionality.

f. Document findings.

Situation:

____ A USB flash drive is not being recognized in a computer. You move the drive to a different USB slot.

____ You provide the user with the registration/authentication code for the antivirus software that was installed in the computer after a virus was removed.

____ You ask open-ended questions.

____ The user explains what has happened in the past few days that was unusual.

____ You phone the user to ask if the system appears to be running faster since the new memory module was installed.

____ You order a new motherboard.

____ You re-enable automatic Windows updates so they get applied in the future and prevent future issues.

____ You believe that the problem is either the motherboard or the processor.

Activities

Internet Discovery

Objective: To become familiar with researching computer items used in designing systems or subsystems

Parts: Computer with internet access

Procedure: Use the internet to answer the following questions. Write the answers and the URL of the site where you found the information.

1. Locate the Bloom's Taxonomy chart that has been modified by Andrew Churches to include verbs for the digital age. Write at least five verbs that Andrew Churches recommends as being relative to the top level of the taxonomy—the creating level—and the URL where you found the chart.

   _____

   _____

   _____

   _____

2. Locate minimum requirements for either a student computer or a staff computer at a particular school.

Write the requirements, the school name, and the URL where you found this information.

3. What are the recommended video standards for use when playing the Pacific Drive game on a PC? Write the answer and the URL where you found this information. Then find a video card that meets those specifications. Document the video card and the price.

4. What are the minimum processor, RAM, and display resolution requirements for a client who wants to run AutoCAD 2025 software? Write the answer and the URL where you found the information.

5. Find a monitor that supports the minimum AutoCAD 2025 display resolution found for Question 4. List the monitor manufacturer, model number, and URL where you found the information.

6. Locate a website that has a troubleshooting flowchart. Write three things the flowchart provides that you find helpful or confusing. Write the URL where the chart was found.

7. Locate one website that lists at least two BIOS/UEFI error codes. Write the URL where this information was found.

8. Find a website that shows at least three recommendations for dealing with irate customers. Write three recommendations and the URL where you found this information.

_____

_____

_____

_____

Soft Skills

Objective: To become familiar with researching computer items used in designing systems or subsystems and to learn how to deal with difficult customers or situations

Activities:

1. Interview or email someone who works in your school to determine the school's minimum hardware requirements for its new computers. Document your findings.

_____

2. In teams of two, find a video that shows how to deal with an irate customer. Document at least three observations from the video as well as the video URL.

_____

_____

_____

3. In teams of two, three, or four, design a computer for a specific purpose. State the purpose and provide all the models, descriptions, and costs. Compete with other teams for the best design.

_____

Critical Thinking Skills

Objective: To become familiar with researching computer items used in designing systems or subsystems

Activities:

1. Refer to Tables 11.1 through 11.4, which provide recommendations for hardware components. Find at least one type of computer configuration for which you disagree with the special hardware components; if you agree with them all, then think of one that should be added. List the component and the reason for your disagreement or addition.

_____

_____

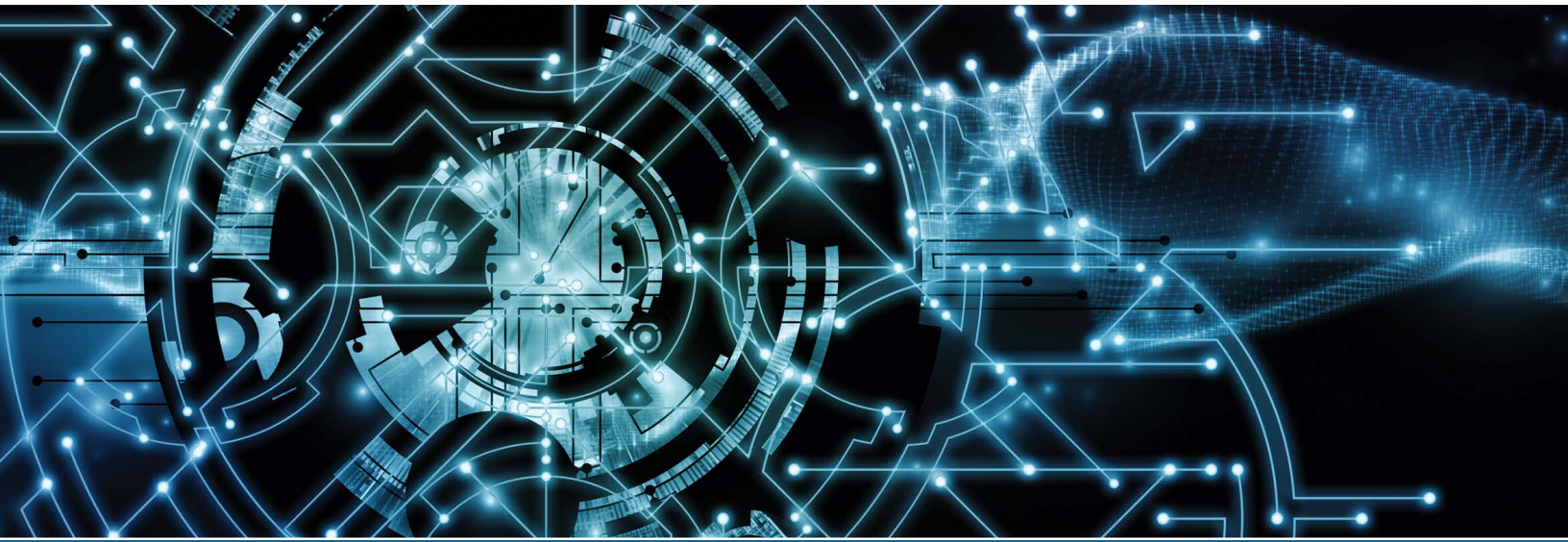
2. Locate an image that shows a map of Bloom's Taxonomy, as modified by Andrew Churches. Explain why designing (in the creating stage) requires higher-level skills than working in the evaluating stage, which includes experimenting, judging, monitoring, and testing.

_____

3. Do you think most technicians are good at designing computers for specific purposes? Explain your opinion.

_____

12 Internet Connectivity, Virtualization, and Cloud Technologies



In this chapter you will learn:

- To describe dial-up networking
- About other internet connectivity options, such as satellite, cable, DSL, and fiber, as well as wireless options such as cellular, long-range fixed wireless, Wi-Fi, and wireless broadband
- To configure a browser and other basic issues related to a browser
- How cloud computing is used for personal and corporate purposes
- Terms associated with cloud computing
- The basics of virtualization, including terms and features associated with it
- The benefits of mentoring in the IT field

CompTIA Exam Objectives:

- ✓ 1201-2.2 Explain wireless networking technologies.
- ✓ 1201-2.5 Compare and contrast common networking hardware devices.
- ✓ 1201-2.7 Compare and contrast internet connection types, network types, and their characteristics.
- ✓ 1201-3.2 Summarize basic cable types and their connectors, features, and purposes.
- ✓ 1201-4.1 Explain virtualization concepts.
- ✓ 1201-4.2 Summarize cloud computing concepts.
- ✓ 1201-5.5 Given a scenario, troubleshoot network issues.
- ✓ 1202-2.11 Given a scenario, configure relevant security settings in a browser.
- ✓ 1202-3.4 Given a scenario, troubleshoot common personal computer (PC) security issues.

Internet Connectivity Overview

Connecting to the internet can be done in a variety of ways: wirelessly or via analog modem, fixed wireless, cable modem, DSL modem, satellite modem, fiber, power line, or cellular network. These technologies have unique installation and configuration methods, but they all have in common the capability to connect a computer to an outside network. Each technology is a viable option for connectivity in a specific situation. By examining and understanding the technologies, you can offer customers connectivity options. More information about troubleshooting network connectivity is provided in Chapter 13, "Networking." Let's start with the oldest method: analog modems.

Dial-up Connectivity

One of the first devices still in operation that was used to connect to the internet is the modem. A modem (which stands for *modulator/demodulator*) connects a computer with the outside world through a phone line. This type of technology is frequently called a **dial-up network** or just dial-up because the analog modem uses the phone line to "dial up," or call, another modem. Modems can be internal or external peripheral devices. An internal modem is an adapter installed in an expansion slot. An external modem attaches to a USB port. A modem converts a signal transmitted over the phone line to digital 1s and 0s to be read by the computer. It also converts the digital 1s and 0s from the computer and modulates them onto the carrier signal and sends the data over the phone line. A modem normally connects to a remote modem through a phone line. Figure 12.1 shows two modems connecting two computers.

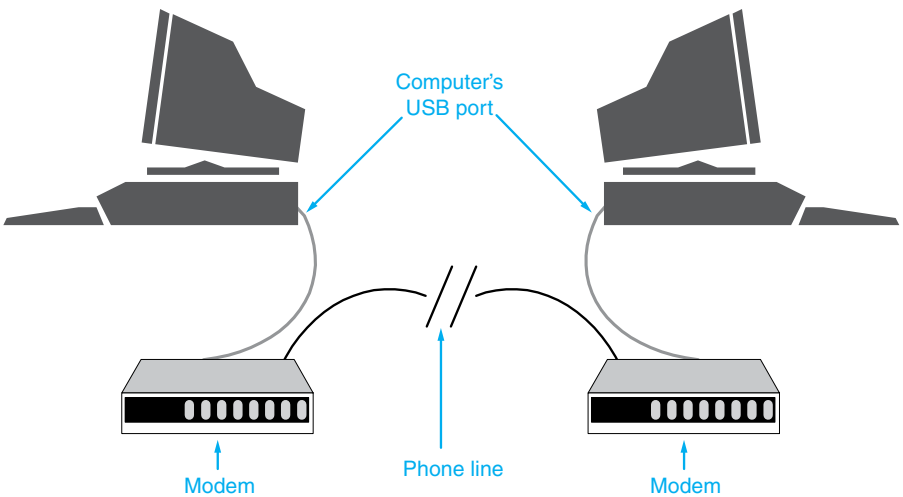


FIGURE 12.1 Sample modem connection

TECH TIP

When connecting a modem to a phone line, be careful with the cabling

Some modems have two jacks on the back. The labeling varies, but one jack is usually labeled PHONE and the other LINE. The LINE jack is for the cable that goes from the modem to the phone wall jack. The modem's PHONE jack is an optional jack that connects a telephone to the modem. Figure 12.2 shows the ports on an internal modem.

Table 12.1 describes basic terminology associated with serial transmissions, such as transmissions that occur with a modem.

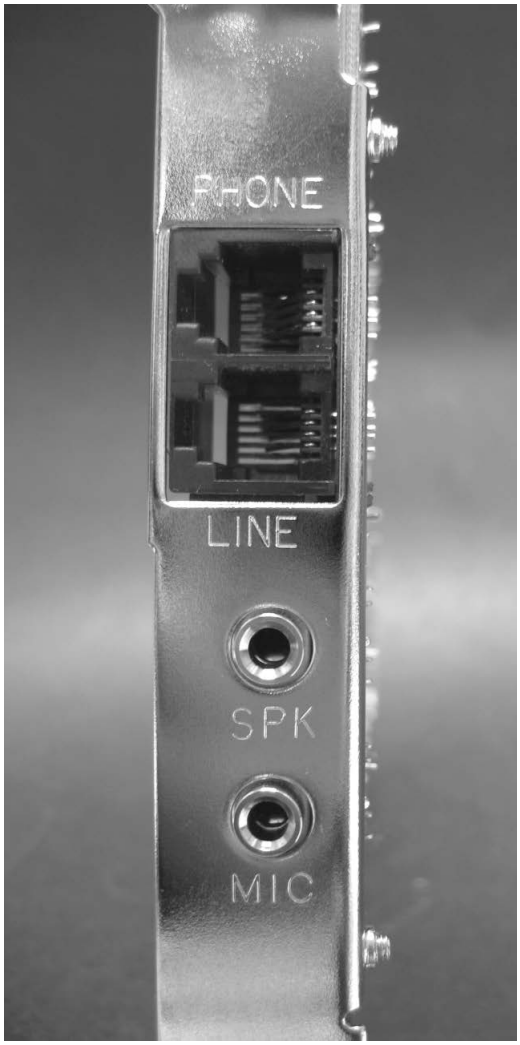


FIGURE 12.2 Internal modem ports

TABLE 12.1 Serial asynchronous transmission terminology

Term	Description
Baud	The number of times an analog signal changes in one second. Some use this term to speak of the modem speed. Modems can send several bits in one cycle, so it is more accurate to specify modem speed in bits per second (bps or b/s).
Bits per second (bps or b/s)	A measurement used to describe the transmission speed of serial devices and ports. Settings include 110, 300, 1,200, 2,400, 4,800, 9,600, 19,200, 38,400, 57,600, and 115,200.
Start/stop bit	A bit used in asynchronous transmission to signal the start or end of the data.

TECH TIP

Configuring transmission speeds

When configuring a serial port or using an application, the configured speed is the rate at which the serial port transmits. This is not the speed for an external serial device that connects to the port (such as a modem).

Serial ports and devices such as internal modems have three important configuration parameters: interrupt, input/output (I/O) address, and COM port number. An internal modem has all these parameters; an external modem uses these same parameters, but they are assigned to the serial port to which the external modem connects. Use *Device Manager* to identify these system resources. Other important settings associated with serial devices include the method of flow control they use, such as XON/XOFF (a software method) or RTS/CTS (a hardware method), the FIFO setting, and handshaking. Be sure both sides of a serial connection match.

To configure a dial-up connection using a 56 kb/ps modem, install the internal modem or connect the external modem to the computer. Ensure that the modem connects to a working phone outlet. In Windows, use the *Access Settings* > *Network & Internet* > *Dial-up* > *Set up a new connection* link unless the manufacturer's instructions say otherwise; some modems have their own installation software.

Cable Modems

One of the most popular items in the modem industry is the **cable modem**, which connects a computer to a cable TV network. Cable modems can be internal or external devices but commonly are external. If a cable modem is external, two methods commonly exist for connecting to a PC: (1) A NIC built into the motherboard is used or an adapter is installed, and a cable attaches between the NIC and the cable modem or (2) the cable modem connects to a USB port on the computer. Figure 12.3 shows the **coaxial** cable on the top for connection to the wall coax connector, both USB and RJ45 network connectors for connecting to a PC, and two additional RJ45 Ethernet network jacks for printers or additional devices.

FIGURE 12.3 Cable modem coax, USB, and Ethernet LAN ports

Cable modem operation is not hard to understand. Internet data comes in through coax cable. The coax cable plugs into the cable modem. The cable modem sends the information out its built-in Ethernet port. A network cable connects from the cable modem's Ethernet port into an Ethernet port on the computer. To send data to the internet, the reverse happens: The computer sends the data out its Ethernet port into the cable modem. The cable modem sends the data out the coax cable onto the cable TV company's network. Notice in Figure 12.3 that there are additional Ethernet ports below the yellow cable. If the cable modem needs to connect to a company or home router, one end of an Ethernet cable is attached to one of the cable modem Ethernet ports, and the other end is attached to the router.

Cable modem speeds vary by geographic location and vendor. Most people are interested in the downstream data (data coming from the internet into the home or business). Downstream speed can be from 40 Mb/s to 10 Gb/s, whereas upstream speeds are typically slower and can be in the range from 10 Mb/s to 10 Gb/s.

xDSL Modems

xDSL is another modem technology. The *x* in the term xDSL refers to the various types of digital subscriber line (**DSL**) that are on the market. The most common one is asymmetric DSL (**ADSL**), but there are many others. ADSL uses faster downstream speeds than upstream. This performance is fine for most home internet users. DSL uses traditional phone lines to send and transmit both voice and internet data. With DSL modems, bandwidth is not shared between people in the same geographic area. The bandwidth paid for is exclusive to the user. DSL is not available in all areas. The HighSpeedInternet.com website lists major DSL providers, other internet technology vendors, and geographic areas.

An internal or external DSL modem can be connected to a regular phone line. The phone line can be used for calls, faxes, and so on at the same time the modem is being used. An external modem can connect to a USB port or an Ethernet network card. Figure 12.4 shows DSL modem ports, including the DSL connector, which connects to the wall outlet and is labeled ADSL, and the multiple Ethernet LAN connections, which could be used to connect to one or more computers, printers, external network storage, or other wired network devices.

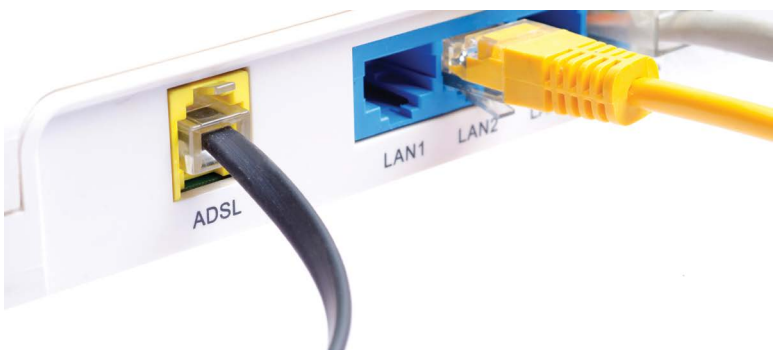


FIGURE 12.4 DSL modem ports

TECH TIP

Corporate DSL, cable, or fiber

Corporate internet connectivity can use DSL, cable, or fiber connections. Chapter 2, "Connectivity," provides more information on fiber cabling.

A drawback to DSL is that the DSL signal needs to be separated from the normal phone traffic. DSL providers typically supply **phone filters** (see Figure 12.5) that must be connected to phone outlets that have telephones, fax machines, and voice recorders attached; these filters prevent signal interference and ensure clear communication.

FIGURE 12.5 DSL phone line filter

VoIP

Traditionally, a company had separate networks for voice and data, with only computers and printers connected to the data network. Voice over IP (**VoIP**) uses a corporate data network and/or the internet for phone traffic rather than using the traditional public switched telephone network (PSTN). Free and purchased VoIP software can be used to enable a user to call someone using the internet. Figure 12.6 shows a VoIP phone that cables to a PC and into the corporate data network. Note that VoIP can also be implemented without a phone through software and using a speaker or headphones and an integrated or external microphone.

FIGURE 12.6 Corporate VoIP phone

A VoIP phone typically connects to an RJ45 data jack that is wired to a power over Ethernet (PoE) network switch that can provide power to the phone through the network cable. Most VoIP phones have a second RJ45 port so that a PC can connect directly to the phone instead of having a second RJ45 wall jack. Corporate VoIP phones commonly use PoE.

In the past, companies also used a separate network infrastructure for the video network, but that has also now been moved onto the data network. **Convergence** is a term used to describe how these data, voice, and video technologies now use one network infrastructure instead of multiple networks. Figure 12.7 shows a video conference in the corporate environment where people join using tablets, laptops, corporate conference rooms, and desktop computers. All of the data from these devices travels over the same corporate network.

FIGURE 12.7 Corporate video conference call

Some free software applications and email accounts also support video conferencing using the internet, such as Skype, Google Meet, Slack, AnyMeeting, or FaceTime. Through these applications, the quality may not be as good as with the traditional PSTN. This is because a guaranteed quality of service (**QoS**) is not provided. QoS prioritizes traffic so that important traffic—such as business transaction traffic and VoIP traffic—is sure to get through. Figure 12.8 shows this concept.

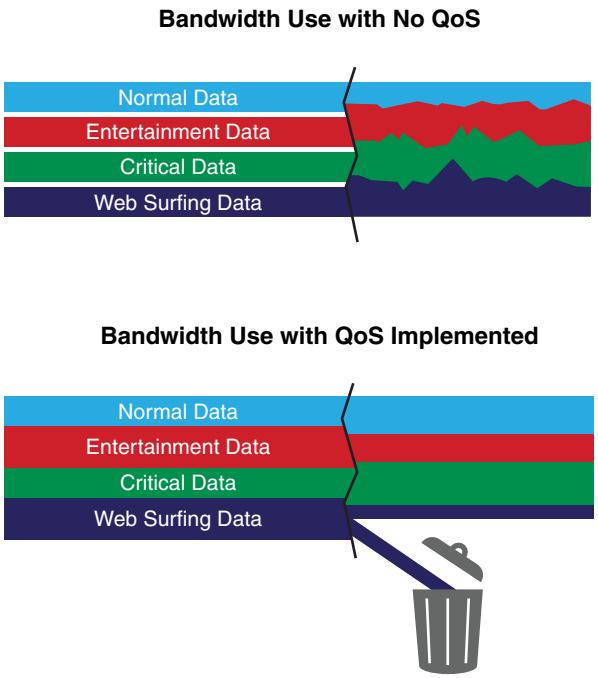


FIGURE 12.8 QoS

TECH TIP

What to do with poor VoIP quality

When QoS is not implemented or when it is not implemented properly, **poor VoIP quality** can occur (so that calls can be dropped or audio may not be clear), and the technician must report this to the network staff. Users may need help due to **jitter** and technical staff might ask that you provide jitter statistics obtained from the phone.

Figure 12.9 shows voice packets (labeled VP) going across the network in a steady stream when there is no jitter. Then it shows voice packets that are sporadically spaced and jitter occurs.

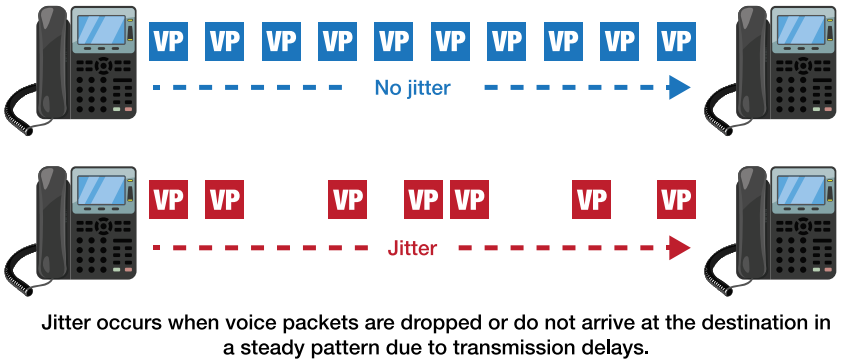


FIGURE 12.9 Jitter

In a network experiencing **latency**, packets get delayed. Latency is measured in milliseconds (ms) and can be caused by such things as too much traffic on a network, a server being overloaded with requests, long distance, or low bandwidth. Jitter is similar to latency except that it is inconsistent timing of the delivery of packets.

Technicians must be aware of VoIP for two reasons:

> A phone installed in a corporate office must be connected to the network in a similar fashion to a PC.
> A phone may be a software application (a soft phone) that has to be installed and configured on a computer.

One last thing to remember about VoIP in the corporate environment is that no corporate network can do away with the PSTN connection to the traditional phone network. A corporate environment will always need to be able to communicate with the outside world and will especially need to be able to contact emergency services such as police, fire, and emergency responders.

Fiber Networks

A high-speed **fiber network** connection is commonly used to bring bundled technologies to subscribers. Such bundles may include phone, internet, and cable TV connectivity. In a fiber network, many fiber-optic cables are used to connect buildings, multiple companies, and home users. A single fiber carries voice, data, and video using three different optical wavelengths. This same type of connectivity is offered at higher speeds to small businesses. Whereas electrical pulses flow through copper cables, light flows through a fiber-optic cable. Instead of an electrical pulse being a 1, the light being on is a 1. A 0 is the light being turned off. Figure 12.10 shows the basic components of fiber-optic cable.

Fiber-optic cable has many advantages, including security, long-distance transmission, and bandwidth. Many government agencies use fiber-optic cable because it offers high security. Unlike signals from other cable media, light signals that travel down fiber are impossible to break and intercept. Also, because light is used instead of electrical signals, fiber-optic cable is not susceptible to electromagnetic interference (EMI) or radio-frequency interference (RFI). Fiber-optic cable is the most expensive cable type, but it also handles the most data with the least amount of data loss. Figure 12.11 shows how fiber-optic cable is installed under a city street, along with electrical conduits.

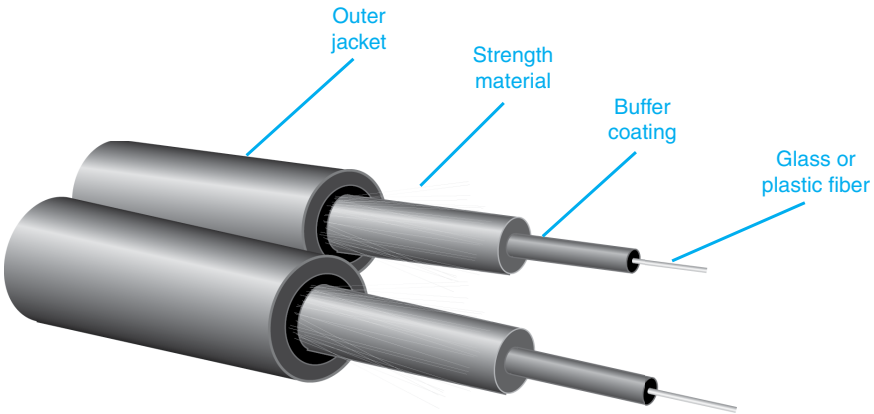


FIGURE 12.10 Fiber-optic cable

FIGURE 12.11 Laying fiber-optic cable

When a fiber connection is used, an optical network terminal (**ONT**) box is mounted on the wall that is near a wall jack near the router. This might be located in a home, basement, phone closet, or garage. The ONT converts the light taken from the fiber cable into electrical 1s and 0s transmitted into the internet modem. An Ethernet cable connects from the ONT to the port labeled broadband or ONT on a device that connects the home or business to the internet. Figure 12.12 shows an ONT box and the connection to the internet modem.

Two terms that are often associated with internet connectivity are upstream and downstream. **Upstream** refers to data sent from your home to the internet. **Downstream** refers to the data pulled from the internet into your computer, as when you download a file or view a web page (see Figure 12.13). With cable modems, downstream (download) transfer rates are faster than upstream (upload) transfers. Downstream speeds can be as high as 5 Gb/s for consumers and even higher for businesses. Upstream speeds vary; with an external cable modem, they tend to be between 384 kb/s and 35 Mb/s. Even though upstream speeds are slower, cable modems greatly improve speed over analog (dial-up) modems.

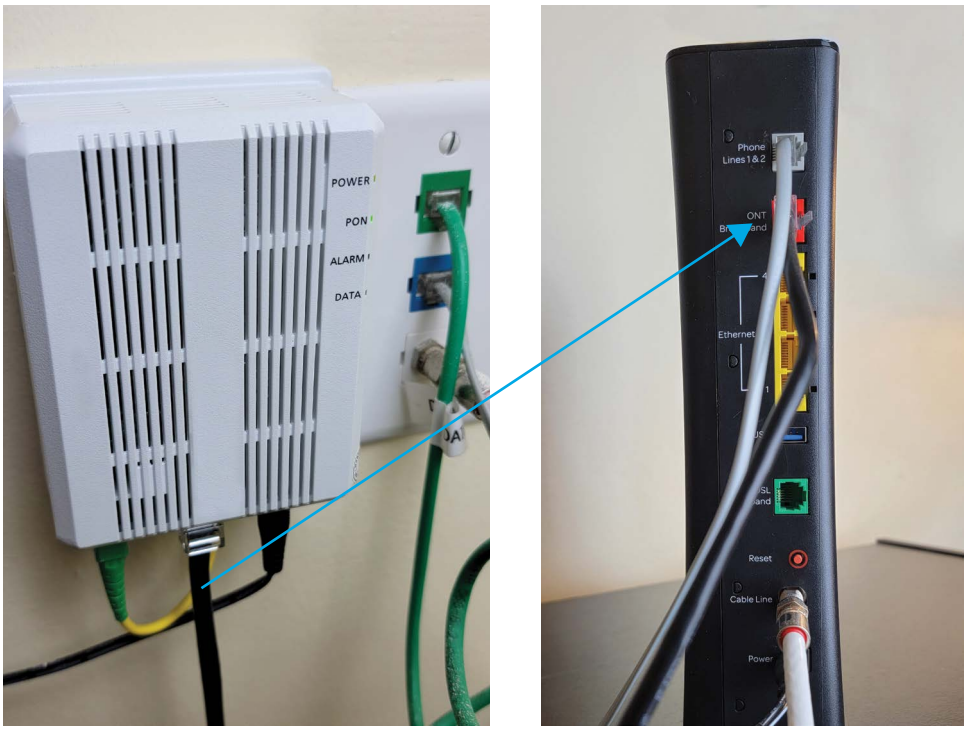


FIGURE 12.12 ONT box and connection to internet modem

Cable or ADSL Modem

FIGURE 12.13 Upstream and downstream

The speed of a cable modem connection depends on two things: the cable company and how many people in the area share the same cable TV provider. Each cable channel uses 6 MHz of the cable's bandwidth. **Bandwidth** is the capacity of the communications channel. Bandwidth is also known as *throughput*, or *line speed*. The cable company designates one of the 6 MHz channels for internet access. Several homes can use the same channel, which reduces the amount of bandwidth each house has available. If you have three neighbors who all use the same cable vendor and they are internet warriors, you will have slower access than if you were the only person in the neighborhood connected.

Satellite Modems

An option available to areas that do not have cable or DSL service is satellite connectivity, where a satellite relays communication back to receivers on Earth. Satellite connectivity requires, at a minimum, a satellite dish and a **satellite modem**. It may also require an analog modem and other

equipment, depending on the satellite provider. With a satellite connection, the data goes from the computer to the satellite dish mounted outside the home or business (see Figure 12.14) to another satellite dish (and maybe more), up to the satellite orbiting Earth, down to the internet service provider (**ISP**), and from the ISP to the website requested; the web page returns via the same path. Satellite connectivity is not as fast as cable or DSL connectivity, but it can be five to seven times faster than dial-up. The downstream speeds can be from 9 kb/s to 24 Mb/s, but they are typically around 500 kb/s. Some providers offer the same upstream speeds.

FIGURE 12.14 Satellite connectivity

With a satellite modem, TV programs accessed via the satellite can be watched at the same time that web pages are downloaded from the internet. However, drawbacks to satellite modems are important to mention:

- The initial cost of installing a satellite modem can be high.
- If other people in the area subscribe to the same satellite service, speed is decreased during peak periods.
- Initial connections have a lag time associated with them, so playing multiplayer games is not very practical.
- Virtual private networks (VPNs) are not always supported.
- Weather elements, such as high winds, rain, and snow, affect performance and connectivity.

Mobile/Cellular Connectivity Overview

Today's working environment is a mobile one with laptops, cell phones, and tablets. Connecting to the internet through an 802.11 wireless network is common, as introduced in Chapter 10, "Mobile Devices" (and discussed further in Chapter 13). Smartphones, computers, and tablets can become **mobile hotspots**. Using a connection such as a USB port, Bluetooth wireless connectivity, or the cellular network, a device can provide wireless internet connectivity to others in the immediate vicinity. Some cell service providers offer this option as part of a cellular plan. The term *mobile hotspot* is also used to refer to an area of wireless connectivity (normally free), such as in a park, coffee shop, or museum. Another way of getting onto the internet is through the use of tethering. **Tethering** refers to sharing an internet connection with other mobile devices in the nearby area wirelessly through Bluetooth or Wi-Fi or through a wired USB connection.

Cellular Connectivity

Mobile devices use the cellular network to connect to the internet. Table 12.2 recaps the different cellular network types.

TABLE 12.2 Cellular network types

Cellular network type	Features
3G	Speeds of 200 kb/s up to 2 Mb/s
4G	Speeds up to 1 Gb/s to support gaming, mobile TV, and video conferencing
LTE (Long Term Evolution)	An optimized version of 4G for video streaming and gaming
5G	Slated to support speeds up to 20 Gb/s. 5G is used in corporate connectivity and Internet of Things (IoT) networks. Drones and balloons can be used in emergency situations to provide 5G connectivity.

Wireless Broadband

An increasingly popular feature with laptops and tablets is **wireless broadband**, with download speeds up to 1 Gb/s (but more commonly between 25 and 50 Mb/s). This technology is sometimes referred to as wireless WAN, mobile broadband, or cellular WAN. Cell phone companies and internet providers offer USB modems, broadband boxes, mobile data cards, and integrated laptop connectivity to enable users to receive, create, and communicate internet information within a coverage area. For people who travel a lot, this option allows for connectivity in places where data connectivity has not previously been feasible. Mobile wireless broadband allows wireless connectivity and hotspot connectivity for devices anywhere you have cell coverage.

TECH TIP

Laptop wireless WAN connectivity

A laptop that ships with integrated wireless WAN capabilities does not need an additional adapter or antenna. However, the BIOS/UEFI must have the option enabled. Some laptops might have a key combination or a switch to enable the connection. The wireless application software is available through the *Start* button.

Long-Range Fixed Wireless

Fixed wireless is a very good internet connectivity solution for states with lots of rural areas, such as Vermont and Kansas. Fixed wireless, which is different from satellite, cellular, or Wi-Fi coverage, has been around for some time. **Long-range fixed wireless** can be used to connect buildings with one another, so that homes and businesses in remote areas can connect to the internet (see Figure 12.15).

Fixed wireless is a more viable option for wireless internet service providers (**WISPs**) due to some changes in the wireless and communications standards. Compared to an unlicensed range, a **licensed range** of wireless spectrum frequencies provides better performance, reliability, and reduced interference from other devices. It also allows larger chunks of data to be transmitted. In the United States, the wireless spectrum is managed by the Federal Communications Commission (FCC), which assigns specific frequencies for a system or a range of frequencies for a particular

service on a first-come, first-served basis in a geographic area. The geographic area is different for different industries; it may be an economic area, a cellular area, a basic trading area, and so on. There are auctions of blocks of frequencies, too, and vendors can obtain a frequency in a secondary market from someone who has obtained one of these blocks.

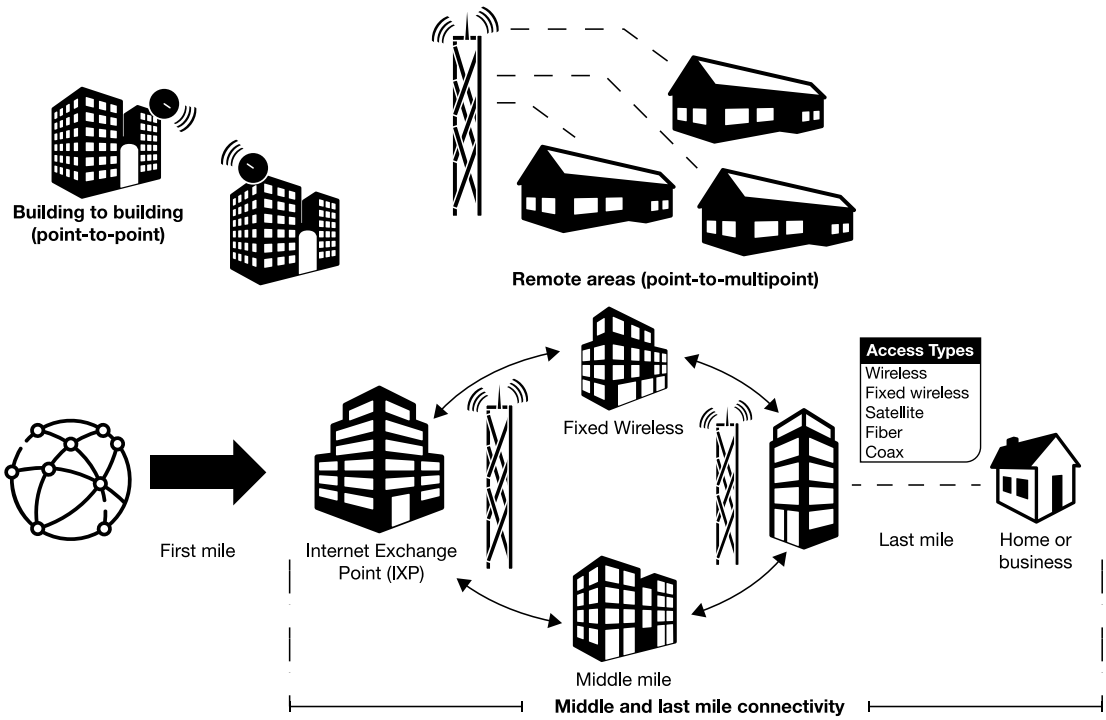


FIGURE 12.15 Long-range fixed wireless uses

The **unlicensed range** of wireless frequencies can get very congested and may be subject to interference from all kinds of devices. Think of the traditional 2.4 and 5 GHz ranges for Wi-Fi. The FCC has opened up areas in the 6 GHz range and subdivided those areas into four Unlicensed National Information Infrastructure (U-NII) bands: U-NII-5, U-NII-6, U-NII-7, and U-NII-8.

There are rules about operating in the unlicensed 6 GHz wireless range. For example, rules specify the two categories of devices that may operate:

> Low-power indoor access points (APs) that cannot be battery operated and devices that connect to them
> Standard-power APs and devices that connect to them

Rules also specify the maximum amount of power that can be transmitted. Table 12.3 summarizes the power requirements for the devices operating in the 6 GHz range. Equivalent isotropic radiated power (EIRP) is a measurement of antenna output.

TABLE 12.3 6 GHz wireless power requirements

Wireless device	Operating band	Maximum EIRP
Standard-power AP	U-NII-5 and 7	36 dBm
Client that connects to standard-power AP	U-NII-5 and U-NII-7	30 dBm
Low-power indoor AP	U-NII-5, U-NII-6, U-NII-7, and U-NII-8	30 dBm
Client that connects to low-power AP	U-NII-5, U-NII-6, U-NII-7, and U-NII-8	24 dBm

You will learn more about wireless networks in Chapter 13. For now, let's consider the web browsers that are used to connect to the internet.

Web Browsers

Web browsers are often used to work on information, data, and files from a server and to surf the internet. Common web browsers include Microsoft Edge, Apple Safari, Mozilla Firefox, and Google Chrome. Edge is the browser that comes with Microsoft-based computers, and Safari is the default browser on an Apple Mac or iPad. In addition, you can download and install other browsers, such as Brave, Firefox, or Chrome. As with any other app or software, be sure to download a browser from the company that makes it:

- **Mozilla Firefox:** mozilla.org
- **Google Chrome:** google.com/chrome
- **Brave:** brave.com

At the source (the website of a company that makes the web browser), a **hash** is generated and sent with the installation file; at the receiving computer, the hash is used to verify that the file that was downloaded is the same as the original file and make sure no corruption occurred. When selecting a web browser, it is crucial to choose one that is regularly updated, actively maintained, and sourced from a reputable provider in a country with strong cybersecurity standards. Avoid browsers from **untrusted sources** such as from ads or email links.

Secure web connections use Hypertext Transfer Protocol Secure (HTTPS). You can see in the web address at the top of a browser that the URL for a secure connection includes https://www.*whatever*. HTTPS uses both HTTP and Secure Sockets Layer (SSL)/Transport Layer Security (TLS) to provide **secure connections**. Part of that process is to issue a security certificate and ensure that the website address matches the web address on the security certificate and also ensure that the certificate is digitally signed by a trusted authority. A notification may appear, saying that a certificate has expired or that an issue has occurred. You will see how to view a certificate later in this chapter (in Table 12.5) and learn more about security certificates in Chapter 18, "Computer and Network Security."

When downloading any information, make sure it comes from a **trusted source** that is a known entity, such as a government agency, a bank, or a website for a specific known company. A related topic is passwords for websites that are accessed using a browser. One security measure might be to use a **password manager**. (This might make more sense after reviewing the concepts in Chapter 18, but it relates here.) Make sure that a user researches various password managers before making a choice and determines if the software has ever had a security breach where data was compromised. Key factors include the following:

- The OS platforms supported, including phone operating systems if the user visits websites via their phone
- Where the password information is saved (in the cloud or locally on the device)
- Whether the software can generate secure unique passwords
- Whether the information is synced across all devices.
- Whether information in accounts is autofilled
- Whether multifactor authentication, which requires two pieces of information to be entered, is used

Browser Features

All browsers have similar features. The most common features are listed in Table 12.4.

TABLE 12.4 Browser features

Feature	Purpose
Address bar	The space where you enter the URL (like pearson.com) of the website you want to access.
Tab	A separate instance of the browser, with its own address bar, that allows multiple sites to be open at the same time.
Bookmark	A website designated as a favorite for easy return.
History	A list of sites previously visited
Refresh	An option that renews a website (which is useful when timeouts occur).
Integrated search	An option that makes it possible to type key words to find a particular site.
Browser extension	Downloadable code that enhances the browser, such as to easily capture what's on the screen, manage passwords, check grammar, remove ads, save content to a file, or easily access an online meeting. Because extensions change settings and may track user information, they are a security risk. Always research any extension and download extensions only from trusted sources.
Browser plug-in	A downloadable executable that adds a specific feature to a browser. Note that some browsers do not support plug-ins anymore for security reasons.

Browser Settings

Because Edge ships with Windows computers, it's easy to use this browser to explain concepts that apply to most browsers. Figure 12.16 shows the menu that opens when you click on the three dots in the upper-right corner of Microsoft Edge as well as the options available within *Settings*. In other browsers, you might click a gear icon or three lines to access the browser settings or tools.

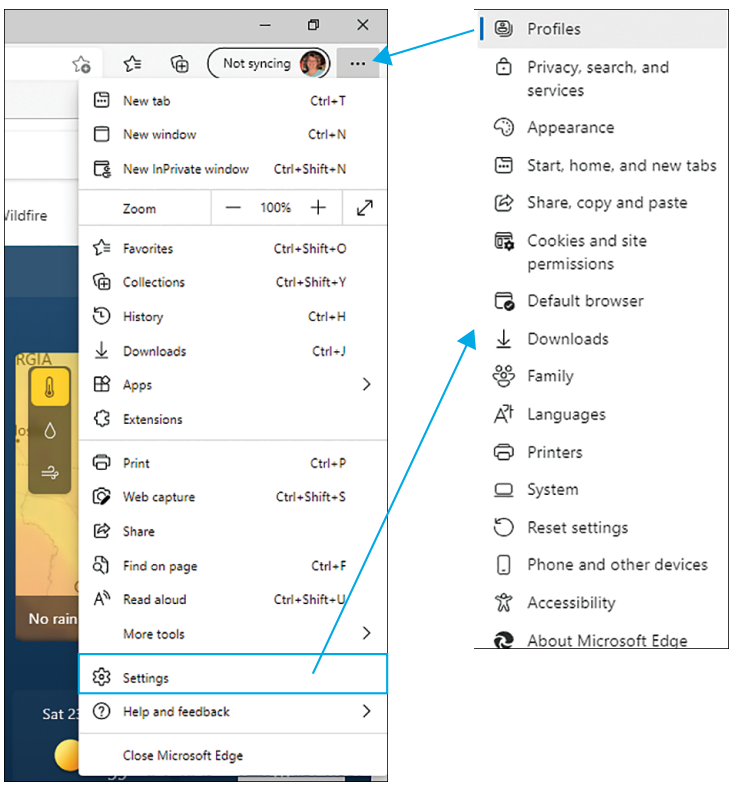


FIGURE 12.16 Settings within Microsoft Edge

The *Internet Options* Control Panel is used to configure some options in non-Windows browsers. Table 12.5 explains the primary purpose of each of the main tabs in the *Internet Options* Control Panel.

TABLE 12.5 Purposes of the Internet Options Control Panel tabs

Tab	Purpose
General	Allows you to configure the home page (the page that opens every time Edge opens or the home icon is clicked), configure how long the browsing history (the websites visited) is kept, configure how tabs are organized and behave, and customize the font, language, and color scheme.
Security	Allows you to configure security options for sites that you trust and sites that you want blocked (see Chapter 18).
Privacy	Allows you to configure how your private information is handled, including cookies and pop-ups (see Chapter 18).
Content	Provides options for controlling security certificates, AutoComplete for ease of completing online forms, and Feeds and Web Slices for providing updated content directly into the browser.
Connections	Provides options for configuring an internet connection, dial-up (phone line) connection, proxy server, or VPN (virtual private network) information. (Proxy servers and VPNs are also covered in Chapters 13 and 18.)
Programs	Provides options for configuring email access, add-ons such as toolbars and extensions, and HTML-editing program options.
Advanced	Shows a list of options that might be set throughout the other tabs, also presented here in one easily configured list of checkboxes.

Some of the common basic web browser configuration settings that you need to know are listed in Table 12.6.

TABLE 12.6 Common web browser configuration settings

Setting or capability	Purpose and how to configure
Default browser	Sets a particular browser as the default to be used when a web link is clicked. Can be set through OS *Settings*, too. Edge: *Settings* > *Default Browser* > *Make default* button Firefox: *Settings* General section > *Make default* button Chrome: *Settings* > *Default Browser* > *Make default* button
Clear browsing data	Removes cookies, websites visited history, and other data that is tracked based on the URLs used. Edge: *Settings* > *Privacy, search, and services* > *Clear browsing data* section Firefox: *Settings* > *Privacy & Security* > *Cookies and Site Data* section > *Clear Data* Chrome: *Privacy and security* > *Clear browsing data*
Clear cache	Used when a particular website does not work or a web page is not formatted correctly. In the most common browsers, you can press Ctrl+⇧Shift+Del to clear the cache.
Private browsing	Does not keep browsing history, cookies, or data collected during a browsing session. Edge: *Three dots* > *New InPrivate window* Firefox: *Three lines* > *New Private Window* Chrome: *Three dots* > *New incognito window*

Setting or capability	Purpose and how to configure
Browser synchronization	Makes browser settings and data such as bookmarks and passwords the same across multiple devices for a particular user who is logged into their account. Edge: Click on account picture > *Turn on sync* button Firefox: *Settings* > *Sync* Chrome: *Settings* > *Turn on sync* button
Security certificate verification	Verifies the authenticity of the security certificate of the current website. Edge: Click lock icon in address bar to see the name of the certificate authority Firefox: Click lock icon in address bar > *More Information* button > *Security* > *View Certificate* button Chrome: Click lock in address bar > *Certificate* (Valid)
Additional security certificate information	Provides additional security certificate information, a list of intermediate certificate authorities, trusted root certification authorities, the ability to import a certificate, and other advanced features. Edge: *Settings* > *Privacy, search, and services* > *Security* section > *Manage certificates* Firefox: *Settings* > *Privacy & Security* > *Certificates* Chrome: *Settings* > *Privacy and security* > *Manage certificates* Note that you might also want to use the Microsoft Certificate Manager to view, modify, update, import, export, or delete a security certificate.
Proxy	Serves as a go-between between the browser and a remote server. To configure your browser as a proxy server, you need some basic configuration information from the network administrator. Then use the *Network & Internet* Settings link to access the *Proxy* option.
Secure DNS	Because the Domain Name System (DNS) is used to translate common web URLs like www.pearson.com to an IP address, DNS is a target for attacks. Use secure DNS to encrypt data sent from a device to the DNS server. Edge: *Settings* > *Privacy, search, and services* > *Security* section > *Use secure DNS* Firefox: *Settings* > *Privacy & Security* > *Enable DNS over HTTPS using:* Chrome: *Settings* > *Privacy and security* > *Security* > *Use secure* DNS

You might determine that a browser extension or a plug-in is causing a browser issue. Here's how to view and potentially disable or remove a browser extension or plug-in:

- **Edge:** Select *Settings and more* option from the upper-right corner > *Extensions*.
- **Firefox:** Select *Open Application Menu* option from the upper-right corner > *Add-ons and themes* > *Extensions or Plugins*
- **Chrome:** From a browser tab in the address textbox, type `chrome://plugins`. From the *Customize and control Google Chrome* option upper-right corner > *More tools* > *Extensions*

Basic Web Browser Issues

Configuring a web browser is one of the first steps in configuring security. **Browser patching** involves upgrading a web browser to provide improved security options. Before upgrading a browser, you must determine the current web browser version. With many Windows-based applications, the version is determined by starting the application, clicking *Help* > *About x* (where *x* is the name of the application), or selecting the question mark menu item.

TECH TIP

Why keep Windows and your web browser current?

Internet hackers frequently target browsers, and constant updates are provided to counter these attacks.

One issue with browsers is that they can be hijacked (see Figure 12.17). A hijacked browser either replaces the home page with another one or directs whatever web page is being used to a different one. This is called a **browser redirection**. Besides sending you to another web page, a redirection can also be used to install a rootkit or install more malware ("bad software"), such as keystroke loggers (to record your keystrokes, including your typed usernames and passwords), perform DNS hijacking, or install a rogue HOSTS file. (The HOSTS file is a text file used to manually map a hostname to a particular IP address.) A **rootkit** is a backdoor into your operating system that may be used to do things that require administrator access. Rootkits can be downloaded and installed to flash drives.

FIGURE 12.17 Web browser redirect

The following recommendations can help with browser hijacking issues:

- Change the home page URL to your normal home page and not the hijacked page. In any browser, go to the web page that you want to be the home page and copy that web address. Then change the home page URL:
  - **Edge:** Access *Settings* > *Start, home, and new tabs* > *Home button* section and enter the URL
  - **Firefox:** Access *Settings* > *Home* option in left menu > type a URL in the *Homepage and new windows* textbox
  - **Chrome:** Access *Settings* > *Appearance* > enable *Show Home* > enter a URL in the *Enter custom web address* textbox
- Clear the browser history/cache (refer to Table 12.6).

- If clearing the browser history/cache does not work, reset the browser settings:
  - **Edge:** Access *Settings* > in the *Clear browsing data* section, select *Choose what to clear* > enable all options > *Clear*
  - **Firefox:** Select *Help* from the three lines menu > *More troubleshooting information* > *Refresh Firefox*
  - **Chrome:** Access *Settings* > expand *Advanced* and select *Reset and clean up*
- Try a different browser to see if the symptom remains. You could also uninstall the browser and reinstall it.
- If necessary, start the computer in *Safe Mode with Networking*. If the web browser works properly in this mode but not when normal booting straight to Windows, a DLL file might have been added to the computer. Run a scan with your anti-malware application.
- Start the browser with no add-ons to see if one of them is causing the problem.
- If the browser starts working, turn on the add-ons one by one to determine which one caused the problem.
- Determine whether the HOSTS file has been modified and includes some rogue entries. The HOSTS file can be found in the C:\Windows\system32\drivers\etc folder.

If **pop-ups** (unwanted messages, screens, or windows) appear continuously, use Task Manager to stop the specific browser process. Reopen the browser and ensure that the pop-up blocker is turned on:

- **Edge:** Access *Settings* > *Cookies and site permissions* > *Pop-ups and redirects* > enable *Block*
- **Firefox:** Access *Settings* > *Privacy & Security* > in the *Permissions* section enable *Block pop-up windows*
- **Chrome:** Access *Settings* > *Privacy and security* > *Site Settings* > in the *Content* section select *Pop-ups and redirects* > *Don't allow sites to send pop-ups or use redirects*

If these steps don't help, use a different browser. Install anti-malware software. You can always uninstall and reinstall a browser, too.

TECH TIP

Browser troubleshooting tools

Firefox has a *Troubleshoot Mode* link available through the *Help* menu option that you can use when you are experiencing issues. Chrome has its own Task Manager that can be used to stop specific processes: select *More tools* from the three dots > *Task manager*. Edge has something similar available from the three dots menu *More tools* option > *Browser task manager*.

Many websites include advertisements. With some browsers, private browsing (refer to Table 12.6) can help reduce or eliminate ads. Free software for **ad blockers** exists, but ensure that any ad blocker you use is legitimate, works on your favorite browser(s), and is downloaded from a legitimate source.

Degraded Browser Performance

If your browser seems to be getting slower and slower, but the rest of the machine is running fine, there are a few things you can do:

- Disable unnecessary add-ons.
- Disable all add-ons and re-enable them one at a time.

> Disable extensions.
> Uninstall and reinstall the web browser.
> Clear the browser cache/history (refer back to Table 12.6).
> Reset the browser settings.
> Use a different web browser.

Introduction to Virtualization

As a help desk technician or a PC technician, you will run into virtualization as this area of computers is becoming very prevalent. **Virtualization** involves using software that allows a single computer to be made into multiple virtual computers. For example, with virtualization, one PC can provide **isolation** by running two operating systems that have no knowledge of each other (see Figure 12.18). You can also use virtualization to have a PC act like a different device (such as a router) and, for example, allow your gaming console to create a virtual private network (VPN) tunnel into your PC and connect to other networks. Another common use of virtualization is with servers, where a powerful machine can host multiple servers separated from one another (see Figure 12.19).

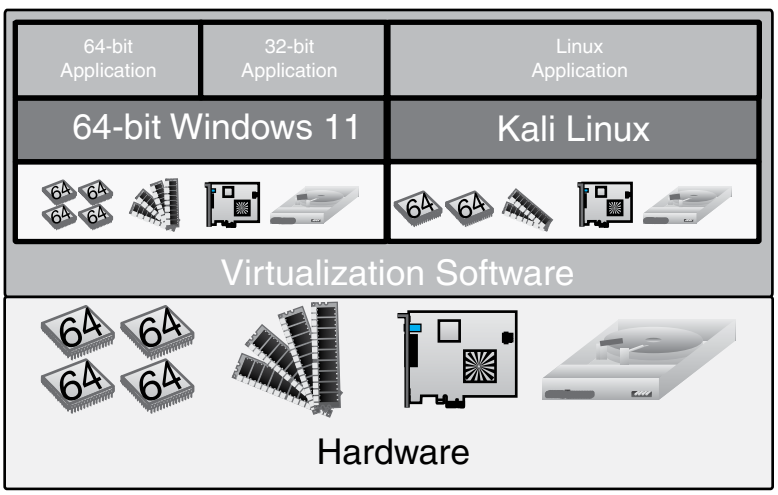


FIGURE 12.18 PC virtualization

Why is virtualization so popular? For one thing, virtualization enables **test development** as it provides a way to test things out in an environment that doesn't hurt anything else. A virtualized computer can provide a **sandbox** to do specific testing, such as opening suspicious software or files without allowing any malware to spread to other computers. In addition, virtualization can be used to run **legacy software** that is made for an older operating system (application virtualization) or even to run that older OS. An example of **cross-platform virtualization** is running an additional OS on a computer, such as running Windows as well as macOS on a Mac. Let's dive into how virtualization is used for desktop computers since that is our focus for a lot of this book.

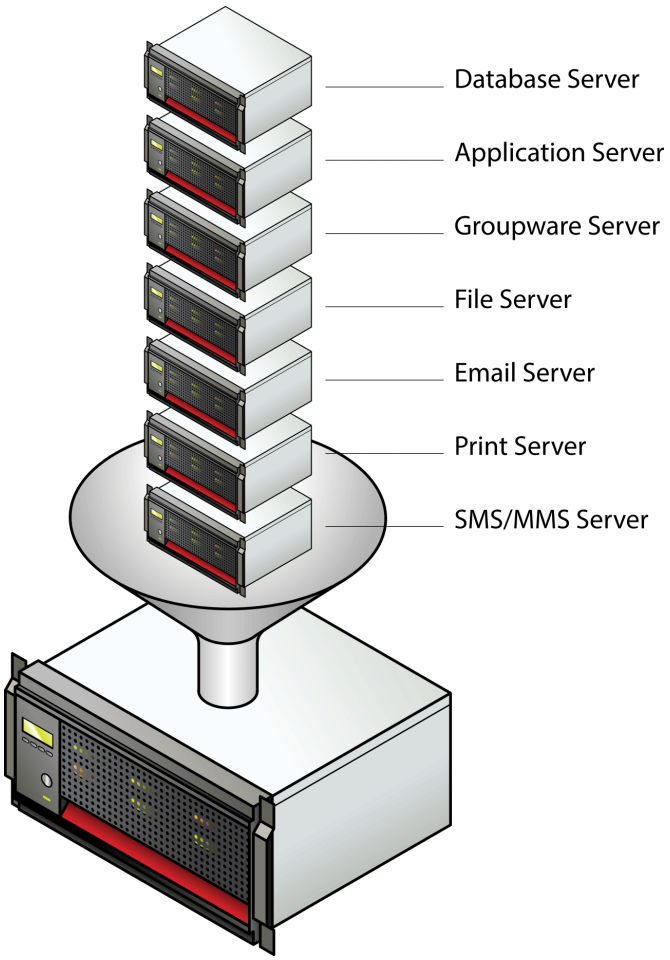


FIGURE 12.19 Server virtualization

Desktop Virtualization Basics

There are two ways to virtualize a desktop computer:

> You can use multiple operating systems on one computer. They can share hardware without affecting each other (or even knowing about each other). Look back at Figures 11.7 and 12.18 to see this concept.

> You can use a server to hold multiple virtualized desktop computers, as shown in Figure 12.20.

A company may have servers and storage and other infrastructure devices in its network operation center. Collectively this equipment is known as the virtual desktop infrastructure (**VDI**). When the equipment for VDI is within the company, this is known as VDI on premises. The infrastructure equipment could also be at another site; this is known as VDI in the cloud. (More cloud concepts are coming in the next section.) The last option is to just get another company to handle these desktop images. This is known as desktop as a service (DaaS). If virtualization is handled within the company, the users are more likely to be able to customize which apps are deployed to each user and have more control over the data generated. With DaaS, new desktops can be provided to users quickly, and upgrades or restoration after failure tend to be quicker.

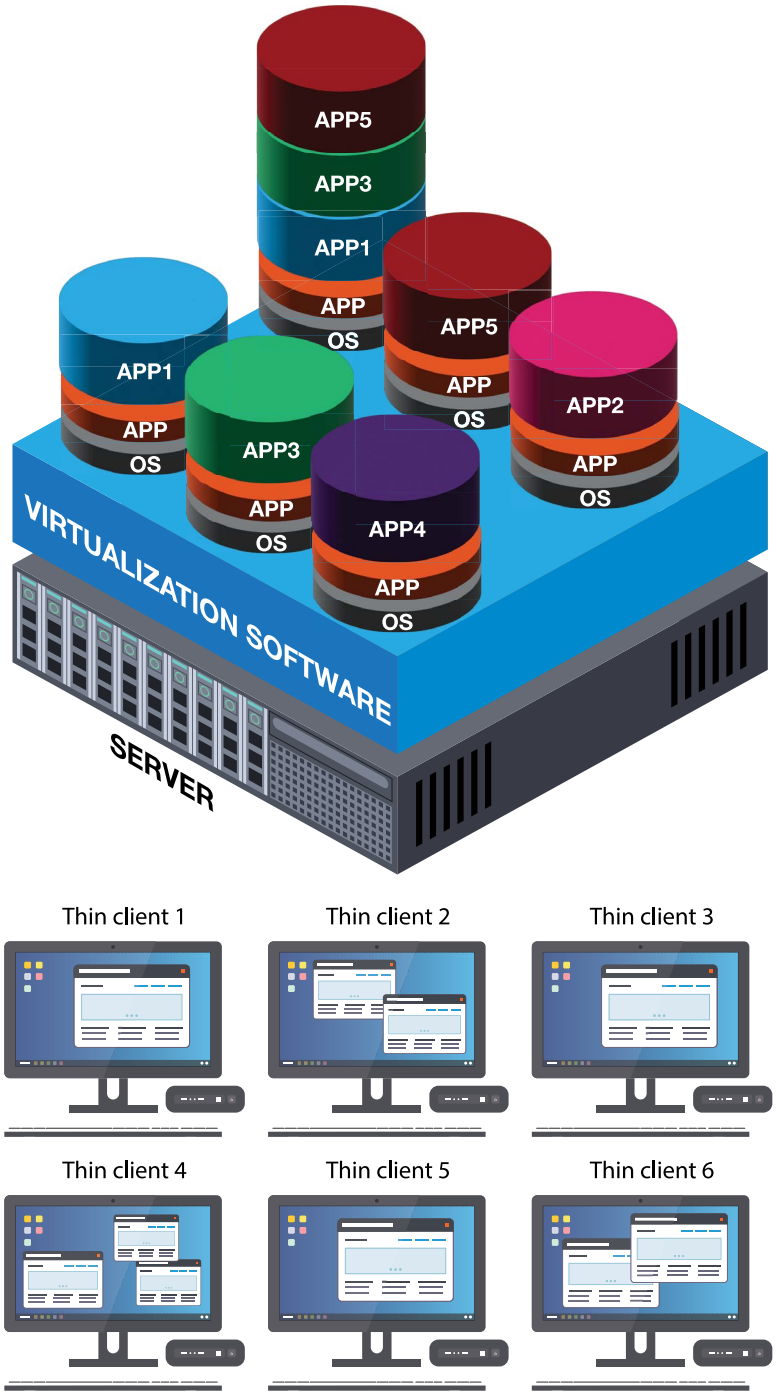


FIGURE 12.20 Desktop virtualization

When you put more than one OS on a PC, the computer has to have a virtualization application such as a VMware Workstation, Oracle VirtualBox, or Microsoft Hyper-V to hold instances of one or more operating systems. Table 12.7 shows some commonly used virtualization terms.

TABLE 12.7 Virtualization terms

Term	Description
Host machine	The real computer that holds multiple operating systems
Virtual machine	Also called a VM, a separate operating system from the host computer OS that has specifically chosen hardware components
Hypervisor	Also called virtual machine monitor or virtual machine manager, the software that can create a virtual machine and allocate resources to the virtual machine
Snapshot or **checkpoint**	A copy or backup of the VM at a particular point in time, which can be used to revert the VM to that point in time (which is a similar concept to a Windows restore point)

The hypervisor, which is like an orchestra conductor for virtualization, is responsible for managing and overseeing the operation of the virtual machines (VMs). The hypervisor oversees RAM, hard drive space, and any processor(s) shared between the VMs.

There are two types of hypervisors:

> A **Type 1 hypervisor** is also known as a native hypervisor because the operating system runs on top of the hypervisor. Examples of Type 1 hypervisors include VMware's ESXi and Microsoft's Hyper-V.

> A **Type 2 hypervisor**, also known as a hosted hypervisor, runs on top of a host operating system such as Windows 11. VMware Player, Oracle VirtualBox, and Windows Virtual PC are examples of Type 2 hypervisors.

In Figure 12.18, there are two CPUs and less RAM (two sticks) in the VM (virtual machine) on the right than in the VM on the left, which uses four CPUs and four sticks of RAM. Within one virtual environment, you should not (and, in some instances, cannot) "install" more hardware than is on the host machine (the real machine), even though some virtualization software allows you to do so. For example, say that the VM on the left in Figure 12.18 is assigned the full amount of RAM that is on the host machine, 64 GB, and the VM on the right is assigned 16 GB. The total is 80 GB, but the host machine has only 64 GB. This is allowed and common in virtual environments. Some virtualization software (but not all) enables you to select 128 GB for the VM on the left, but doing so causes degradation in the virtual environment.

Working with VMs makes restoring an operating system (or a VM that holds an operating system) much easier than using the traditional operating system–based restoration methods. Technicians today are expected to know the basics of working in a virtual environment.

TECH TIP

You have to buy the OS license

A common misconception about virtualization is that you don't have to buy both operating systems when two operating systems are installed. This is not always true and depends on the virtualization software used. If you want to install Linux in one virtual machine, Windows 11 in another virtual machine, and Windows Server 2022 in a third virtual machine, you have to purchase any operating system that requires a license (Windows 11 and Windows Server in this example).

Virtualization Resource and Emulator Requirements

When you implement virtualization, you are required to have more resources than you would have with a standard PC. You need more CPU power, more RAM, and more storage space.

(Look back at the "Virtualization Workstations" section in Chapter 11, "Computer Design and Troubleshooting Review," to review hardware components.)

Most Windows versions today have some type of emulation or virtualization included. An emulator is hardware or software that makes one operating system behave like an older or different one. Windows XP Mode is a program you can download from Microsoft.com that is designed to run Windows XP applications in a protected environment. Windows Virtual PC allows other Windows operating systems to run inside Virtual PC and provides one-click access to Windows XP Mode, which is integrated into Virtual PC.

Windows 10 Pro and higher versions have replaced Virtual PC with Hyper-V. To enable Windows Hyper-V, access the *Programs and Features* Control Panel > *Turn Windows features on or off* > enable *Hyper-V* checkbox (see Figure 12.21).

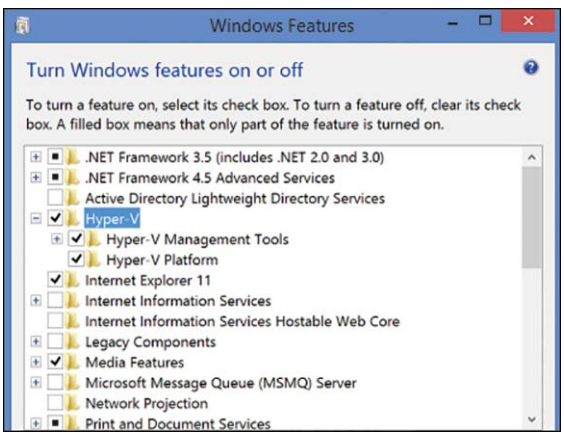


FIGURE 12.21 Enabling Hyper-V in Windows

TECH TIP

Hyperthreading may need to be enabled

Research your hypervisor type to determine whether hyperthreading needs to be enabled in the BIOS/UEFI.

Each virtual machine can connect to a network using one of two basic options (and note that in Hyper-V, these options are configured through a virtual switch):

- **Internal network:** This option allows a particular VM access to other virtual machines that connect to the same network (though they may be on a different computer or in another VM on the same computer).
- **External network:** This option allows a particular VM access to a different (external) network from within the VM. In a college environment, for example, if a student computer can access the internet and that same computer is configured for virtualization, a VM on that student computer can be configured for the external network and have access to the internet.

Virtualization Security

A critical security risk with virtual machines is VM escape, where a hypervisor or operating system vulnerability allows an attacker to break out of the isolated VM environment, potentially compromising multiple VMs and the host system. When using virtualization, each virtual machine needs the same protection as an individual computer. All security concepts apply not just to the host machine but to each virtual machine as well.

TECH TIP

A VM can get a virus

A common misconception about virtualization is that you don't have to worry about security because you are in a "protected" environment. This is not true. One operating system is indeed protected from the other operating system, but all virtual machines are susceptible to viruses and security attacks. It is important to install the appropriate protection. See Chapter 18 for more information on security.

Containers

Somewhat related to virtualization is the concept of containers. A **container** is an environment that holds all of the files and associated resources needed for code, an app, or a service that is separate from other apps (see Figure 12.22). The container can be on a server, in a VM, or run on a cloud platform (covered next and in Chapter 13). Containers can easily be replicated, added, or deleted as needed without affecting other containers. Containers are more portable than VMs. A container can be networked with other containers or have its own public IP address and connect with an external network.

Imagine that some code is needed within an online financial company app that is used to show current market sectors. If a lot of people are using that code, more instances of that app can be spun up within a container without having to dedicate more resources or duplicate the entire financial app. Another benefit is that everything needed to run the app is in the image file within the container.

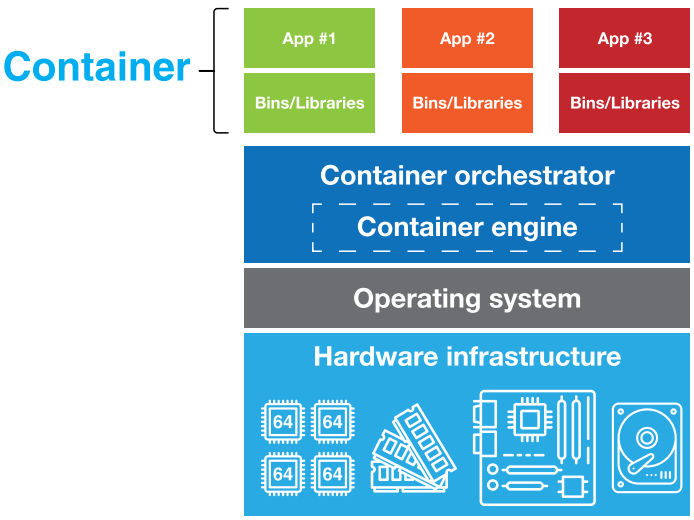


FIGURE 12.22 App container

Cloud Computing

Cloud computing was briefly introduced in Chapter 9, "Printers/Multifunction Devices," with printing to the cloud, and you have already heard how a desktop image might be provided by a remote company. You need to learn a bit more about cloud computing because cloud technologies are prevalent in small, medium, and large businesses alike.

What does it mean to say that something is "in the cloud"? It simply means the network device, application, storage, connectivity, server, and more are not located within the company's physical location. Cloud technologies have been around for years. They might be used, for example, for a small business that doesn't have the resources or staff to create and maintain a web server. That web server can be hosted elsewhere, in which case it is considered "in the cloud"—that is, out on the internet somewhere (see Figure 12.23) .

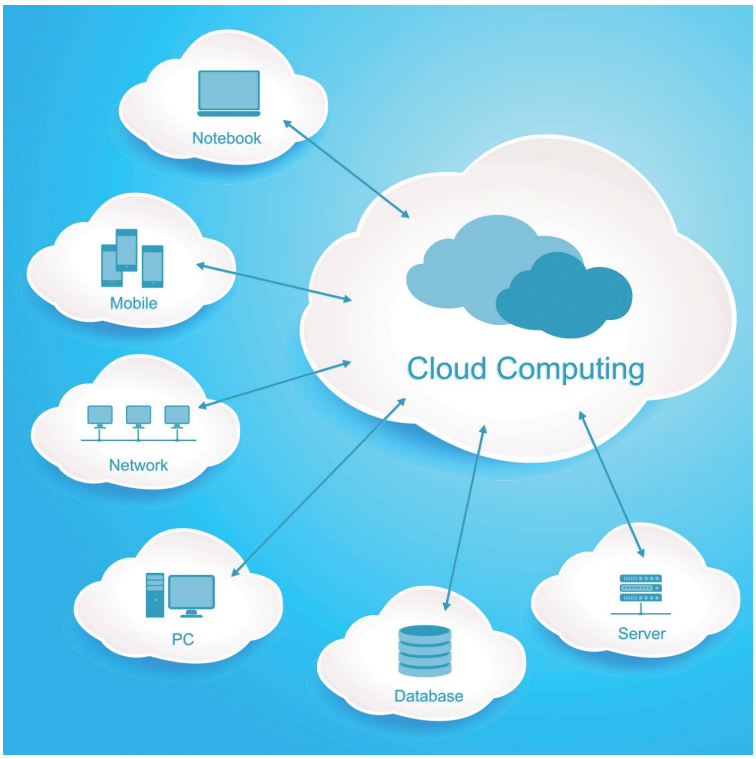


FIGURE 12.23 The concept of "in the cloud"

Cloud Services and Models

Different types of services are provided by cloud vendors, as outlined in Table 12.8.

TABLE 12.8 Cloud service types

Cloud service type	Description
Software as a service (**SaaS**)	Applications such as learning management, enterprise resource planning (ERP), human resources management (HRM), payroll, antivirus, and inventory management systems are hosted by another company. Cloud-based applications that you might be more familiar with—such as Microsoft Office 365, GitHub, a personal calendar, or a diet tracker—are also considered SaaS.
Desktop as a service (**DaaS**)	Users access a virtual desktop that is managed by another company or for which the equipment is located elsewhere. This would simply be the computer in a virtual environment so that the company that uses this service does not have to worry about software licenses, technicians to maintain operating system updates, and backups. A virtual desktop also includes a virtual network interface card (NIC), or virtual NIC, as discussed in more detail in Chapter 13.
Platform as a service (**PaaS**)	Servers, databases, operating system, storage, and development tools are provided in an outside environment to relieve the support burden on a company that needs an environment to perform high-level programming and develop applications.
Infrastructure as a service (**IaaS)**	Routers, switches, servers, virtual machines, load balancers, access points, storage, and other infrastructure devices are provided through the online environment.

Cloud Technologies

Just about any technology that is used within a corporate environment or personal computing environment can be offered as a cloud service. The most popular offerings for business include the following:

- **Off-site email applications:** Instead of a company having to house its own email servers, email services are commonly housed in the cloud environment, either on the company's own servers located in a remote location or provided by a cloud-hosted email provider.
- **Cloud file storage services:** Many people use external storage, such as Microsoft OneDrive, Google Drive, Apple iCloud, Dropbox, SugarSync, Box, SpiderOak, or Tresorit. A popular feature of cloud-based storage is **file synchronization**, which allow for files and folders to be synced between devices and accessed from anywhere. It is important to have enough bandwidth when syncing to the cloud.
- **Virtual application streaming/cloud-based applications:** Applications can be virtualized so that each application doesn't have to be installed on individual devices. This prevents conflicts with other apps and provides better security controls. Some applications use streaming, which involves sending just some of the code needed to run the application and works well on mobile devices.
- **Cloud-based network controller:** Vendors commonly have network controllers that control network devices (as discussed in Chapter 13). As shown in Figure 12.24, a cloud-based network controller might be used to monitor and control switches located at the main company and branch offices. Figure 12.25 shows a cloud-based network controller that is used to control and monitor access points.

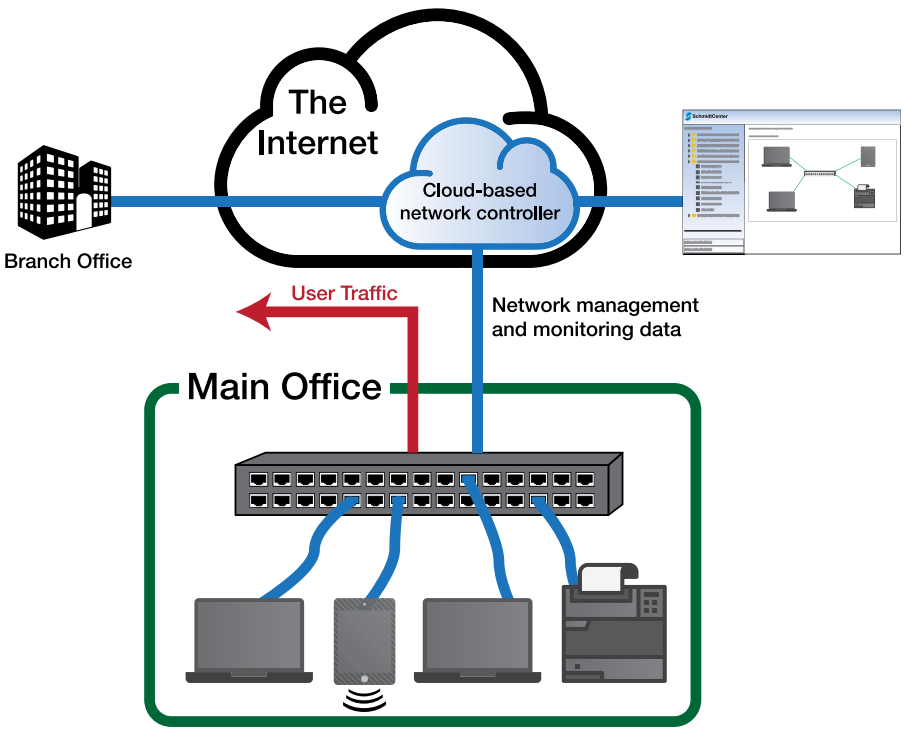


FIGURE 12.24 Cloud-based network controller for switch control

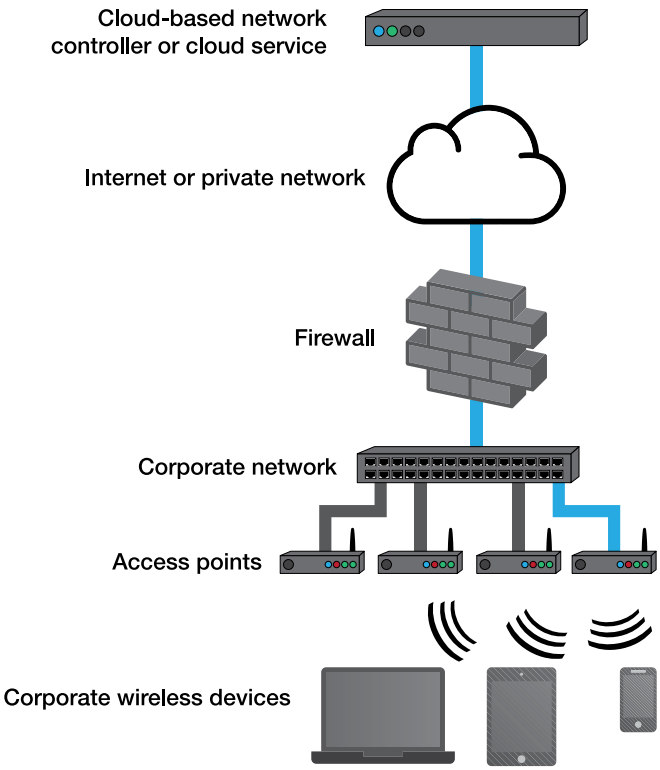


FIGURE 12.25 Cloud-based network controller for access point control

Cloud Service Deployment Methods

Cloud services can be deployed in a combination of ways: private, public, hybrid, and community (see Figure 12.26). A **private cloud** is part of a company's network infrastructure that is located outside the business in a remote location, but the company has responsibility for managing the software and/or hardware. For example, a college may purchase licenses for a learning management system (LMS). The LMS could run on servers that are located in a remote vendor's location, but the college network administrators install, update, and maintain responsibility for supporting the LMS. Large businesses tend to be the biggest users of private clouds. With a private cloud deployment, a business doesn't have to worry about providing power, cooling, and space for the equipment and optionally can pay for redundant internet access and equipment and other features from the cloud provider.

A **public cloud** is an environment operated by a cloud provider. The cloud provider provides services to all business sizes for a cost. Again consider an LMS as an example; the servers and software for the LMS could be provided by the LMS vendor, which has the servers in a service provider's building. In a public cloud, the vendor or cloud provider has the responsibility for managing the software and/or hardware. In a public cloud deployment model, several companies pay for the services of the public cloud vendor. For an LMS, many colleges might purchase the public cloud option and allow another company to configure, monitor, and maintain the LMS.

A **hybrid cloud** is a combination of a private cloud and a public cloud. For example, a company using cloud services is responsible for the licensing and maintenance of the LMS in the private cloud but might need additional storage or servers during peak times. A hybrid cloud solution could be implemented as a failover solution as well. In such a case, the private cloud is used, but if a disaster occurs or during planned maintenance periods, the company uses the application in the public cloud instead.

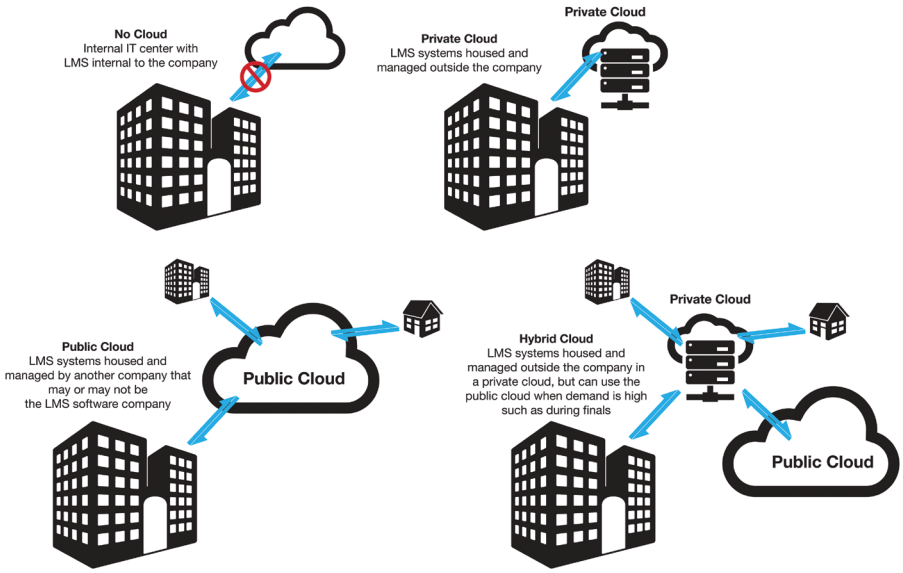


FIGURE 12.26 Cloud deployment models

With a **community cloud**, a number of organizations have access to IT resources that are in the community cloud. An example of this might be an IT system created by a consortium of colleges in one state that are co-developing the system. The system could be housed in the cloud and tested on systems in the cloud. The cost for the community cloud would be shared by all the colleges in the consortium.

Cloud Characteristics/Advantages

Cloud computing has many potential benefits to businesses, including reduced costs, increased flexibility, increased efficiency, and consistently applied software patches and upgrades. Costs related to network operations centers have increased due to the use of and reliance on technology throughout a business. Common network center costs and overhead include power, hardware, hardware redundancy, storage, fire protection system, licensing, cabling/interconnectivity, and backups. Cloud computing enables an organization to drastically cut down or even eliminate network center costs.

Other advantages of using cloud technology include the following:

> **Corporate focus:** Cloud computing enables a company to focus on core IT services or the true function of the company, while a vendor focuses on its particular strengths, such as technical expertise on a particular product, staffing levels, quality of service, customer service, and so on.

> **Availability:** Cloud computing supports **availability**, offering continuous 24/7 access from anywhere and possibly any device. Access is on-demand, meaning that it is available when and where the customer needs it.

> **Elasticity:** Cloud computing facilitates **elasticity**—that is, quick expansion or contraction of services, software, and/or hardware. For example, if another server or more storage or more of anything else is needed, the vendor can access resources that allow expansion on demand. For a company using an internal system, such an expansion might take several months because of the time needed to requisition and obtain the resources.

> **Shared resources:** A big part of cloud computing is taking advantage of resource pooling. **Shared resources** between companies or even within the same company can include servers, applications, hardware components such as RAM and CPUs, data storage, internet

connections, and network infrastructure equipment. Think back to virtualization, which is a big part of the cloud environment. Within one computer, the virtualized environment provides resource pooling, such as sharing RAM or CPUs between the multiple operating systems loaded. The resources could be resources owned by the company but housed elsewhere (internal shared resources), or they could be shared with other companies and hosted by an external vendor. By using an outside vendor's services, a company can pool resources with other companies that have the same need. A vendor might have access to hundreds of servers. Say that Company A needs just a few servers right now, but Company B has a high usage rate. The outside vendor can allocate servers to Company B to handle the load right now and later reallocate the additional servers to Company A, when its usage increases. Multiple companies using resources from the same cloud vendor is known as **multitenancy**. In contrast, if a company uses its own equipment rather than using cloud services, the equipment has **dedicated resources** that tie up CPU power, RAM, and storage space for an app that might show erratic usage when other apps could be using those resources.

> **Service rates:** A cloud provider can allocate resources easily by providing a **metered utilization** service, for which a company pays an amount based on how much of the service it uses on an hourly or monthly basis. Some providers charge a data rate based on **egress** (how much data leaves the cloud) and **ingress** (how much data enters the cloud). There is also a fee structure that involves a fixed charge and usually involves fixed resources or configurations.

SOFT SKILLS: MENTORING

Every great technician can tell you that they have had at least one mentor along the way. When you hear the word *mentor*, it probably conjures up other words and phrases in your head—coach, guide, teacher, adviser, positive influence, leader, example, and so on. No technician can attain their ultimate level without being mentored. Also, no technician can learn everything from a book or from personal experience. Others helping us along the way enable us to learn faster and more efficiently.

When you enter your first (second, third, or fourth) job in the IT field, you should take a few days to look around the company. Find someone who appears to be very professional and knowledgeable—someone you want to emulate. Talk to that person and explain your goals. Ask if they will mentor you—helping you with problems you cannot solve and giving you advice about office politics (see Figure 12.27).

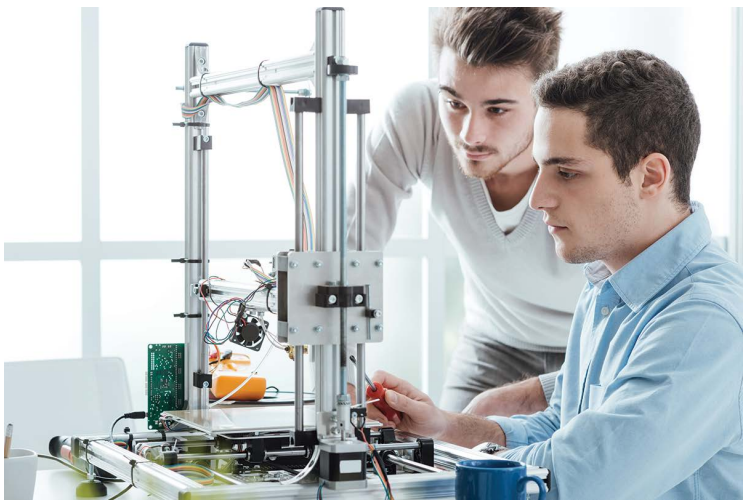


FIGURE 12.27 Mentoring

Mentoring is an important part of life. Not only should you consider being mentored, you should consider mentoring others. Many technicians hoard information from other technicians and computer users. Knowledge is power, and by sharing information with others and helping them along the way, you cement and expand your own knowledge.

Chapter Summary

- Serial devices must be configured for the number of bits, parity, stop bits, FIFO setting, flow control such as XON/XOFF (software method) or RTS/CTS (hardware method), and handshaking. The two sides of a connection must match.
- Internet connectivity can be provided by an analog modem, satellite modem, cable modem, fiber, DSL modem, or wirelessly through the cell phone network, wireless broadband, long-range fixed wireless, a WISP, or a Wi-Fi network.
- Cable modem bandwidth is shared by the subscribers in an area. If the number of subscribers is too many and the cable bandwidth is unacceptable, a direct fiber connection might be an option.
- A DSL modem uses a phone line. ADSL has faster downstream speeds than upstream speeds.
- VoIP uses a corporate network and/or the internet for voice connectivity. Internet-based VoIP does not offer QoS.
- Wireless communications have both licensed and unlicensed frequency ranges. The licensed range has better performance due to reduced interference. Some of the unlicensed ranges still have rules associated with them.

- Technicians frequently have to configure web browsers. With most browsers, you use the *Settings* option to begin the configuration process.
- Keep a web browser current for security reasons.
- Private browsing prevents a web browser from storing browsing history information and passwords.
- A hijacked browser redirects to a different web page. Pop-ups can be managed by using a pop-up blocker.
- Disable add-ons to prevent pop-ups and prevent browser hijacking.
- Virtualization can be used to test apps, operating systems, or code; as a sandbox to prevent other devices from being affected; or to run an older OS.
- Desktop virtualization can be done within a company on premises using a VDI or provided as a cloud service (DaaS).
- A computer that uses virtualization must have more hardware to run more than a single operating system environment.
- A virtual desktop is an operating system that is in a virtual machine and used in a corporate environment to more easily manage multiple computers.
- A container has all the code, libraries, and bins needed to create an application. Containers can be easily replicated, deleted, and added as needed.
- Cloud technology services are classified as SaaS, DaaS, IaaS, and PaaS. Cloud deployment models include private, public, hybrid, and community clouds.
- Shared resources can be internal or external.
- Cloud services can be provided as measured services, as metered services, or for a flat fee.
- Mentoring is important when you get started as a technician and as you gain experience.

A+ CERTIFICATION EXAM TIPS

- ✓ Know cable modem DSL, and ONT connectivity/hardware.
- ✓ Be aware of the implications of a frequency range being licensed or unlicensed and the regulatory requirements for wireless power.
- ✓ Know the difference between and features of the following internet connection types: cable, DSL, cellular, WISP, satellite, and fiber.
- ✓ Know the differences between SaaS, PaaS, DaaS, and IaaS and between public, private, hybrid, and community cloud deployments.
- ✓ Be able to describe how desktops can be virtualized through a VDI on site (on premises) or from the cloud.
- ✓ Know the purpose of setting up a virtual machine, including using it as a sandbox, for test development, for application virtualization, when using legacy software or an OS, or for cross-platform virtualization. Also be aware of the resource and security requirements involved in using virtualization.
- ✓ Know the meanings of the following cloud-related terms: shared resources, dedicated resources, elasticity, metered utilization, availability, multitenancy, and file synchronization.
- ✓ Explain the purpose of a container.
- ✓ When troubleshooting a network, be aware of jitter and how it might be used in determining issues with VoIP quality.
- ✓ Be able to install and configure browsers and know what a trusted or untrusted source is as well as how hashing is used. Be able to install and configure extensions, plug-ins, and browser features. Know settings for pop-up blockers, clearing the cache, private browsing, ad blockers, proxies, secure DNS, and data synchronization.
- ✓ Be able to recommend, install, and configure a password manager. Be able to recognize a secure connection and know what a security certificate is and how to manage it.

Key Terms

3G, 4G, 5G, ad blocker, ADSL, availability, bandwidth, browser extension, browser patching, browser plug-in, browser synchronization, browser redirection, cable modem, certificate warning, checkpoint, clear browsing data, clear cache, coaxial, community cloud, container, convergence, cross-platform virtualization, DaaS, dedicated resources, dial-up network, downstream, DSL, egress, elasticity, fiber network, file synchronization, hash, host machine, hybrid cloud, hypervisor, IaaS, ingress, isolation, ISP, jitter, latency, legacy software, licensed range, long-range fixed wireless, LTE, metered utilization, mobile hotspot, multitenancy, ONT, PaaS, password manager, phone filter, poor VoIP quality, pop-up, private browsing, private cloud, proxy, public cloud, QoS, rootkit, SaaS, sandbox, satellite modem, secure connection, secure DNS, security certificate verification, shared resources, snapshot, test development, tethering, trusted source, Type 1 hypervisor, Type 2 hypervisor, unlicensed range, untrusted source, upstream, VDI, virtual machine, virtualization, VoIP, wireless broadband, WISP, xDSL

Review Questions

1. A company outsources corporate payroll to a company that provides a cloud-based solution. What type of cloud service is being provided?

   [DaaS | SaaS | PaaS | IaaS]

2. A company has its email server in the cloud. The company has a network administrator assigned to maintain and manage the email server. Which cloud deployment model is used?

   [community | private | public | hybrid]

3. Which internet connectivity type handles the most data with the least amount of data loss?

   [long-range fixed wireless | DSL modem | cable modem | fiber]

4. In which situation would an ONT be used?

   a. When wireless broadband is used

   b. When a small business has a fiber connection

   c. When a home has internet connectivity through a satellite dish

   d. When internet connectivity is provided through a long-range fixed wireless system

5. What is VoIP?

   a. A cable modem technology

   b. A method used to wirelessly connect to the internet

   c. A method of using a network to carry voice traffic

   d. Network communication that is faster on downloads than on uploads

6. What component does DSL use to separate and transmit both voice and data signals simultaneously without blocking the phone line for phone calls?

   [modem surge protector | phone filter | ONT | RJ11 connector]

7. What are the advantages of using a licensed wireless frequency range? (Choose two.)

   [reduced oversight and management | increased reliability | cannot be used by WISPs | reduced interference | lack of secondary markets]

8. Which IT technology is used when a company has implemented VDI?

   [desktop virtualization | wireless connectivity | fiber connectivity | web browser security]

9. What is one drawback to a cable modem?

   _____

   _____

10. What does *asymmetrical* mean in relation to an ADSL modem?

    _____

11. Which virtualization component manages VMs?

    [hypervisor | filter | virtual NIC | virtual BIOS/UEFI]

12. Which solution would not help a system that has slow performance in a web browser?

    a. Reset the browser settings.

    b. Clear the browser cache and history.

    c. Disable extensions and add-ons.

    d. Return the OS to a previous version.

13. What is wireless broadband?

    _____

    _____

14. What is most important when syncing data to the cloud?

    [CPU speed | amount of free hard disk space | amount of RAM | speed of RAM | internet connection bandwidth]

15. What is a symptom of a hijacked browser?

    a. The browser settings have been reset.

    b. There are no websites found in the browser history.

    c. A different web page than the one that was expected appears.

    d. A pop-up warning appears.

16. [T | F] A hotspot provides wired network connectivity.

17. What would be the purpose of an Ethernet connection on a cable modem or a DSL modem?

    a. To connect a PC to the phone jack on the wall

    b. To connect a PC to the jack provided by the internet provider

    c. To connect a PC to the modem

    d. To connect the modem to the jack provided by the internet provider

18. A customer has a new laptop with wireless WAN capabilities; however, the software does not connect to the internet. What would you suggest to the customer?

    _____

    _____

19. What is the purpose of a browser extension?

    a. Enhances security

    b. Provides code that enhances the browser

    c. Provides the ability to run legacy software

    d. Doesn't retain history, cookies, or data collected during the session

20. List two ways mentoring can help in the IT field.

    _____

    _____

Exercises

Exercise 12.1 Exploring Internet Connectivity Options

Objective: To explore different methods of internet connectivity

Note: This exercise can be done with information found in the chapter or as an internet research exercise (which would require a device with internet access).

Procedure: Research and document two advantages and two disadvantages of each of the types of internet connectivity listed in Table 12.9.

TABLE 12.9 Advantages and disadvantages of internet connectivity types*

Type	Two disadvantages	Two advantages
56 kb/s modem		
Cable modem		

Type	Two disadvantages	Two advantages
DSL modem		
Fiber		
Satellite modem		
Wireless broadband		

* Answers may vary; possible answers are given.

Exercise 12.2 Exploring the Internet Options Window

Objective: To explore the different tabs in the *Internet Options* Control Panel

Note: This exercise can be done with information found within the chapter, as an internet research exercise (which would require a device with internet access), or on a Windows computer.

Procedure: Indicate in Table 12.10 the *Internet Options* Control Panel tab (General, Security, Privacy, Content, Connections, Programs, or Advanced) that would be used to perform each task.

TABLE 12.10 Internet Options Control Panel tabs to use for specific tasks

Task	*Internet Options* tab
Enable pop-up blocker	
Specify the maximum amount of disk space for temporary internet files	
Configure security certificates	
Disable an add-on	
Designate which program opens sound files on web pages	
Configure a proxy server	
Configure the version of HTTP supported	
Configure a VPN	
Designate the URL to be used as the home page	
Configure settings related to inside the corporate network (as opposed to the internet)	
Set the default font used for a web page	

Activities

Internet Discovery

Objective: To obtain specific information regarding a computer or its associated parts on the internet

Parts: Computer with internet access

Questions: Use the internet to answer the following questions.

1. Locate a cable modem website that explains how to increase speed on a cable modem. Write the URL where you found the answer as well as the recommendation.

   _____

   _____

   _____

   _____

2. Determine whether cable or DSL modems are supported in your area. If so, determine as many vendors as you can for these products.

   _____

3. Find one vendor of VDSL in the United States and write down the name of the vendor and the URL where you found the answer.

   _____

   _____

4. Find a website that provides cloud-based desktop virtualization. Write down pros and cons of its services and the URL of the vendor.

   _____

   _____

   _____

5. Determine how much a vendor charges to enable the mobile hotspot option or determine a phone/device that supports the mobile hotspot option. Document the price or phone model number and the URL where you found this information.

   _____

   _____

6. Find a vendor in your state that sells wireless broadband for a laptop. What type of technology does it use (USB, integrated, and so on)? Write the URL, the vendor name, the model number, and the cost.

   _____

Soft Skills

Objective: To enhance and fine-tune a future technician's ability to listen, communicate in both written and oral forms, and support people who use computers in a professional manner

Activities:

1. Divide the class into three groups—two groups that will be debating against one another and a third group of judges. The judges have 45 minutes to determine the rules of how the debate is to be conducted. During the same 45 minutes, the two debating groups should research material and plan a strategy for either cable modems or DSL modems. At the end of 45 minutes, the debate will start, and the judges will mediate with the rules they establish and present to the two teams before the debate begins. The judges, along with the instructor, determine which group proved its point the best.

   _____

2. Using whatever resources are available, research one of the following that has been assigned to you. Share the results with the class.

   What is the fastest DSL, cable, or analog connection within a 60-mile radius of your school?

   _____

   What is the most common type of internet connectivity for home users in your area?

   _____

   What is the most common type of internet connectivity among businesses in your area?

   _____

   What are the type and speed of the internet connectivity at your school?

   _____

   What are the type and speed of the internet connectivity at a college in your state?

   _____

   Which types of DSL services are available in your state?

   _____

   Which types of cable modem services are available in your state?

   _____

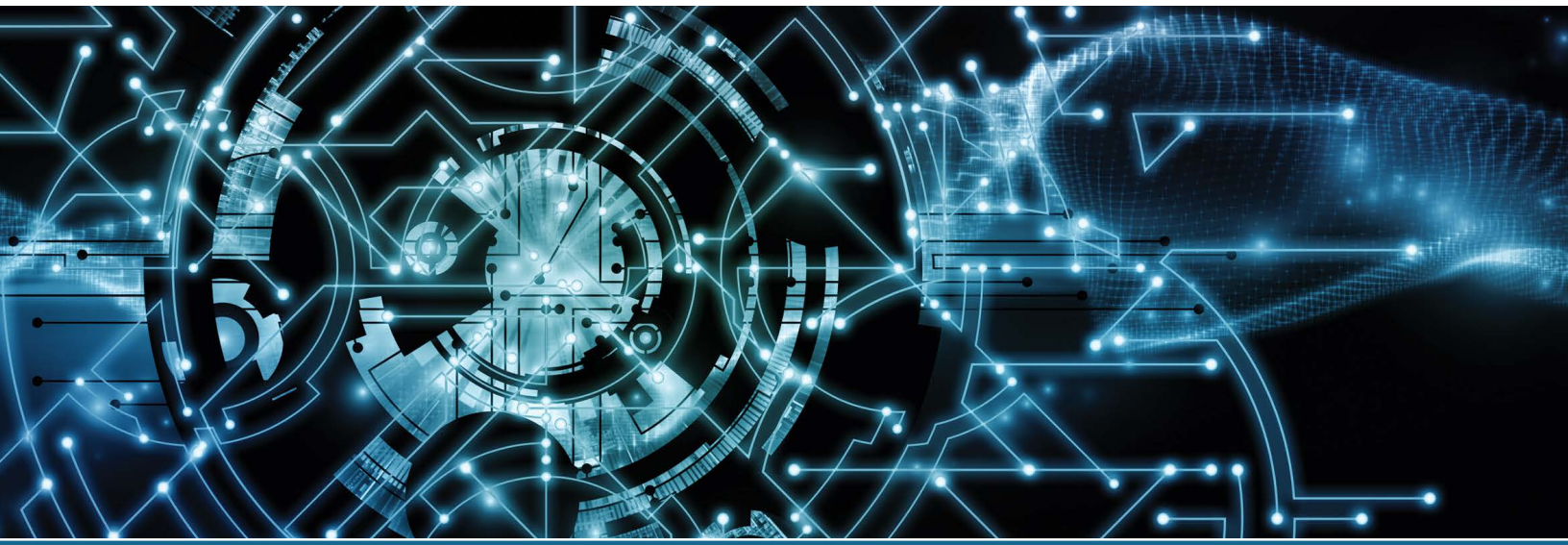
Critical Thinking Skills

Objective: To analyze and evaluate information as well as apply learned information to new or different situations

Activities:

1. In groups of three, research one of the following issues, as designated by the instructor. Share your findings with the other groups.
   - What are the pros and cons of changing the settings on a smartphone so that it can be a hotspot? Be prepared to share your findings.
   - What wireless broadband options are available from one of the most popular mobile phone providers in the area? Detail one option and its rate plan and cost. Be prepared to share your findings.
   - Determine the best internet connectivity rates for a small business in the area where your school is located. Share at least two competitors' rates, if possible. Detail the connectivity speeds and costs per vendor and be prepared to share your findings.
   - Find at least three VoIP solutions for home users. Prepare a chart that shows vendors, options, pros and cons of each option, costs, and customer ratings (and comments, if possible). Be prepared to share your findings.
2. In groups of two, write two problems that can affect analog/cable/DSL modems on two separate index cards. Give one problem to another class group and the other problem to a different class group. Your group will receive two index cards from two different groups as well. Solve the problems given to you, using any resource available. Share your group findings with the class.

13 Networking



In this chapter you will learn:

- To identify common network cables and connectors
- About Ethernet networks
- About the OSI and TCP/IP models, different networking protocols, differences between TCP and UDP, and important TCP or UDP port numbers
- To identify MAC, IPv4, and IPv6 addresses
- To set up wired and wireless networks
- Common network troubleshooting tools
- To configure and access a network printer
- Important network servers
- The basics of SDN
- To share data using a network
- How to be a proactive technician

CompTIA Exam Objectives:

- ✓ 1201-2.1 Compare and contrast Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) ports, protocols, and their purposes.
- ✓ 1201-2.2 Explain wireless networking technologies.
- ✓ 1201-2.3 Summarize services provided by networked hosts.
- ✓ 1201-2.4 Explain common network configuration concepts.
- ✓ 1201-2.5 Compare and contrast common networking hardware devices.
- ✓ 1201-2.6 Given a scenario, configure basic wired/wireless small office/home office (SOHO) networks.
- ✓ 1201-2.7 Compare and contrast Internet connection types, network types, and their characteristics.
- ✓ 1201-2.8 Explain networking tools and their purposes.
- ✓ 1201-3.2 Summarize basic cable types and their connectors, features, and purposes.
- ✓ 1201-3.5 Given a scenario, install and configure motherboards, central processing units (CPUs), and add-on cards.
- ✓ 1201-3.7 Given a scenario, deploy and configure multifunction devices/printers and settings.
- ✓ 1201-5.4 Given a scenario, troubleshoot common mobile device issues.
- ✓ 1201-5.5 Given a scenario, troubleshoot network issues.
- ✓ 1202-1.3 Compare and contrast basic features of Microsoft Windows editions.
- ✓ 1202-1.5 Given a scenario, use the appropriate Microsoft command-line tools.
- ✓ 1202-1.6 Given a scenario, configure Microsoft Windows settings.
- ✓ 1202-1.7 Given a scenario, configure Microsoft Windows networking features on a client/desktop.
- ✓ 1202-2.1 Summarize various security measures and their purposes.
- ✓ 1202-2.3 Compare and contrast wireless security protocols and authentication methods.
- ✓ 1202-2.10 Given a scenario, apply security settings on SOHO wireless and wired networks.
- ✓ 1202-3.3 Given a scenario, troubleshoot common mobile OS and application security issues.
- ✓ 1202-3.4 Given a scenario, troubleshoot common personal computer (PC) security issues.

Networking Overview

Networks are all around us. A few examples include the following:

- A network of roads and interstate highways
- A telephone network
- The electrical network that provides electricity to our homes
- The cellular network that allows cell phones/smartphones to connect to one another as well as to the wired telephone network and the internet
- The air traffic control network
- Your network of friends and family

A network as it relates to computers is two or more devices that have the capability to communicate with one another. A network allows computer users to share files; communicate via email; browse the internet; share a printer, modem, or scanner; and access applications and files. Networks can be divided into major categories based on the size and type of network. Table 13.1 describes these different networks.

TABLE 13.1 Types of networks

Network type	Description
Personal area network (**PAN**)	A PAN consists of personal devices such as keyboard, mouse, TV, cell phone, laptop, desktop, mobile device, and pocket video games that can communicate in close proximity through a wired or wireless network. A Bluetooth keyboard connected with a PC is an example of a PAN.
Local area network (**LAN**)	A LAN is a group of devices that can share resources in a single area, such as a room, home, or building. The most common LAN technology is Ethernet. The computers in a wired networked classroom are an example of a LAN.
Wireless LAN (**WLAN**)	WLANs are used in home and business networks and include devices such as laptops, tablets, smartphones, and smart home devices that transmit data through the air.
Metropolitan area network (**MAN**)	A MAN provides connectivity between sites within the same city and multiple LANs. It can be wireless or use fiber cabling. For example, multiple college campuses connected within a city may be connected to form a MAN.
Wide area network (**WAN**)	A WAN provides connectivity between sites on a large geographic scale. Two remote locations that have connectivity between them as part of the company network are a WAN.
Wireless WAN (**WWAN**)	A WWAN provides wireless connectivity for a larger geographic area, using a mix of technologies, such as cellular or long-range fixed wireless.
Wireless mesh network (**WMN**)	A WMN provides wireless connectivity that is especially good in emergency situations because WMNs pass data between peer radio devices and can be used over large distances.
Storage area network (**SAN**)	A SAN is a collection of storage devices that are used by multiple servers/network devices and centrally managed.

Let's go into a few of these network types a little deeper so the acronyms can bring visuals to your mind.

Bluetooth PAN

A PAN is a network that has components that are in close proximity to one another. The most common type of PAN that you know uses a technology called **Bluetooth**. Bluetooth devices include audio/visual products, automotive accessories, keyboards, mice, phones, game controllers, cameras, wireless cell phone headsets, sunglasses with radios and wireless speakers, and other small wireless devices.

Bluetooth works in the 2.4 GHz range, similarly to business wireless networks. Traditional Bluetooth has three classes of devices (1, 2, and 3) that have a range of less than 30 feet (less than 10 m), 33 feet (10 m), and 328 feet (100 m), respectively, and a maximum transfer rate of 24 Mb/s. Bluetooth version 5 introduced a second type of Bluetooth called Bluetooth Low Energy (BLE) that supports longer distances for speeds up to 2 Mb/s. Vendors tout ranges of up to 800 feet (243 m), although such distances are not defined in the standard. BLE is good for Internet of Things (IoT) devices such as sensors and household controls for cameras, a stove, or lights. The BLE standard is not compatible with the classic Bluetooth standard, but smartphones or other devices might have the capability of using both.

Bluetooth supports both data and voice transmissions. Up to eight Bluetooth devices can be connected in a piconet or PAN (a small network). Bluetooth has always had security features integrated into it, including 128-bit encryption (for scrambling of data). Figure 13.1 shows a Bluetooth connection between a cell phone mounted on a runner's arm and a fitness device on the runner's wrist so that the phone app can be used to configure the device and download the activity data.

FIGURE 13.1 Bluetooth connectivity

A Bluetooth network provides computer-to-computer connectivity between Bluetooth devices. Each computer must support a PAN in order to join the network. In Windows 11, use *Settings* > *Bluetooth & devices* > *Bluetooth*. Review Chapter 10, "Mobile Devices," for complete installation steps.

LANs

LANs can be wired or wireless, but a LAN that is wireless is called a WLAN. Let's focus on the wired type first. A LAN is two or more devices connected via wiring. You can connect two devices with a cable between their NICs to form a LAN, but most LANs today are Ethernet LANs. An **Ethernet** LAN has a central device called a hub or a switch. An Ethernet cable connects an RJ45 port on the network device to the switch or hub, as shown in Figure 13.2. The hub or switch typically has 2 to 48 ports on the front.

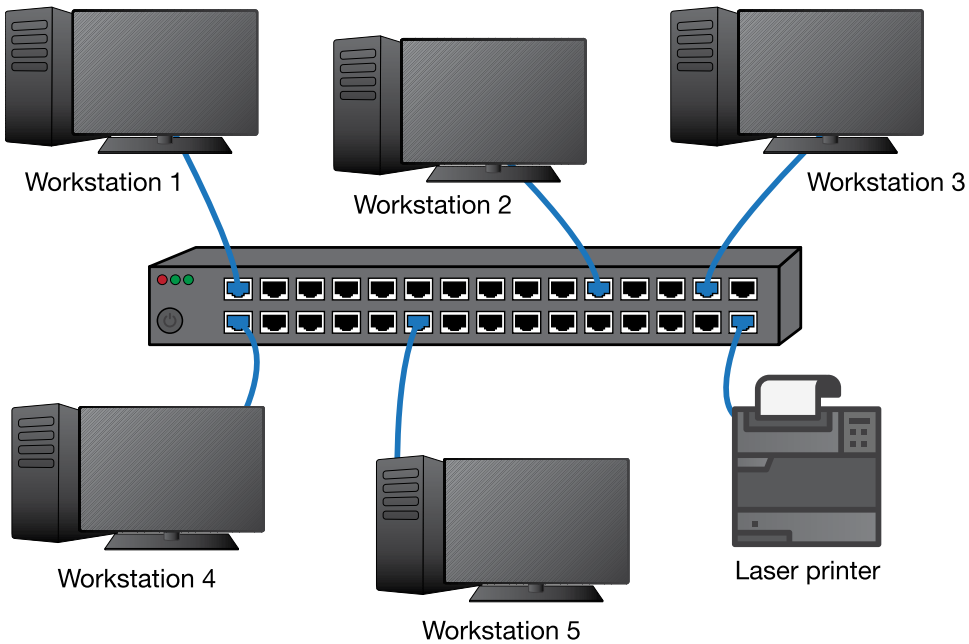


FIGURE 13.2 Ethernet LAN

A hub is not as intelligent as a switch. A switch takes a look at each data frame as it comes through the switch. A hub cannot do this. You sometimes have to look at the model number to tell the difference between a hub and a switch because they are similar in appearance.

TECH TIP

Why a switch is better than a hub

When a workstation sends data to a hub, the **hub** broadcasts the data out all ports except for the port that received the original data (the port the data came in on). A better solution is a **switch**, which keeps a table of addresses. When a switch receives data, it looks up the destination MAC address (an address burned into a NIC) in the switch table and forwards the data out the port for which it is destined.

When a hub is used, collisions may occur because two devices can place data onto the network at the same time. Every device has to delay in sending data for a period of time, and then transmissions can reoccur. This isn't an efficient use of bandwidth. A switch eliminates collisions and therefore is a better network device to use.

Switches can be either managed or unmanaged. A **managed switch** has an IP address assigned and can be configured, modified, and monitored through a corporate network. An **unmanaged switch** simply connects devices so that they form a network. A switch in a home or small business wired network would likely be an unmanaged switch.

TECH TIP

Ethernet networks are physically wired in a star

The most common network topology used today is the star topology, which is used with Ethernet networks.

In a star topology (refer to Figure 13.2), each network device has a cable that connects between the NIC on the device and the hub or switch. If one computer or cable fails, all other devices continue to function. However, if the hub or switch fails, the network goes down.

Star topologies are easy to troubleshoot. If one network device goes down, the problem is in the device, cable, or port on the hub or switch. If a group of network devices goes down, the problem is most likely in the device that connects them together (the hub or switch).

Table 13.2 lists the different types of Ethernet networks. In the term 100BaseT, *100* means that the network runs at 100 Mb/s. The *T* at the end of 100BaseT means that the computer uses twisted pair cable. The *1000* in 1000BaseT means that 1,000 Mb/s is supported. *Base* means that the network uses baseband technology, which means data is sent over a single channel on a single wire. In contrast, broadband, which is used in cable TV systems, allows multiple channels using different frequencies to be carried over a single wire.

TABLE 13.2 Ethernet standards

Ethernet type	Description
10BaseT	10 Mb/s over Cat 3 or Cat 5 UTP cable
100BaseT	100 Mb/s over Cat 5 or higher UTP cable
1000BaseT	Also known as Gigabit Ethernet; 1,000 Mb/s or 1 G/ps over Cat 5e or higher UTP cable
1000BaseSX	1 Gb/s using multimode fiber (a type of cable made of plastic or glass that carries data using light)
1000BaseLX	1 Gb/s using single-mode fiber
2.5G/5GBaseT	2.5 or 5 Gb/s over Cat 6 or higher cable
10GBaseSR	10 Gb/s over multimode fiber
10GBaseLX4	10 Gb/s over multimode or single-mode fiber
10GBaseLR	10 Gb/s up to 6.2 miles (10 km) using single-mode fiber
10GBaseER	10 Gb/s up to 24.85 miles (40 km) using single-mode fiber
10GBaseT	10 Gb/s over UTP (Cat 6 or higher) or STP cable
25GBaseLR	25 Gb/s over fiber up to 6.2 miles (10 km)
25GBaseER	25 Gb/s over fiber up to 24.85 miles (40 km)
40 Gigabit Ethernet	40 Gb/s over single-mode fiber or 100 feet (30 m) using copper
100 Gigabit Ethernet	100 Gb/s over multimode or single-mode fiber

LANs typically are based on one of two models: a workgroup model or a domain model. A **workgroup** LAN is used in a wired home or small business network. A **domain** is used in a corporate environment and usually contains multiple networks. A domain typically contains servers, databases, and shared resources that are centrally managed. Table 13.3 compares the two types.

TABLE 13.3 Workgroup and domain network characteristics

Workgroup	Domain
Typically fewer than 20	Typically more than 20 devices
All devices are usually on one network	Contains multiple networks
Each network device must have user accounts configured	User accounts are centrally managed
More of a security risk	Security is centrally managed, with security policies applied

Workgroup	Domain
Might contain a web server, file server, or network-attached storage (NAS) but may have no servers	Storage is centralized, and multiple servers are usually involved
Easier to implement changes	Any change requires planning
Each PC uses a workstation OS	Each server requires a network operating system (NOS)
Requires fewer resources	Network resources are centralized, located in another location, cloud-based, or a combination of these

Figure 13.3 shows the type of wired and wireless connectivity used in a workgroup. Figure 13.4 shows the kind of connectivity that can be used in a network domain.

FIGURE 13.3 Wired and wireless connectivity in a workgroup network

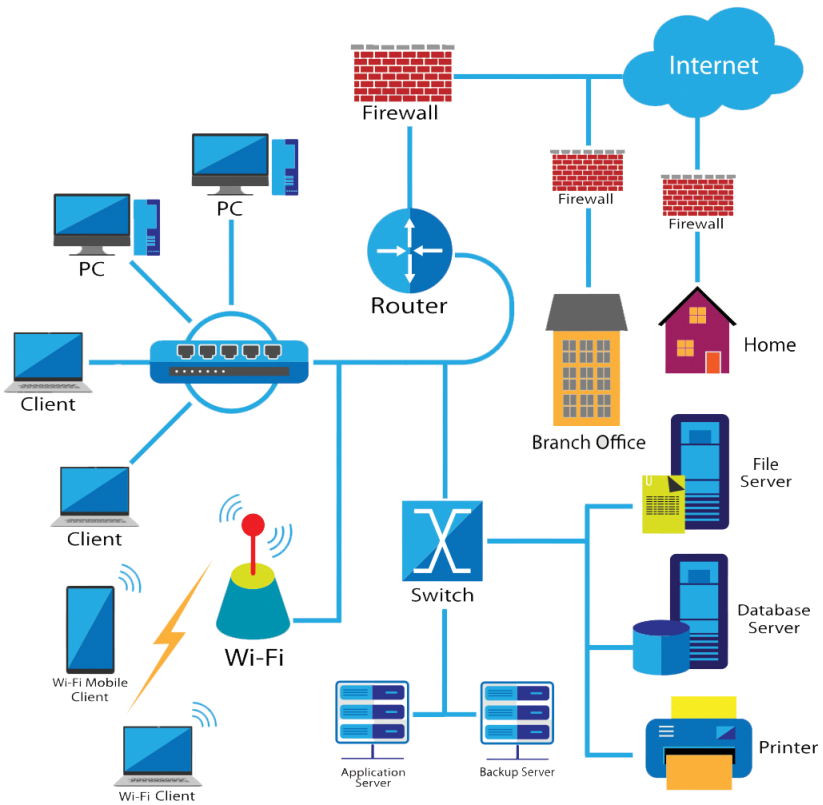


FIGURE 13.4 Domain network

Figure 13.5 shows the type of equipment found in a network operations center (NOC) that could be used with a domain-based network.

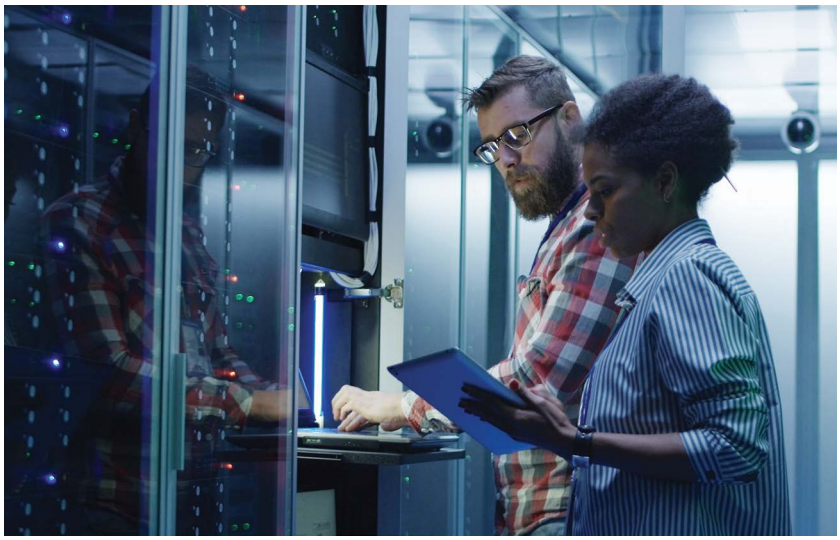


FIGURE 13.5 Network operations center (NOC)

When connecting to a wired LAN using a Microsoft operating system, you are typically presented with three or four choices, depending on the OS version you are using: workgroup network, guest network, public network, private network, or domain. A home or work environment is considered a **private network**, and private addresses are used. Characteristics of your computer can be seen or discovered by other devices. A **public network** is a network that you might use in a community library or at a hotel. Each user uses a network profile, which helps Windows determine the appropriate security and sharing settings for the current network connection. The option chosen defines, to some extent, the type of network you could configure. Table 13.4 describes the basic choices.

TABLE 13.4 Windows network options

Network option	Description
Workgroup	Used to configure a device participating in a small home or business network. Use the *System* Control Panel to select this option.
Domain	Used to configure a device in an enterprise corporate environment where policies are enforced and deployed. Use the *System* Control Panel to select this option.
Private	Used when you are on a trusted network such as a home or corporate network. Use *Network & Internet* > *Ethernet* Settings option to select a wired network or select the wireless network > *Properties* option.
Public	Used to configure a device on a network where the other devices are unknown. Network discovery is disabled. Use the *Network & Internet* > *Ethernet* Settings option to select a wired network or select the wireless network > *Properties* option.

WLANs

Wireless local area networks (WLANs), commonly known as Wi-Fi networks, are widely used in homes and businesses to connect multiple devices wirelessly. WLANs connect wireless devices like phones, tablets, laptops, TVs, smart speakers, and other devices that using a specific range of radio frequencies (see Figure 13.6).

FIGURE 13.6 WLAN connectivity

SANs

A storage area network (SAN) has a large number of hard drives mounted in a unit that attaches to the network, and that storage is centrally managed. Figure 13.7 shows a person installing a server, and behind him is a SAN.

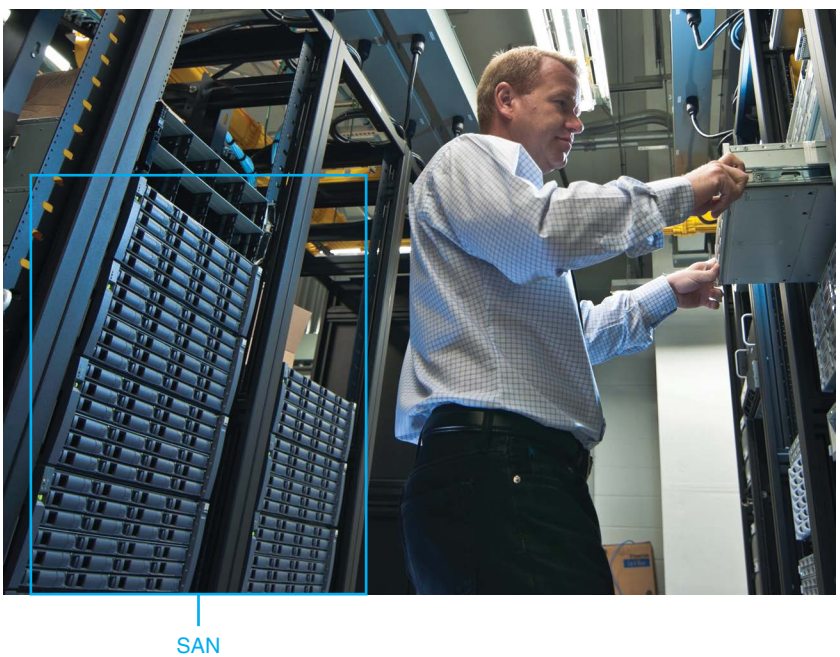


FIGURE 13.7 Storage area network (SAN)

If a PC needed to access data on a SAN, it could do so through the normal LAN, but the PC might also contain a special network interface card (NIC) to connect to the SAN **iSCSI** or Fibre Channel (**FC**) connections (look back at Figure 2.40 in Chapter 2, "Connectivity," to see fiber connectors), as shown in Figure 13.8. Connectivity between a SAN and servers also is also accomplished by using these connectivity methods, as shown in Figure 13.9.

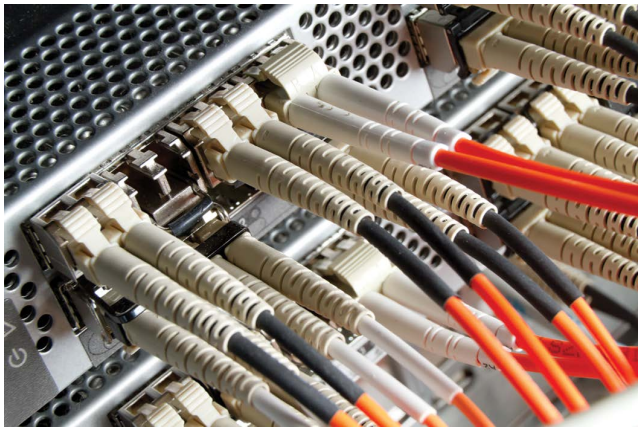


FIGURE 13.8 SAN fiber connectivity

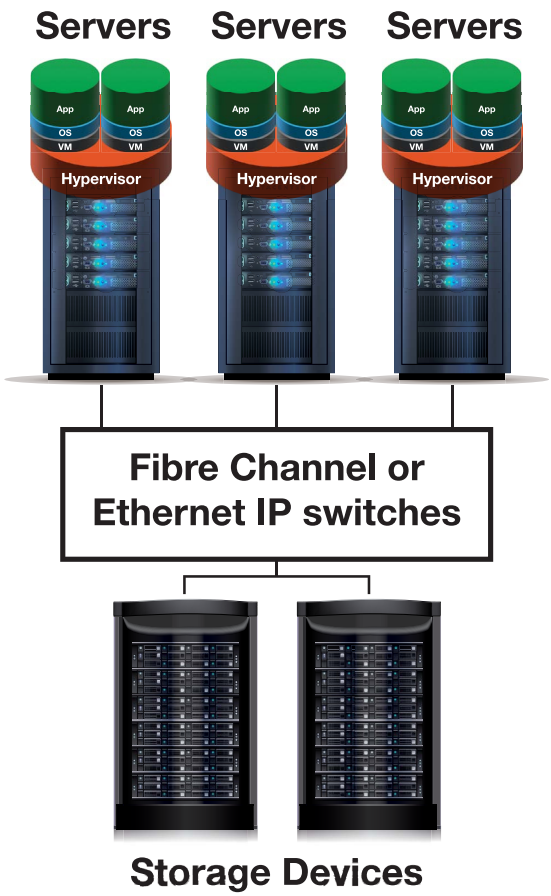


FIGURE 13.9 SAN connectivity to servers

Networks are essential infrastructure in modern businesses and homes. Understanding network devices and their functions is crucial for any IT professional, regardless of their specific career path. This knowledge forms the cornerstone of effective technology management and problem solving in today's interconnected digital environments. No matter what IT position you are aspiring to, you will have to deal with networking concepts.

Network Media Overview

A network requires some type of medium to transmit data. This medium is normally some type of cable or air. Air is used in wireless networking when data is sent over radio frequencies, using radio,

microwave, and electromagnetic signals. The most common types of cable are twisted pair copper and fiber-optic cable, although some older networks used coax cable. Video networks also use coax. (Refresh your knowledge of coax and fiber-optic cable concepts by reviewing Chapter 2.)

Copper Media

Copper media is the most common type of cabling used to connect devices to a network. Copper media comes in two major types: twisted pair and coaxial. Let's dive into each type.

Twisted Pair Cable Overview

Twisted pair cable comes in two types: shielded and unshielded. The acronyms used with this type of cable are STP (shielded twisted pair) and UTP (unshielded twisted pair). The most common type of copper media used with computer networking and phone cabling is **UTP** cable. **Twisted pair cable** has four pairs of conductors entwined around each other—hence its name. Figure 13.10 shows the physical properties of an unshielded twisted pair cable.

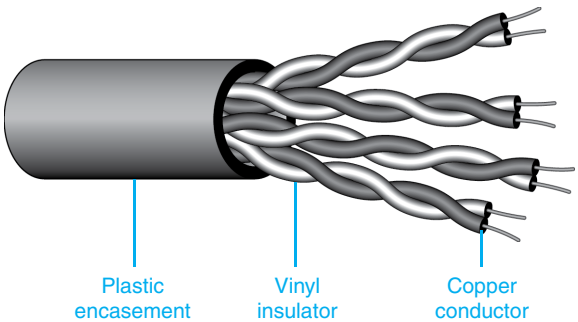


FIGURE 13.10 UTP cable

STP cable has extra foil that provides more shielding. Shielded twisted pair cable is used in industrial settings, such as factories, where extra shielding is needed to prevent outside interference from adversely affecting the data on the cable. It is also used with **direct burial cable** and underground outdoor cabling that has waterproofing and extra insulation so tubing or pipes are not required.

UTP cable is measured in gauges. The most common sizes of UTP cable are 22-, 23-, 24-, and 26-gauge unshielded twisted pair cables. UTP cables come in different specifications called categories. The most common are categories 5e, 6, 6a, and 7. People (and cable manufacturers) usually shorten the name *Category* to *Cat*, so Category 6 is spoken of as Cat 6. The categories determine, in part, the speed of a network. Table 13.5 describes some of the categories of UTP cable. You can also refer to Table 2.6 in Chapter 2 for a recap of the major Ethernet characteristics.

TABLE 13.5 UTP cable categories

Category	Description
Cat 5e	Known as Cat 5 enhanced. Can be used with 10BaseT, 100BaseT, and 1000BaseT (Gigabit) Ethernet networks. Cables are rated to a maximum of 328 feet (100 m). Supports frequencies up to 100 MHz per pair (speeds up to 1 Gb/s).
Cat 6	Supports 10 Gigabit Ethernet better than Cat 5e but uses larger-gauge (thicker) cable. Note that the 10 Gb/s standard has a shorter distance of 180 feet (55 m). Supports frequencies up to 250 MHz per pair (speeds up to 1 Gb/s). More stringent specifications to prevent crosstalk (signals from one wire going over into another wire). Commonly used in industry.
Cat 6a	Supports 10GBaseT Ethernet and frequencies up to 500 MHz (speeds up to 10 Gb/s with cabling at a shorter distance of 180 feet/55 m).

Category	Description
Cat 7	Backward compatible with Cat 5e and 6. Supports 10G/40GBaseT Ethernet and frequencies up to 600 MHz (speeds up to 40 Gb/s). Cat 7 commonly uses shielded twisted pair (STP) cabling or variations of it such as foiled twisted pair (FTP), shielded foil twisted pair (SFTP), or shielded screened twisted pair (SSTP).
Cat 8	Supports 25G/40GBaseT Ethernet and allows speeds up to 40 Gb/s using only STP at time of press. Used in data centers and server rooms.

A special type of UTP or STP cable is plenum cable. A plenum is a building's air circulation space for heating and air-conditioning systems. **Plenum-rated cable** is treated with Teflon or some other fire-retardant materials to reduce its susceptibility to fire. Plenum cable is less smoke producing and less toxic when burning than regular networking cable.

The alternative to plenum cable is polyvinyl chloride (**PVC**) cable, which has a plastic cable insulation or jacket. PVC cable is cheaper than plenum cable, and it can have flame retardant added to make the cable flame retardant if necessary for compliance with building codes. PVC is usually easier to install than plenum cable.

Terminating Twisted Pair Cable

Twisted pair cable has an RJ45 connector that has a tang (a little plastic clip) to securely insert the connector into an RJ45 jack, as shown in Figure 13.11. Tangs frequently get broken, technicians must often make Ethernet cables as part of the job. If a tang breaks off, the RJ45 connector is cut off, and a new RJ45 connector is attached. This is known as *terminating* a cable. To create a new cable, you purchase a spool of twisted pair cable, cut off a suitable length, and add an RJ45 connector to each end.

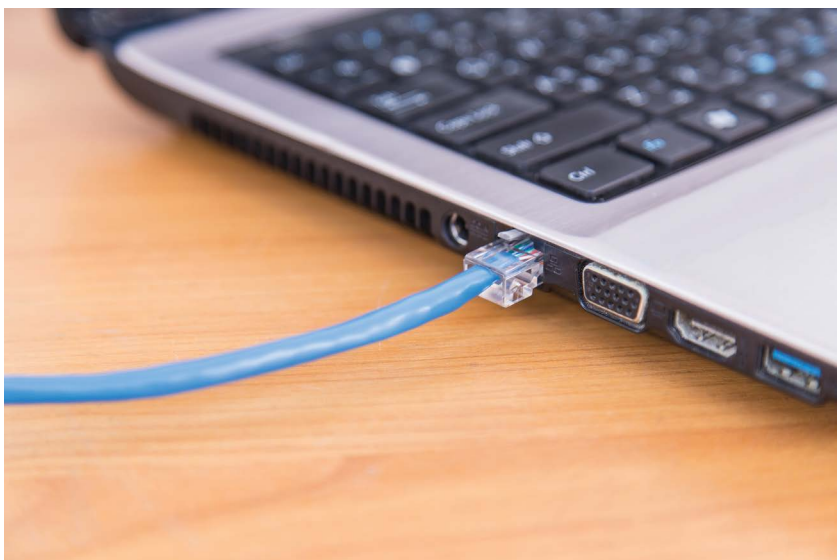


FIGURE 13.11 UTP connector with tang

Twisted pair cable uses either an **RJ45** (8 conductor) or **RJ11** (4 conductor) connector. RJ45 connectors are used with network cabling. Twisted pair cable used with networking has eight copper wires that are grouped in colored pairs (see Figure 13.12). Each pair is twisted together to prevent crosstalk, which occurs when a signal on one wire interferes with the signal on an adjacent wire.

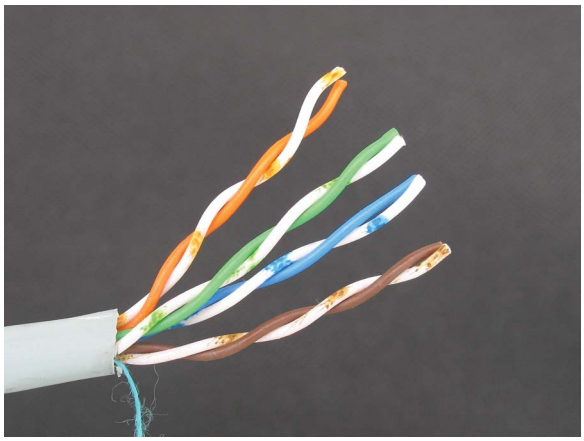


FIGURE 13.12 UTP color pairs

To connect a computer to a switch or network wall outlet, a **straight-through cable** (also known as a patch cable) is used. Both ends of the cable would be wired to the **T568A** standard, or both ends of the cable would be wired to the **T568B** standard (the more popular method). When connecting two computers (or two switches) together, a **crossover cable** is used. A crossover cable has one RJ45 connector created to the T568A standard and the other end created to the T568B standard. Figure 13.13 shows the color codes associated with the T568A and T568B standards. Figure 13.14 shows the location of pin 1 on an RJ45 port and on a connector. Notice in both figures how the tang is pointing down toward the floor.

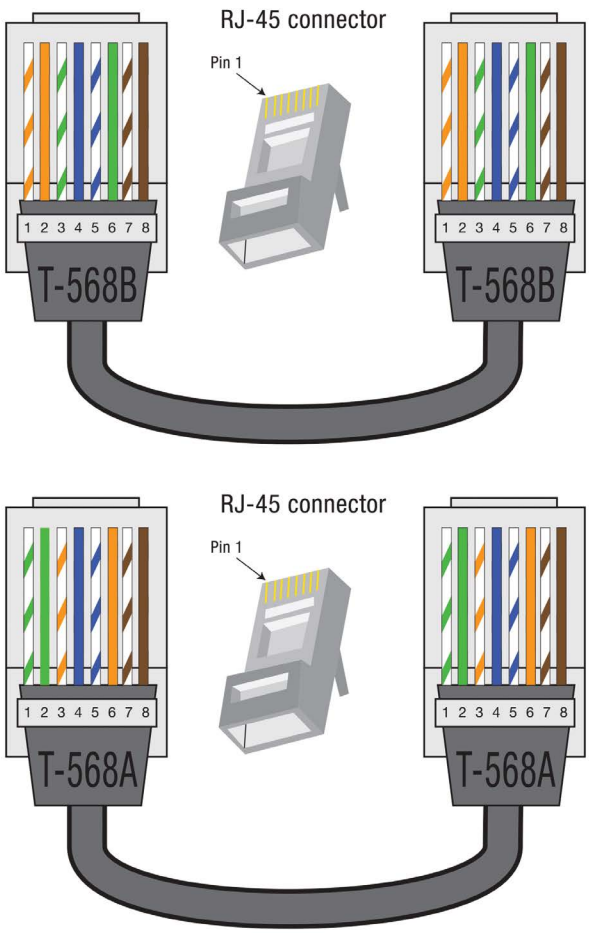


FIGURE 13.13 UTP cabling by color and wiring standards

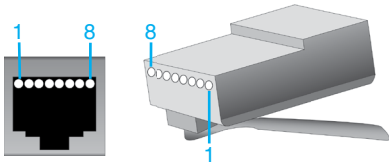


FIGURE 13.14 Pin 1 on an RJ45 port and connector

TECH TIP

Networking two PCs without a switch or hub

If you have two PCs with Ethernet NICs installed, you can connect them with a crossover cable attached to the RJ45 jack on each NIC.

To start creating your own cable, the plastic encasement must be stripped away with a **cable stripper** (also known as a wire stripper and shown in Figure 13.15) to expose approximately 1 inch (2 cm) of the vinyl insulator that covers the copper conductors. Look back at Figure 13.12 to see the exposed conductors after the insulator has been stripped.

FIGURE 13.15 Cable stripper

A **crimper** is a specialized tool used to attach RJ45 connectors to network cables. Most crimping tools are designed with additional features to support cable preparation, typically including a built-in blade for stripping cable insulation. In the first photo in Figure 13.16, the cable is being stripped of the plastic encasement. It's important not to cut into the vinyl insulator. The second photo in Figure 13.16 shows the vinyl insulator stripped away.

FIGURE 13.16 Crimper used as a wire stripper and stripped UTP cable

After the plastic encasement is removed, untwist the cable pairs and place them in the proper color order. Wiggle each cable back and forth to make it more pliable. Cut the cables straight across, leaving 1/2 inch (1 cm) of cable. Insert the cables into the RJ45 connector in the correct color order. Ensure that the tang points toward the floor.

A common mistake when making a cable is not pushing the wires to the end of the RJ45 connector. Before crimping, look at the end of the RJ45 connector. You should see each wire jammed against the end of the RJ45 connector, and you should see what looks like a set of eight gold eyes staring at you when you turn the connector end toward you to verify that the conductors are pushed far enough into the connector before crimping.

Another check to perform before crimping is to ensure that the plastic encasement is inside the RJ45 connector. You do not want the vinyl insulator outside the connector, or data errors can occur. Notice in Figure 13.17 how the blue plastic encasement is in the wider part of the RJ45 connector. No unprotected wires are outside the plastic connector.

TECH TIP

Push the cable firmly into the jack

It is important to fully insert a UTP cable into an RJ45 jack and in the standardized color order. A common mistake new technicians make is putting on the RJ45 connector upside down.

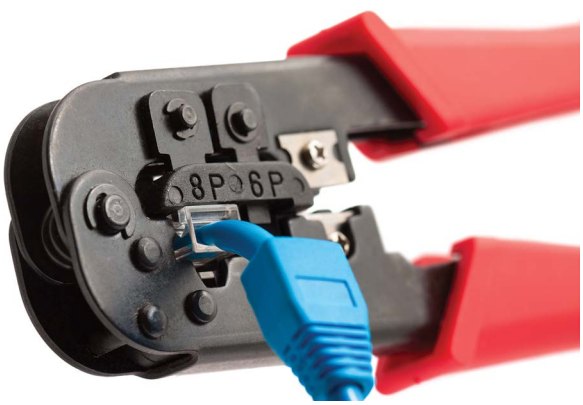


FIGURE 13.17 Crimping an RJ45 connector

When you have verified the color order, ensured that the eight gold connectors are pushed to the end, and verified the plastic encasement inside the RJ45 connector, you are ready to crimp. Crimping involves carefully inserting the RJ45 connector into the crimper (while keeping the wires pushed firmly into the connector) and pressing the crimper handles together firmly until the cable clicks and releases. Figure 13.17 shows a store-bought Ethernet cable that probably had a broken tang and that has a protective sleeve that normally is positioned over the plastic part of the RJ45 connector. You must move the sleeve back before you can cut off the damaged RJ45 connector and replace it. You then slide the sleeve back over the RJ45 connector when crimping is complete.

After crimping, you must use a **cable tester** to ensure that the cable is ready for use. Figure 13.18 shows a cable tester. Plug one end of the cable into the RJ45 jack on the main tester piece (yellow case) and the other end into the RJ45 cap. Each cable tester is different, so review the instructions, if necessary.

FIGURE 13.18 Cable tester

Twisted Pair Cable in the Corporate Environment

With twisted pair cable, all network devices connect to one central location, such as a patch panel, hub, or switch. Refer to Figure 13.2 to see how straight-through cables connect each network device to a switch. In a corporate environment, a patch panel is used. A **patch panel**, which mounts in a network wiring rack, has network ports on the front of it and wiring connected to the back of it to provide network connectivity. In Figure 13.19, the first photo shows the front of the patch panel, and the second photo shows the back.

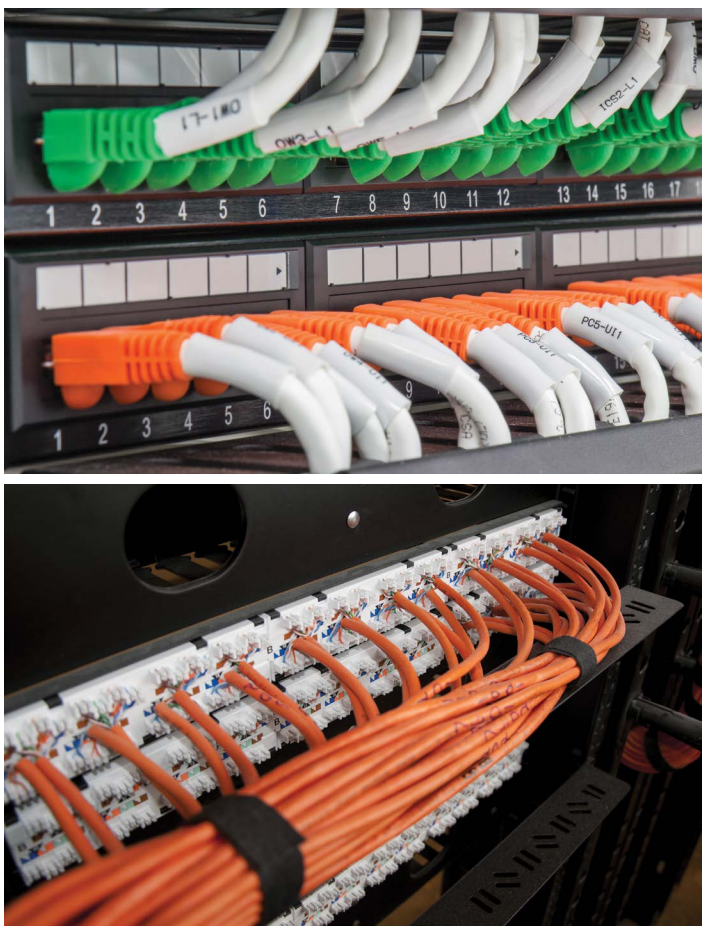


FIGURE 13.19 Front and back of a patch panel

A UTP cable connects from a network device to an RJ45 wall jack. That wall jack has UTP cabling (see Figure 13.20) that goes from the back of the wall jack to the back of a patch panel, as shown in Figure 13.21. A straight-through UTP patch cable connects from a port on the front of the patch panel to a switch located in the same network rack. Figure 13.21 also shows the cabling from PCs to a switch in a corporate environment.

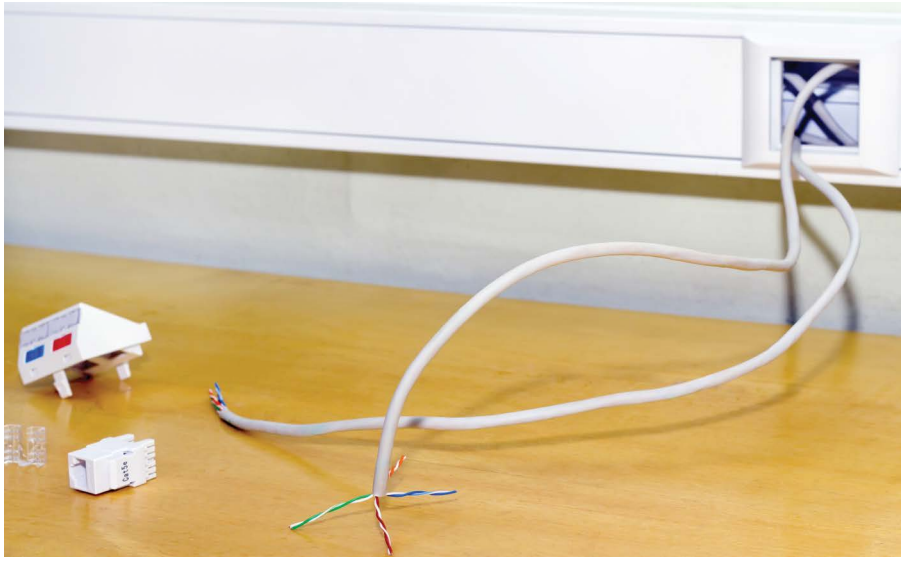


FIGURE 13.20 Network wall jack

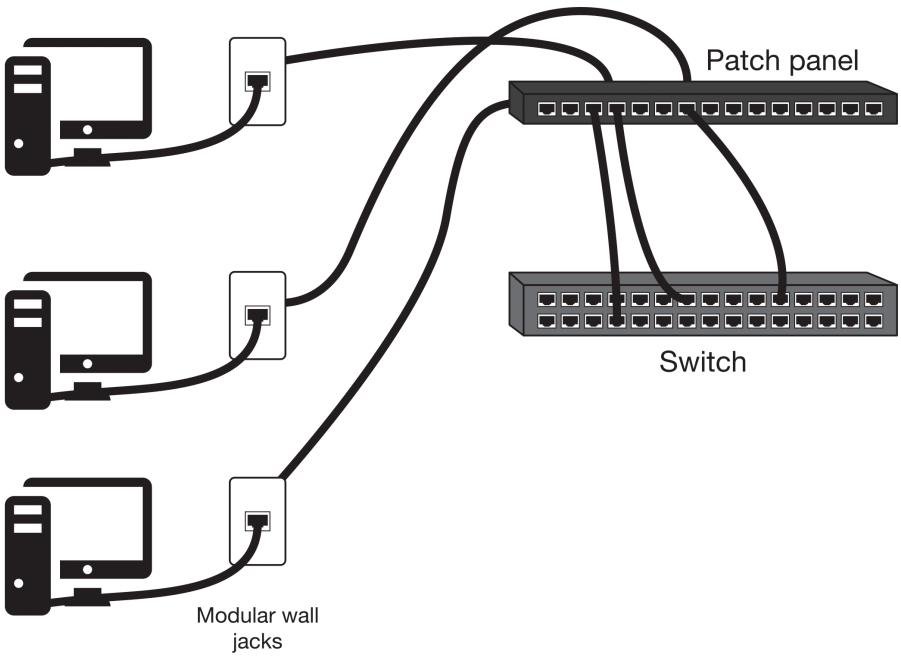


FIGURE 13.21 Corporate network connectivity from PCs to a switch

Ethernet cabling from the end device to the switch normally consists of three runs: (1) the cable from a patch panel to the wall at a maximum of 295 feet (90 m), (2) the 16-foot (5 m) maximum patch cable from the wall to a network device, and (3) a 16-foot (5 m) maximum cable from a patch panel to a switch. The total length of cable from device to patch panel can be 328 feet (100 m).

TECH TIP

Label both cable ends

When installing any type of network cable, you should label both ends with a unique identifier that normally includes the building and/or room number.

Power over Ethernet (PoE)

Corporate phones, IP cameras, projectors, wireless access points, and even audio systems or monitors can be powered through a technology called Power over Ethernet (**PoE**). The different standards for PoE are summarized in Table 13.6.

TABLE 13.6 PoE standards

Common name	IEEE standard	Description
PoE Standard (Type 1)	802.3af	2 pairs of UTP provide up to 15.4W of power to a port and 12.95W and 48V to power a device such as a voice over IP (VoIP) phone, wireless AP, or camera.
PoE Plus (PoE+ or Type 2)	802.3at	4 pairs of UTP provide up to 30W of power to a port and 25.5W and 50V to 57V to power a device such as an alarm system or a motion-tracking cameras.
PoE++ (Type 3)	802.3bt	4 pairs of UTP provide up to 60W of power to the port and 51W and 50V to 57 V to power a device such as a video phone or a door access reader.
PoE++ (Type 4)	802.3bt	4 pairs of UTP provide up to 100W of power to the port and 71W and 52V to 57 V to power a device such as a monitor, laptop, or point-of-sale register.
PoDL (Power over Data Lines)	802.3bu	2 or 4 pairs of UTP provide 0.5W to 50W to 12V, 24V, or 48V sensors and cameras in automobiles. Also known as Single-pair Power over Ethernet (SPoE).
POH (Power over HD-Base-T)	802.3at	4 pairs of UTP provide up to 100W of power to the port and 100W and 52V to 57 V to power a device due to the end device being able to determine cable length and draw.

Power over Ethernet (PoE) can be implemented using several methods. A **PoE switch** is a network switch with built-in PoE capabilities that is capable of providing power and data transmission through the same Ethernet cable. Another option is a PoE patch panel, which serves as a centralized connection point that can distribute both power and data to multiple devices and that is often used in larger network installations. A third method involves using a **PoE injector**, also known as a power injector, which is a standalone device that adds voltage to a standard Ethernet cable, enabling PoE functionality for non-PoE switches or individual devices. Figure 13.22 demonstrates these concepts.

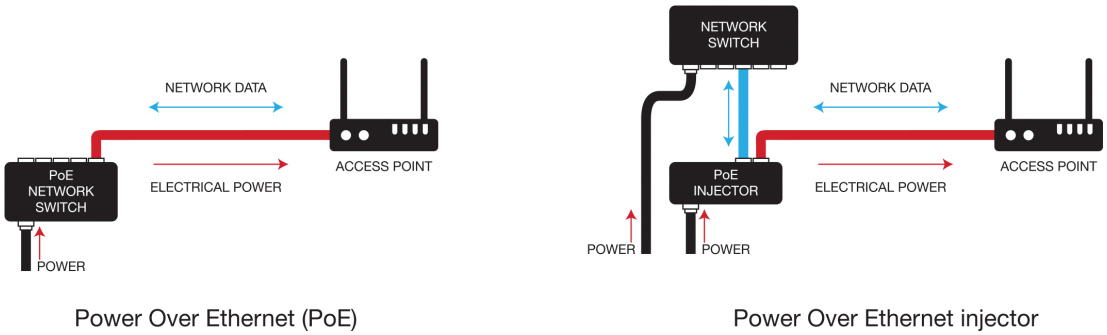


FIGURE 13.22 Access point with PoE and PoE injector

Ethernet over Power

One way to create an Ethernet network without switches, hubs, or a crossover cable between two PCs is to use electrical outlets. **Ethernet over Power** (EoP) (also known as powerline communication) sends network data to EoP modules plugged in to power outlets to extend Ethernet networks. Some EoP modules support wireless connectivity as well. To use EoP, you need a minimum of two EoP modules. One module plugs in to a power outlet near the internet modem. An Ethernet cable attaches from the internet modem to the EOP module. A second EoP module connects somewhere else in the home or business, near a device that has trouble connecting to the internet due to the absence of Ethernet wiring or weak wireless RF signal. Then, when you attach an Ethernet cable between the stranded device and the EoP module, the device has internet access. Figure 13.23 shows this concept.

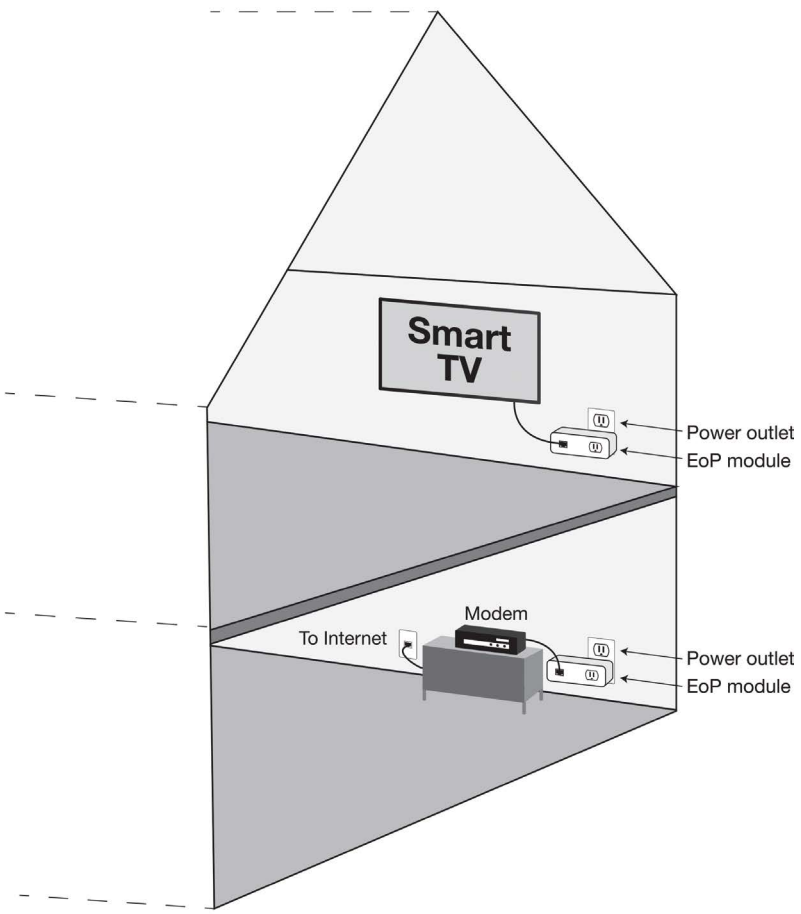


FIGURE 13.23 Ethernet over Power connectivity

Protecting Your Network and Cable Investment

Quite a bit of money is spent on network cabling. IT professionals are charged with protecting this investment as well as ensuring that cabling does not cause personal safety risks. Network devices should be locked in a secure room or cabinet when possible. Figure 13.24 shows network cabinets that have network devices as well as cabling installed inside them.

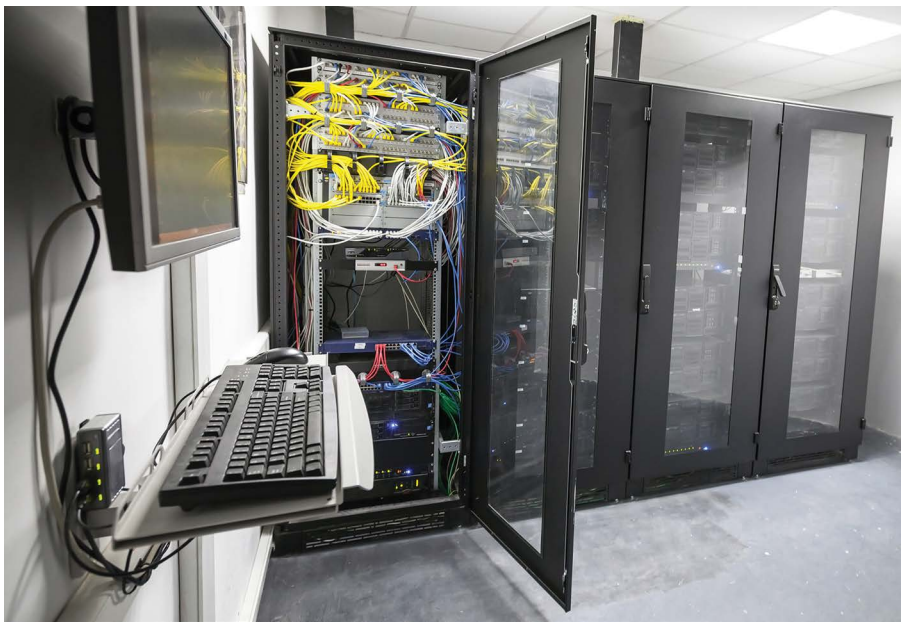


FIGURE 13.24 Network cabinets

Network racks, such as the one shown inside the cabinet in Figure 13.24, require grounding so that all of the equipment mounted to the rack is the same potential. Electrical codes indicating how this is done vary by country and state. On painted racks, it is important to remove the paint from a small section and attach a ground cable that connects from the rack to building ground or an electrical panel; electricians commonly do this. You might also see a ground wire connected to a UPS that provides backup power to network equipment.

Network cable can be pulled through walls and over ceilings but should be installed in conduit or raceways (mesh racks or ladder racks that keep the cable away from other things), if possible. A professional **cable management system** can help keep network cables organized. Ensure that network cabling is not a trip or other safety hazard in any location. Of course, this increases the cost of the network installation, but it protects the network cabling and people. Figure 13.25 shows a network closet that is typical of the closets in many companies. Figure 13.26 shows a network wiring rack with a cable management system.

A ladder rack is a network cable accessory that holds multiple cables going across a room or from one side of a room to a network rack that is located away from the wall. Figure 13.27 shows a network cable ladder rack with bundles of cables.

FIGURE 13.25 Messy network wiring rack

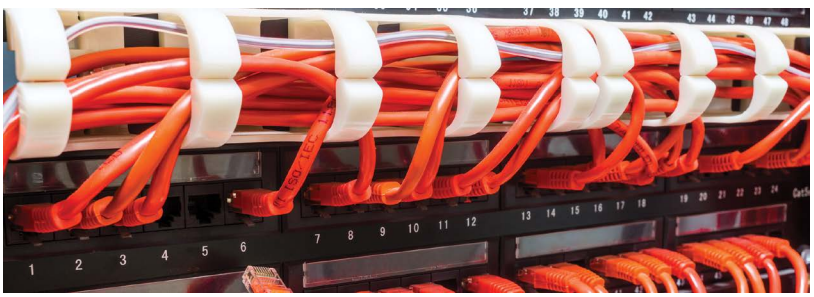


FIGURE 13.26 Cable management system

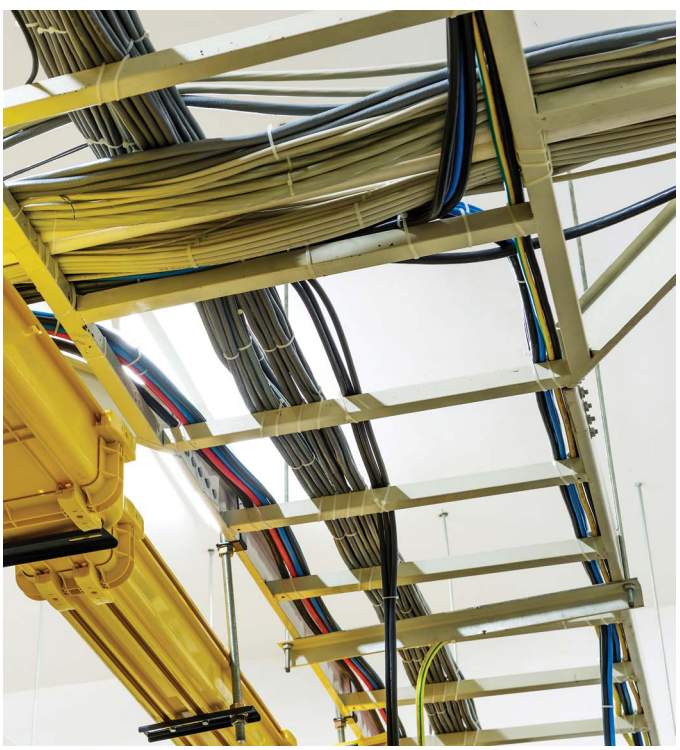


FIGURE 13.27 Network cable ladder racks

Network Cabling and Troubleshooting Tools

Table 13.7 and Figure 13.28 describe and show network-related tools used in making cable and troubleshooting cable issues.

TABLE 13.7 Network cabling tools

Tool	Description
Cable stripper	Removes outer jacket on UTP cables. (Refer to Figures 13.15, 13.16, and 13.28.) Also called a wire stripper.
Cable tester	Checks coaxial and UTP cable (depending on the model). (Refer to Figures 13.18 and 13.28.)
Crimper	Permanently attaches an RJ45 or RJ11 connector to cable. (Refer to Figures 13.16 and 13.17.)
Loopback plug	Attaches to a specific port and tests the port or communications circuitry to see if a signal can be sent out and received. If the test succeeds, the port and communications circuits are good.
Multimeter	Takes voltage, resistance, and current readings. Can be used to check whether data racks are grounded. (Refer to Figures 5.21, 5.22, and 5.23 in Chapter 5, "Disassembly and Power.")
Punchdown tool	Connects network cables to a patch panel (see Figures 13.28, 13.29, and 13.30) or phone cables to a **punchdown block** (see Figure 13.30). If there is a low/high setting, use the low setting for phone and high for network cables.
Tone generator and toner probe	Used to identify cables when they are not labeled or when they are labeled incorrectly. A **tone generator** connects to a cable or is inserted into a network jack. The tone generator injects a tone down the cable. The **toner probe** (see Figure 13.28) is touched to the other end of a cable to identify it.
Network tap	Monitors/copies network data and can be a hardware device, as on some corporate switch models, or software. If hardware, think of a T-shaped device. The device typically has two ports that are used to allow the data to come in and then flow out. One or more additional ports are used to send the data that flowed through the first two ports out to a device that captures the data for further analysis. Also known as a breakout tap.

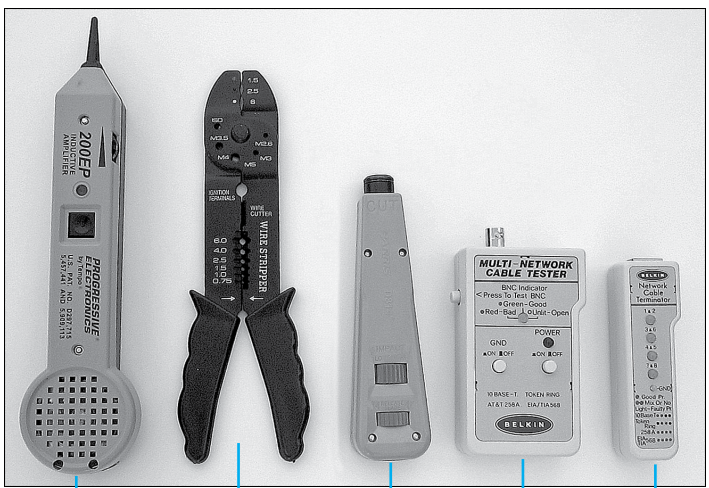


FIGURE 13.28 Network tools

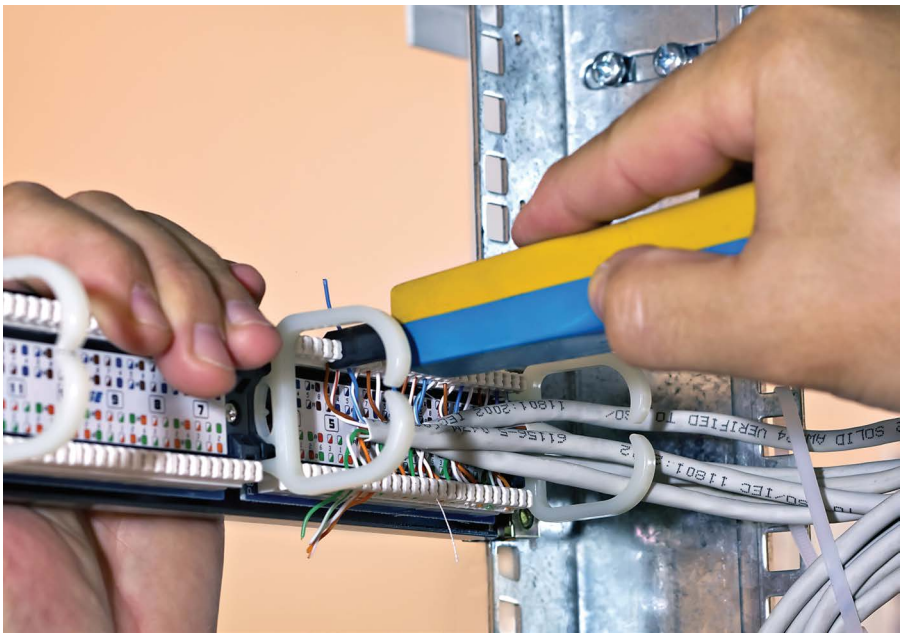


FIGURE 13.29 Punchdown tool with a network patch panel

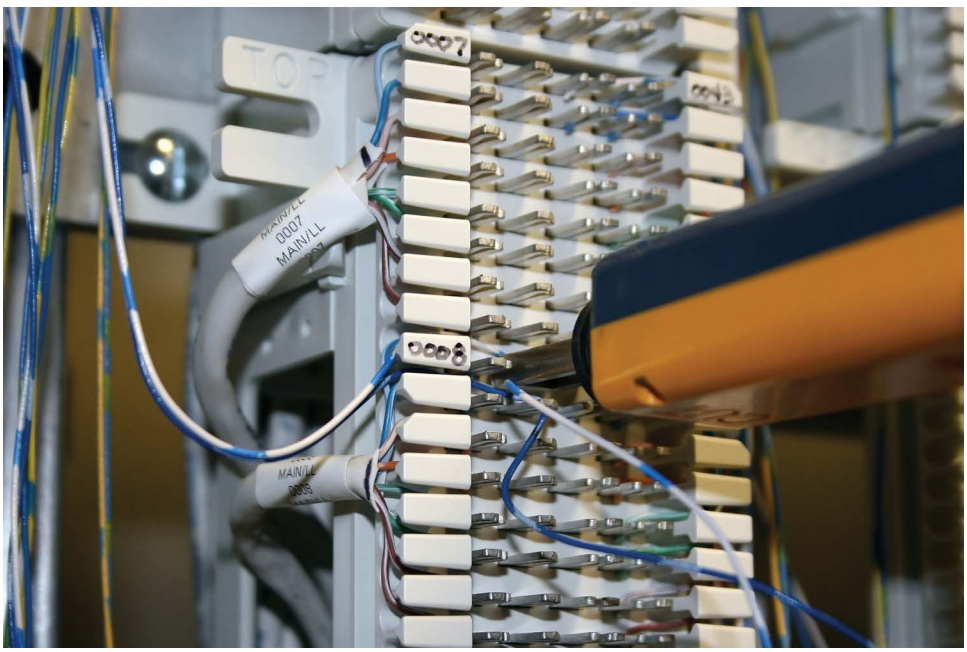


FIGURE 13.30 Punchdown tool with a phone punchdown block

The OSI Model

The International Organization for Standardization (ISO) developed a model for network communications known as the OSI (Open Systems Interconnect) model. The **OSI model** is a standard for information transfer across the network. The model sets several guidelines, including (1) how the different transmission media are arranged and interconnected, (2) how network devices that use different languages communicate with one another, (3) how a network device contacts another network device, (4) how and when data gets transmitted across the network, (5) how data is sent to the correct device, and (6) how it is known if the network data was received properly. All these tasks must be handled by a set of rules, and the OSI model provides a structure into which these rules fit.

Can you imagine a generic model for building a car? This model would state that you need some means of steering, a type of fuel to power the car, a place for the driver to sit, safety standards, and so forth. The model would not say what type of steering wheel to put in the car or what type of fuel the car must use but would just be a blueprint for making the car. The OSI model is a similar model for networking.

The OSI model divides networking into different layers so that it is easier to understand (and teach). Dividing the network into distinct layers also helps manufacturers. If a particular manufacturer wants to make a network device that works on Layer 3, the manufacturer has to be concerned only with Layer 3. This division helps networking technologies emerge much faster.

The layers of the OSI model (starting from the top and working down) are application, presentation, session, transport, network, data link, and physical (see Figure 13.31).

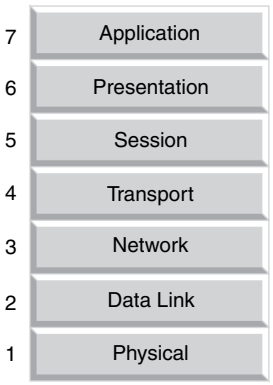


FIGURE 13.31 OSI model layers

Each layer of the OSI model (except for the physical layer, which is at the bottom) uses the layer below it. Each layer provides some function to the layer above it. For example, the data link layer cannot be accessed without first going through the physical layer. If communication needs to be performed at Layer 3 (the network layer), the physical and data link layers must be used first.

TECH TIP

OSI mnemonic

A mnemonic to help remember the OSI layers is Active People Seldom Take Naps During Parties. For example, A in Active reminds you of the application layer, P in People reminds you of the presentation layer, and so on.

Each layer of the OSI model from the top down (except for the physical layer) adds information to the data being sent across the network. Sometimes, this information is called a *header*. Figure 13.32 shows how a header is added as a packet travels down the OSI model. Note that at Layer 2 both a header and a trailer are added. Information at the physical layer is normally called *bits*. When referring to information at the data link layer, use the term *frame*. When referring to information at the network layer, use the term *packet*.

Each of the seven OSI model layers performs a unique function and interacts with the layers surrounding it. The bottom three layers handle the physical delivery of data across the network. The top four layers handle the ins and outs of providing accurate data delivery between computers and their individual processes, especially in a multitasking operating system environment.

The OSI model can be confusing when you first learn about networking, but it is important. Understanding the model helps when troubleshooting a network. Knowing where a problem occurred narrows the field of possible solutions. Table 13.8 describes the layers of the OSI model.

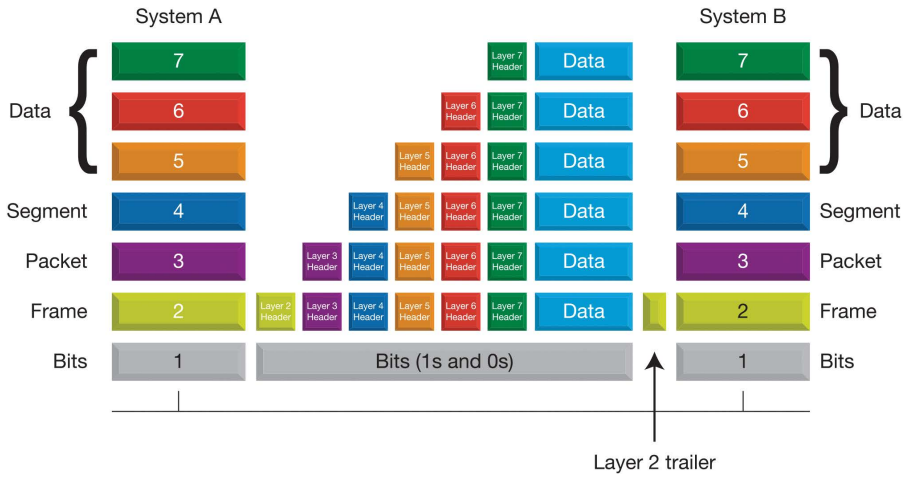


FIGURE 13.32 OSI peer communication

TABLE 13.8 OSI model

OSI model layer	Description
Application	Provides network services (file, print, and messaging) to any software application running on the network.
Presentation	Translates data from one character set to another.
Session	Manages communication and synchronization between network devices.
Transport	Provides mechanisms for how data is sent, such as reliability and error correction.
Network	Provides path selection between two networks. **Routers** reside at the network layer and send data from one network toward the destination network. Encapsulated data at this layer is called a *packet*. Multilayer switches can operate at this layer.
Data link	Encapsulates bits into frames. Can provide error control. A MAC address is at this layer. Layer 2 switches operate at this layer.
Physical	Defines how bits are transferred and received. Defines the network media, connectors, and voltage levels. Data at this level is called *bits*. Hubs, cables, and NICs operate at this level.

The TCP/IP Model

A **network protocol** is a data communication language. A protocol suite is a group of protocols that are designed to work together. Transmission Control Protocol/Internet Protocol (**TCP/IP**) is the protocol suite used in networks today. It is the most common network protocol and is required when accessing the internet. The TCP/IP protocol suite consists of many protocols, including Transmission Control Protocol (TCP), Internet Protocol (IP), Dynamic Host Configuration Protocol (DHCP), File Transfer Protocol (FTP), and Hypertext Transfer Protocol (HTTP), to name a few. The TCP/IP model describes how information flows through a computer when TCP/IP-based protocols are used. The TCP/IP model has only four layers, in contrast to the seven layers in the theoretical OSI model. Because there are fewer layers and because the TCP/IP model consists of protocols used on the internet, it is easier to study and understand networking from the perspective of the TCP/IP model. Do not refer to the TCP/IP model layers with layer numbers. Only the OSI model layers are called Layer 1, Layer 2, and so on. Figure 13.33 shows the TCP/IP model and message formatting, and Table 13.9 describes the layers.

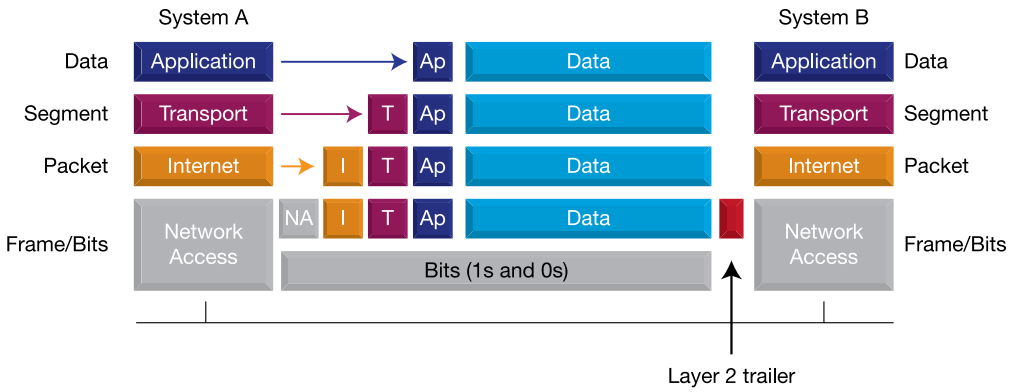


FIGURE 13.33 TCP/IP model and message formatting

TABLE 13.9 TCP/IP model layers

TCP/IP model layer	Description
Application	TCP/IP-based application layer protocols format data for specific purposes. Equivalent to the application, presentation, and session layers of the OSI model. Protocols include HTTP, Telnet, DNS, HTTPS, FTP, TFTP, TLS, SSL, POP, SNMP, IMAP, NNTP, and SMTP.
Transport	Transport layer protocols add port numbers in the header so a computer can identify which application sent the data. When data returns, this port number allows the computer to determine into which window on the screen to place the data. Protocols include TCP and UDP.
Internet	Sometimes called the internetwork layer, IP is the most common internet layer protocol. IP adds source and destination **IP addresses** to uniquely identify the source and destination network devices. An IP address is a unique 32- or 128-bit number assigned to a NIC.
Network access	The network access layer defines how to format the data for the type of network used. For example, if Ethernet is used, an Ethernet header, including unique source and destination MAC addresses, will be added here. A **MAC address** is a unique 48-bit hexadecimal number burned into a chip on the NIC. The network access layer would define the type of connector used and put the data onto the network, whether it be voltage levels for 1s and 0s on the copper cable or pulses of light for fiber.

Table 13.10 shows what devices operate at the OSI and TCP/IP model layers. Wireless devices are covered later in this chapter.

TABLE 13.10 Devices and the OSI and TCP/IP models

Network devices	OSI model layer	TCP/IP model layer	Description
Router, wireless router	Network	Internet (internetwork)	A router connects two or more networks.
Switch, wireless access point, wireless bridge	Data link	Network access	A switch connects devices to a LAN and learns MAC addresses. An access point connects wireless devices to form a WLAN. A wireless bridge connects two networks.
Hub, wireless antenna, cable, connectors	Physical	Network access	A hub connects devices to a LAN. An antenna receives wireless signals. A cable connects a device to a wired network. A connector attaches to a cable.

Network Addressing

A network adapter normally has two types of addresses assigned to it: a MAC address and an IP address. A MAC address is a unique 48-bit hexadecimal number that is burned into a chip located on a NIC. A MAC address is unique for every computer on the network. However, a MAC address has no scheme except that the first 24 bits represent the manufacturer. A MAC address is known as a Layer 2 address or a **physical address**. A MAC address is normally shown in one of the formats listed in Table 13.11.

TABLE 13.11 MAC address formats

Address format	Description
00-11-11-71-41-10	Groups of two hexadecimal digits are separated by hyphens.
01:11:11:71:41:10	Groups of two hexadecimal digits are separated by colons.
0111.1171.4110	Groups of four hexadecimal digits are separated by periods.

IP addressing provides a much more organized way of addressing a computer, and an IP address is sometimes known as a Layer 3 address, in reference to the OSI network layer. There are two types of IP addresses: IPv4 (IP version 4) and IPv6 (IP version 6).

IPv4 is the most common IP addressing used on LANs. An IPv4 address is a 32-bit number that is entered into a NIC's configuration parameters. This address is used when multiple networks are connected and when accessing the internet. An IPv4 address is shown using dotted decimal notation, such as 192.168.10.4.

TECH TIP

What is in an IPv4 address?

An IPv4 address is separated into four sections called octets. The octets are separated by periods, and each one represents 8 bits. The numbers 0 to 255 can be represented by 8 bits.

IPv6 addresses are 128 bits in length and shown in hexadecimal format. IPv6 addresses are used by corporate devices and by most internet service providers. Today, a computer has both an IPv4 address and IPv6 address assigned. An example of an IPv6 address is fe80::13e:4586:5807:95f7. Each set of four digits represents 16 bits. When an octet contains just three digits (for example, 13e), there is a "silent" zero in front that has been omitted from the octet (013e). A double colon (::) in an IPv6 address represents a string of zeros that has been omitted. Only one set of double colons is allowed in an IPv6 address. Many network cards are assigned IPv6 addresses, even where IPv6 is not used.

One IPv6 address assigned to a NIC is a link-local address. An IPv6 **link-local address** is used to communicate on a particular network. This address cannot be used to communicate with devices on a different network. A link-local address can be manually assigned or, more commonly, may be automatically assigned. Figure 13.34 shows a home computer that has an IPv6 link-local address that has been automatically assigned. You can also see the IPv4 address in this figure.

```
Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . : gateway.2wire.net
   Link-local IPv6 Address . . . . . : fe80::13e:4586:5807:95f7%10
   IPv4 Address. . . . . . . . . . . : 192.168.1.64
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.1.254
```

FIGURE 13.34 IPv6 link-local address and IPv4 address

IPv4 addresses are grouped into five classes: A, B, C, D, and E. Class A, B, and C addresses are used by network devices. Class D addresses are used for multicasting (sending traffic to a group of devices, as in a distributed video or a web conference session), and Class E addresses are used for experimentation. It is easy to tell which type of IP address is used by a device: You just need to look at is the first number shown in the dotted decimal notation. Table 13.12 shows the common classes of addresses.

TABLE 13.12 Classes of IPv4 addresses

Class	First octet (number) of the IP address
Class A	0 to 127
Class B	128 to 191
Class C	192 to 223

The IP address 12.150.172.39 is a Class A address because the first number is 12. The IP address 176.10.100.2 is a Class B IP address because the first number is 176. The IP address 200.1.1.1 is a Class C address.

IP addresses are also classified as public addresses and private addresses. A **private IP address** is used inside a home or business. This address is not allowed to be transmitted across the internet. The service provider or company translates the address to a **public IP address** that is seen on the internet. Table 13.13 shows the private IP address ranges for the IPv4 classes.

TABLE 13.13 IPv4 private IP addresses

Class	First octet (number) of an IP address
Class A	10.*x*.*x*.*x* (where the *x* represents any number from 0 to 255), or 10.0.0.0 through 10.255.255.255
Class B	172.16.*x*.*x* through 172.31.*x*.*x*, or 172.16.0.0 through 172.31.255.255
Class C	192.168.*x*.*x*, or 192.168.0.0 through 192.168.255.255

More IPv4 Addressing

An IP address is broken into two major parts: the network number and the host address. The **network number** is the portion of an IP address that represents which network the computer is on. All computers on the same network have the same network number. The **host address** (or host portion of the address) represents the specific computer on the network. Every computer on the same network has a unique host number; if their host numbers weren't unique, the computers could not communicate.

The number of bits that represent the network number and the host address depends on which class of IP address is used. With Class A IP addresses, the first 8 bits (the first number) represent the network portion, and the remaining 24 bits (the last three numbers) represent the host number. With Class B IP addresses, the first 16 bits (the first two numbers) represent the network portion, and the remaining 16 bits (the last two numbers) represent the host number. With Class C IP addresses, the first 24 bits (the first three numbers) represent the network portion, and the remaining 8 bits (the last number) represent the host number. Figure 13.35 illustrates this point.

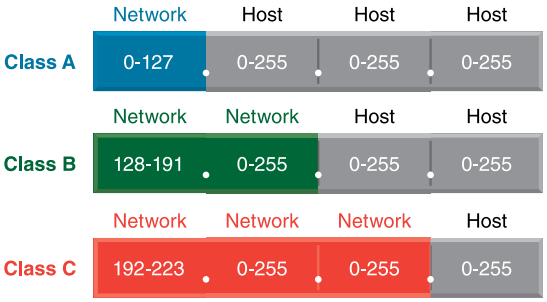


FIGURE 13.35 IP addressing (network and host portions)

To see how IP addressing works, say that a business has two networks connected with a router (see Figure 13.36). On each network, there are computers and printers. Each of the two networks must have a unique network number. For this example, one network has the network number 192.168.151.0, and the other network has the network number 192.168.152.0. Notice that each network number is a Class C IP address because the first number is 192.

With a Class C IP address, the first three numbers represent the network number. The first network uses the numbers 192.168.151 to represent the network part of the IP address. The second network uses the numbers 192.168.152 in the network part of the address. Remember that each network must have a different network part of the IP address from any other network in the organization. This is part of the **IP addressing scheme** designed by a network engineer and implemented by technicians. Almost all organizations and home networks use private addresses (refer to Table 13.13) for their IP addressing scheme.

The last part of the IP address (the host portion) is used to assign a unique number to each network device. On the first network, each device has a number that starts with 192.168.151 because that is the network part of the number, and it stays the same for all devices on that network. Each device has a different number in the last portion of the IP address—for example, 192.168.151.1, 192.168.151.2, 192.168.151.3, 192.168.151.4, and so on (as shown in Figure 13.36).

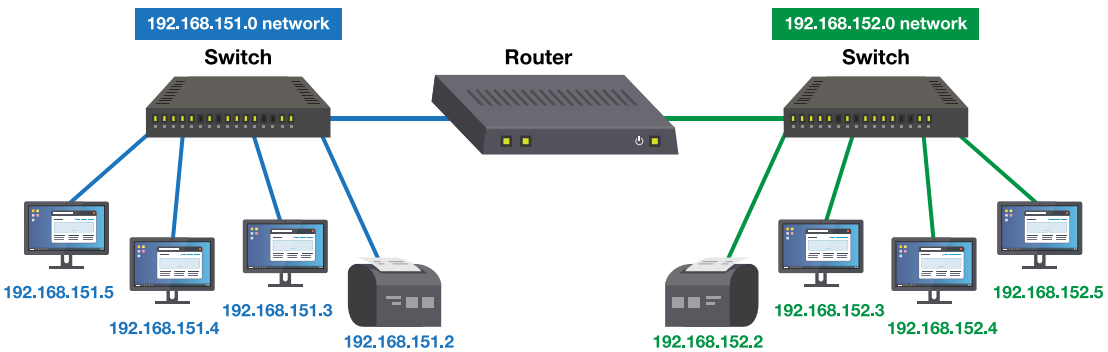


FIGURE 13.36 IP addressing (two networks example)

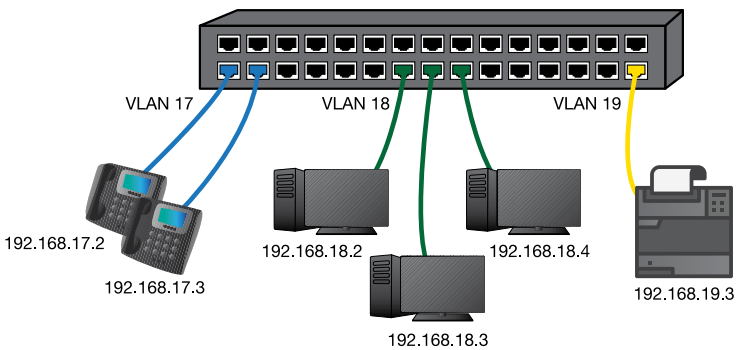
On the second network, each device has a number that starts with 192.168.152 because that is the network part of the IP address. The last number in the IP address changes for each network device. In this example, no device can have a host number that has 0 in the last octet because that number represents the network. In addition, no device can have an IP address where the last octet in the host portion of the address is 255 because that represents the **broadcast address**, which is the IP address used to communicate with all devices on a particular network.

In this example, no network device can be assigned the IP addresses 192.168.151.0 or 192.168.152.0 because these numbers represent the two networks. Furthermore, no network device can be assigned the IP addresses 192.168.151.255 or 192.168.152.255 because these numbers represent the broadcast addresses used with the 192.168.151.0 network and the 192.168.152.0 network. An example of a Class B broadcast address is 172.16.255.255. An example of a Class A broadcast address is 10.255.255.255.

VLANs

Another way of separating devices into networks is by using VLANs. A virtual local area network (**VLAN**) is giving a number to a grouping of devices within a switch. For example, IP phones, PCs, and printers typically connect to a switch, and companies that have switches that support VLANs create separate networks for different types of devices or for devices in particular locations. For example, if you had two IP phones, three PCs, and a printer connected to the same switch, you might configure the switch ports that connect to the IP phones as VLAN 17, the switch ports that connect to the PCs as VLAN 18, and the port that connects to the printer as VLAN 19. The IP addressing schemes used within a company commonly include the VLAN number as part of the IP addressing. Notice in Figure 13.37 that the phones have IP addresses 192.168.17.*x* (where *x* is a unique number) and that the PCs have IP addresses 192.168.18.*x*. The printer has the IP address 192.168.19.3.

Switch configured with VLANs*



*A switch that supports VLANs has all ports in VLAN 1 unless they are configured otherwise.

FIGURE 13.37 VLANs

Not all switches can be configured with VLANs, but on a switch that does support VLANs, all ports are assigned to VLAN 1 by default. If a switch does not support VLANs, then all ports need to be considered to be in the same network, and all devices connected to the switch will be in the same network.

Benefits of VLANs include the following:

- Separation of networks at Layer 2
- Reduced broadcast messages
- Ease of applying security
- Ease of applying quality of service (QoS)

Subnet Masks

In addition to assigning a computer an IP address, you must also assign a computer a subnet mask. The **subnet mask** (sometimes shortened to *mask*) is a number that a computer uses to determine which part of the IP address represents the network and which portion represents the host. The default subnet mask for a Class A IP address is 255.0.0.0, the default subnet mask for a Class B IP address is 255.255.0.0, and the default subnet mask for a Class C IP address is 255.255.255.0. Table 13.14 recaps this important information.

TABLE 13.14 Subnet masks

Class	First number	Network/host number	Subnet mask
A	0–127	*N.H.H.H**	255.0.0.0 (/8)
B	128–191	*N.N.H.H**	255.255.0.0 (/16)
C	192–223	*N.N.N.H**	255.255.255.0 (/24)

**N* = network number; *H* = host number

Sometimes subnet masks are shown with a slash (/) followed by a number; this is known as prefix notation format. The number represents how many consecutive 1s are in the subnet mask. For example, /8 indicates that there are eight consecutive 1s in the subnet mask, or 11111111.00000000.00000000.000000000. Notice that the subnet mask is all 0s after the eight 1s are shown. A technician might have to refer to network documentation, and the subnet mask to use will be shown in prefix notation format. The prefix notation format for a Class A address is /8, Class B is /16, and Class C is /24.

A subnet mask does not always have to follow classful boundaries. Sometimes, a technician might see a subnet mask that looks like the following examples: 255.255.254.0 or /23, 255.255.255.192 or /26, or 255.255.255.240 or /28. These are known as classless inter-domain routing (CIDR) subnet masks. **CIDR** (pronounced "cider") is a method of allocating IP addresses based on the number of host addresses needed for a particular network. Because the subnet mask dictates where the network portion ends and where the host portion begins, CIDR subnet masks are different from the standard 255.0.0.0, 255.255.0.0, and 255.255.255.0 subnet masks.

To help you better understand the concept, let's look at how a /23 subnet mask becomes 255.255.254.0. The /23 means there are 23 1s in a row in the subnet mask, and the rest of the numbers are 0s; keep in mind that there are just eight 1s in each of the subnet mask sections where you enter the number. Write down the 23 1s with only eight digits in each section. Place 0s after the 1s for the remaining digits, keeping in mind that a subnet mask, like an IP address, has 32 bits. Then you perform simple binary-to-decimal conversion to get the subnet mask in dotted decimal notation, which is required to enter it on a network device:

11111111.11111111.11111110.00000000
255 . 255 . 254 . 0

Appendix A, "Subnetting Basics," goes into CIDR in a lot more detail.

Wireless Networks Overview

Even though wireless devices are covered elsewhere in the book, a networking chapter would not be complete without discussing wireless networking. Wireless data transfer occurs in both licensed and unlicensed ranges. In one of the licensed wireless ranges, a company or service provider has to obtain a specific frequency—or possibly a frequency range—from the Federal Communications Commission (FCC) or its designee. Licensed wireless offers better performance than unlicensed, but it involves costs. Licensed wireless is used for radio and TV, military systems, and cellular communications.

Wireless networks are popular in home and corporate environments. These networks transmit data over the air using either unlicensed ranges, such as infrared (1 THz to 400 THz range) for things like your TV remote, or radio frequencies (the traditional **2.4 GHz** or **5 GHz** range, and the newer **6 GHz** range).

Wireless networks are great in places that are not conducive to running cabling, such as outdoor centers, convention centers, bookstores, coffee shops, and hotels, as well as between buildings

and between nonwired rooms in homes (as illustrated in Figure 13.38) or businesses. Wireless networks operate at Layers 1 and 2 of the OSI model and can be installed indoors or outdoors.

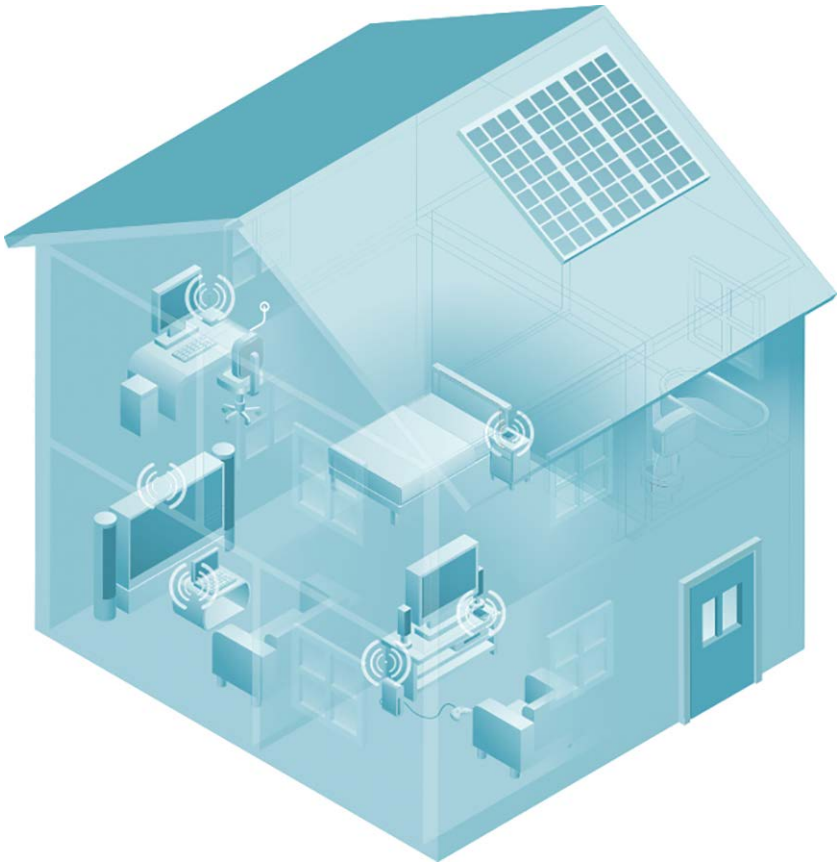


FIGURE 13.38 Wireless connectivity within a home

TECH TIP

What if I want wireless connectivity for my desktop computer?

Desktop workstations usually have integrated RJ45 Ethernet connections, but for wireless networking, a wireless NIC is required and may have to be added.

Laptops and portable devices are frequently used to connect to wireless networks and have wireless capabilities integrated into them. A technician must be familiar with installation, configuration, and troubleshooting of both wired and wireless technologies.

Wireless Network Standards

The IEEE 802.11 committees define standards for wireless networks, and these standards can be quite confusing. Table 13.15 shows the current and proposed wireless network standards.

TABLE 13.15 IEEE 802.11 standards

Standard	Purpose
802.11a	Came after the 802.11b standard. Has speeds up to 54 Mb/s but is incompatible with 802.11b. Operates in the 5 GHz range.
802.11b	Operates in the 2.4000 and 2.4835 GHz radio frequency ranges, with speeds up to 11 Mb/s.
802.11e	Provides standards related to quality of service.
802.11g	Operates in the 2.4 GHz range, with speeds up to 54 Mb/s, and is backward compatible with 802.11b.
802.11i	Relates to wireless network security and includes AES (Advanced Encryption Standard) for protecting data.
802.11n	Operates in the 2.4 and 5 GHz ranges and is backward compatible with the older 802.11a, b, and g equipment. Offers speeds up to 600 Mb/s using MIMO (multiple input/multiple output) antennas and allows a maximum of four simultaneous data streams.
802.11ac (Wi-Fi 5)	Operates only in the 5 GHz range, which makes it backward compatible with 802.11n and 802.11a. Offers speeds up to 6.93 Gb/s using MU-MIMO (multi-user MIMO) antennas and allows a maximum of eight simultaneous data streams.
802.11ad	Works in the 60 GHz range, with speeds up to 6.76 Gb/s. Also known as Wi-Gig.
802.11ax (**Wi-Fi 6** or 6E)	Operates in the 2.4, 5, and 6 GHz ranges and is backward compatible with 2.4 and 5 GHz devices. Supports multiple wireless devices more efficiently and allows a maximum of eight simultaneous data streams using MU-MIMO antennas.
802.11be (**Wi-Fi 7**)	Uses the 2.4, 5, and 6 GHz ranges and allows a maximum of 16 data streams. Has a sophisticated mechanism that enables dynamic frequency band management by selectively mitigating interference while maintaining continuous network connectivity.

Wireless Network Components

The most common components of a wireless network are wireless NICs, access points, wireless bridges, and wireless routers. Table 13.16 describes the purposes of these devices.

TABLE 13.16 Common wireless devices

Wireless device	Description
Access point (AP)	The central connecting point for a wireless network. Coordinates wireless access for wireless devices. May connect to a wired network.
Wireless bridge	A physical device or software that connects two or more networks. May connect a wireless network to a wired network. An example of a wireless bridge is a building where all devices connect wirelessly to the bridge. The bridge connects to the wired network, which eventually connects to the internet. Many access points or wireless routers can be placed in bridged mode.
Wireless NIC	Integrated into a wireless device, such as a laptop, smartphone, or tablet.
Wireless router	An AP/router device that normally has both wireless capability and a few wired Ethernet ports. It is a router because it connects multiple networks.
Wireless printer/ multifunction device	Common type of home/small office device that can print, scan, and copy.

Major types of wireless NICs include integrated ports, USB, and PCIe. Figure 13.39 shows a wireless USB NIC with a detachable antenna.

FIGURE 13.39 Wireless USB NIC

To determine whether you have a wireless NIC installed on a Windows 10/11 device, access *Settings* > *Network & Internet* > *Wi-Fi* appears in the window to the left if you have it installed and the adapter is not enabled. Use the *Change adapter options* from the *Advanced network settings* section to see all adapters and to see if any are disabled.

Figure 13.40 shows the Network Connections window of a computer that has virtualization enabled, a wired Ethernet port, Wi-Fi, and Bluetooth installed. Note that the wireless NIC is not being used, but it is enabled.

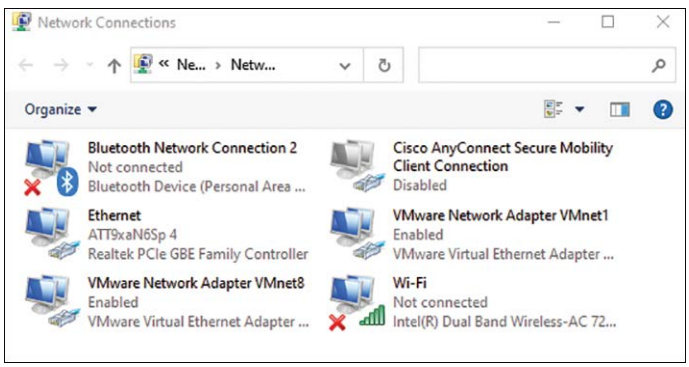


FIGURE 13.40 Wireless NIC in the Network Connections window

A wireless access point (AP) is a device that receives and transmits data from multiple computers that have wireless NICs installed. The AP can be a unit that connects to the corporate network, as shown in Figure 13.41, or can be a wireless router, as shown in Figure 13.42. It is the wireless AP part of the router that needs the three antennas shown in the figure.

Wireless routers commonly have switch ports built into them. This is referred to as having router/switch functionality. You might hear a wireless router referred to as a router/switch, but regardless of the name, such a device has switch ports integrated, as shown in Figure 13.42. Much like a wired router, a wireless router is used to connect devices between networks such as a home network and the internet. The switch part of the device is used to create a wired LAN, and each wired device has an Ethernet cable that runs between the device and the switch port on the wireless router.

FIGURE 13.41 Corporate access point

FIGURE 13.42 Wireless router with integrated switch ports

Wireless Network Design

The easiest way to describe an access point is to think of it as a network hub, but instead of connecting wired devices and sharing bandwidth, the AP connects wireless devices that share bandwidth. Each access point can handle 30 to 100 wireless devices, depending on the wireless standard being used, vendor, environment (wood, drywall, brick, concrete, and so on), amount of usage, and type of data sent.

When designing a wireless network you need to take into account several factors:

> Which standard you are going to use (802.11n, 802.11ac, 802.11ax, etc.).

> Which frequency range/**frequency band** you are going to use in a specific location and the type of devices to consider for a specific frequency. A multiband plan is commonly used in a corporate environment. For example, you might want to use the 2.4 GHz range for a wireless network for guests and the 5 GHz range for company devices since the 5 GHz range is not as crowded with devices as the 2.4 GHz range is. The 6 GHz band is also a good choice when there are a lot of devices, for streaming HD video, and for online gaming. Another idea would be to design based on the type of equipment, such as using the 2.4 GHz range for PC-based devices and the 5 GHz range for Apple and cellular devices. The 2.4 GHz range is better for long distances and when there are solid objects (walls/columns) in the area. To see which band a computer is using, access the *Wi-Fi* Windows Settings option > *Hardware properties* link.

> The location of the AP and what interference is around the area where the AP will be installed.

Let's take a look at some of the details involved with design.

Each AP is assigned a service set identifier (**SSID**). It is common for an AP to have a default SSID that can be changed. An SSID is a set of 32 alphanumeric characters used to differentiate between different wireless networks. It is common to have more than one SSID configured on a wireless router/AP, as illustrated in Figure 13.43. Figure 13.44 shows a screen capture of a sample wireless configuration for a 802.11ac TP-Link wireless router.

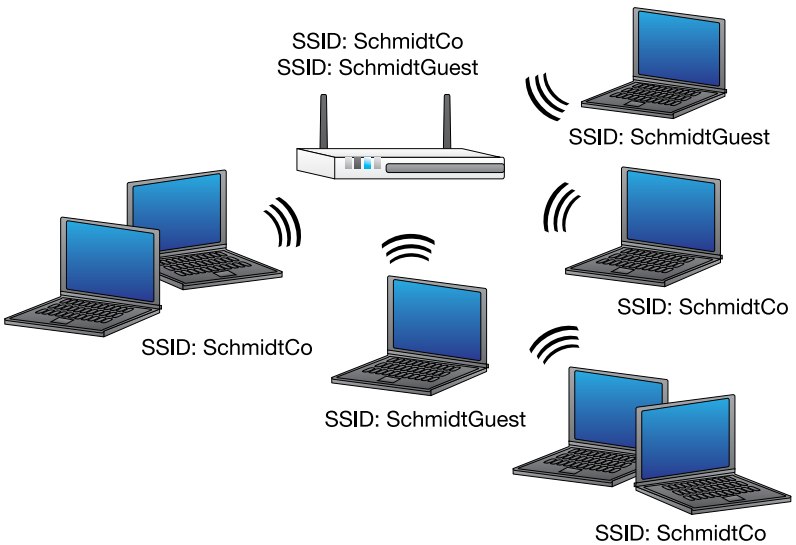


FIGURE 13.43 Each wireless network has its own SSID

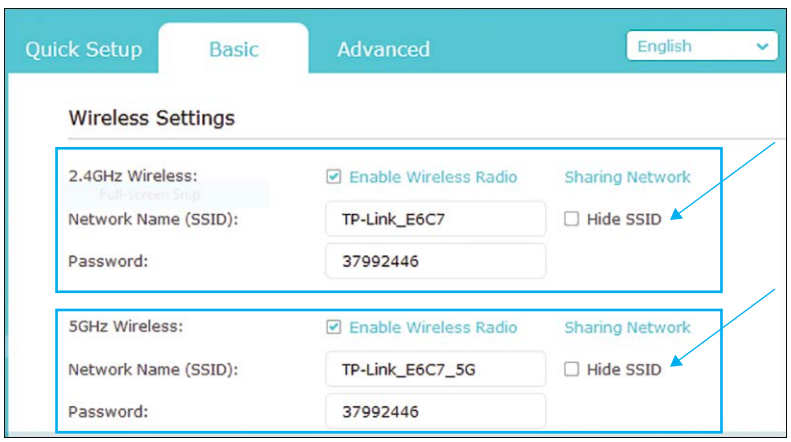


FIGURE 13.44 Configuring SSIDs and SSID broadcasting on a TP-Link wireless router

An AP broadcasts the SSID by default, but this setting can be changed. When the AP is broadcasting the SSID, wireless NICs can automatically detect that particular wireless network. When the AP is not broadcasting (that is, when the SSID cannot be found in the list of wireless networks), the SSID can be manually configured through the AP's configuration window. Look back at the 2.4 GHz and 5 GHz configurations shown in Figure 13.44. Beside each SSID is a *Hide SSID* checkbox that you can check to disable SSID broadcasting.

An access point can be wired to or can connect wirelessly to another AP, can have a wired or wireless connection to a wireless repeater (also called a **wireless extender**), or can connect to a wired network. The access point can then relay the transmission from a wireless device to another network or to the internet through the wired network. If two access points are used and they connect two different wireless networks, two different SSIDs are used. Figure 13.45 shows this concept. If two access points connect to the same wireless network, the same SSID is used. Figure 13.46 shows this concept.

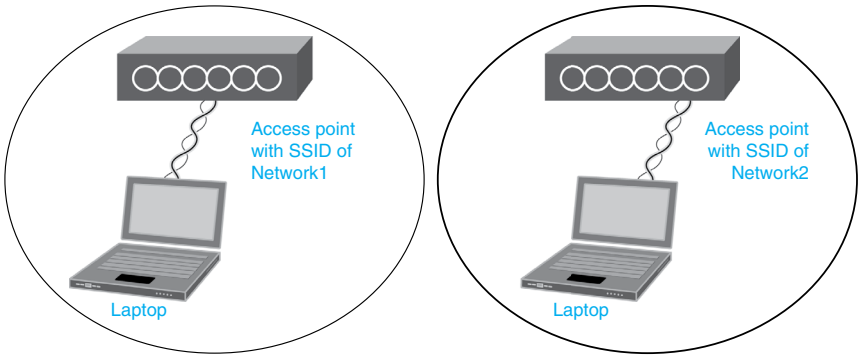


FIGURE 13.45 Two separate wireless networks with two SSIDs

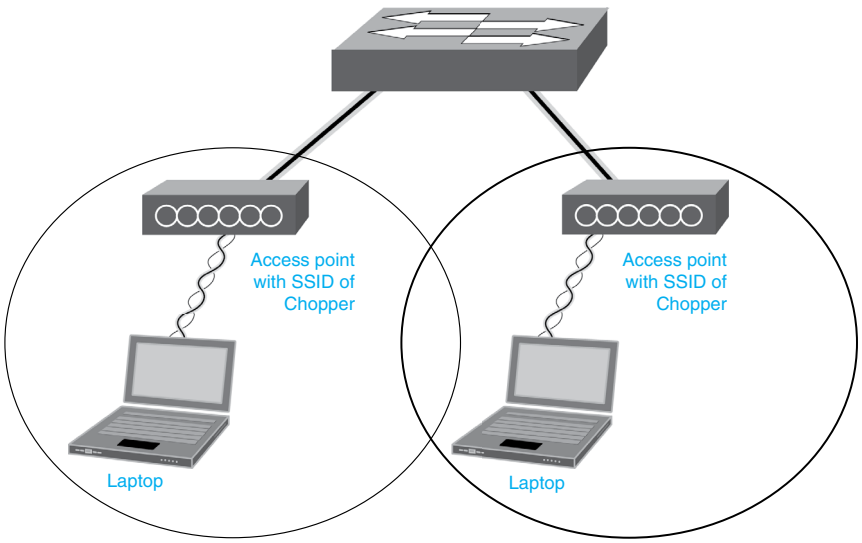


FIGURE 13.46 One extended wireless network with the same SSID on both APs

A home or small business network can expand its wireless network by using a wireless repeater (also known as a wireless range extender). In such a case, the access point cannot normally be connected to the wired LAN. Instead, the repeater access point attaches to a "root" access point. The repeater access point allows wireless devices to communicate with it and relays the data to the other access point. Both access points have the same SSID (see Figure 13.47).

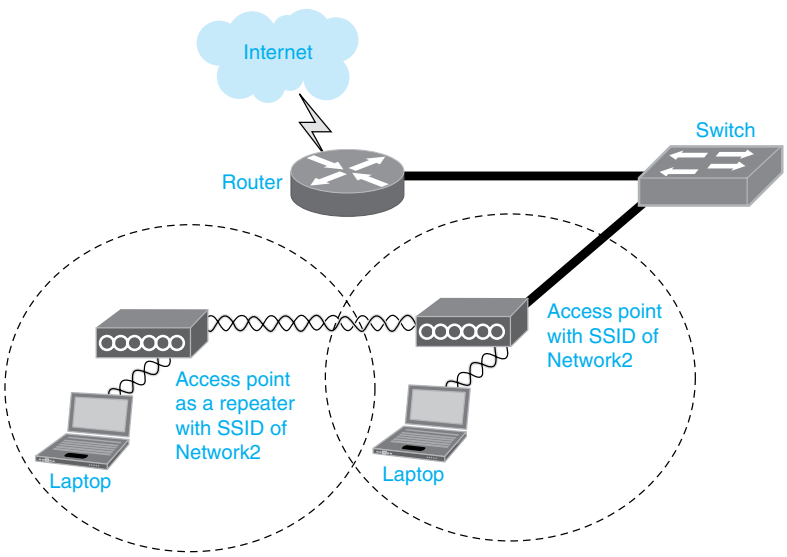


FIGURE 13.47 Access point as a repeater

Wireless Channel ID

In addition to having an SSID, an access point can be configured with a number known as a channel ID. The channel ID, sometimes known simply as the **channel**, is a specific number that defines the frequency at which the access point operates. With an AP that has a 2.4 GHz antenna, up to 14 channels are available, depending on where in the world the wireless network is deployed. In the United States, only 11 channels are used; they are listed in Table 13.17.

TABLE 13.17 Wireless frequency channels

Channel ID number	Frequency (in GHz)
1	2.412
2	2.417
3	2.422
4	2.427
5	2.432
6	2.437
7	2.442
8	2.447
9	2.452
10	2.457
11	2.462

The frequencies shown in Table 13.17 are center frequencies. The center frequencies are spaced 5 MHz apart. Each channel is actually a range of frequencies. For example, the channel 1 range is 2.401 to 2.423, with the center frequency being 2.412.

TECH TIP

Channel ID must match

The channel ID (frequency) must be the same between an access point and a wireless NIC for communication to occur between any wireless devices on the network.

The three commonly used nonoverlapping channel IDs are 1, 6, and 11. By using these three channel IDs, each of the three access points mounted near one another does not experience interference from the other two. This is because each center frequency does not overlap with the adjacent frequency channels (see Figure 13.48).

Notice in Figure 13.48 that each center frequency is 5 MHz from the next center frequency. Also notice that each channel is actually a range of frequencies, as shown by the shaded ovals. Channels 1, 6, and 11 clearly do not overlap and do not interfere with each other. Other nonoverlapping channel combinations could be Channels 2 and 7, Channels 3 and 8, Channels 4 and 9, and Channels 5 and 10. The combination of Channels 1, 6, and 11 is preferred because it gives you three channels with which to work. Figure 13.49 shows a different way of looking at how Channels 1, 6, and 11 do not overlap.

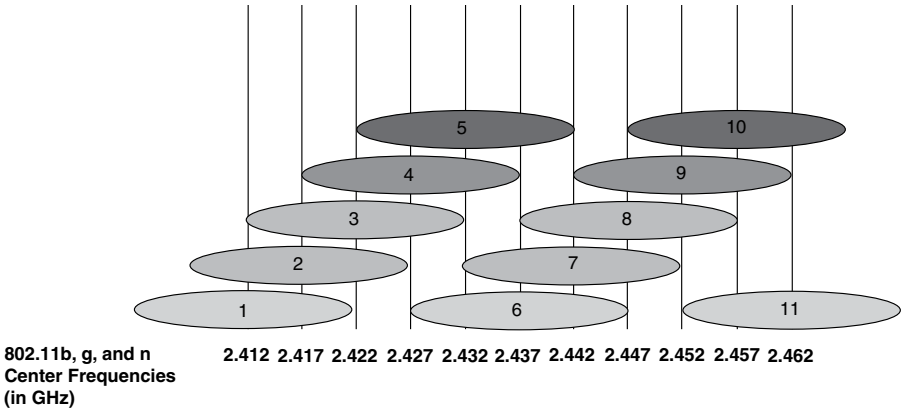


FIGURE 13.48 802.11b/g/n 2.4 GHz nonoverlapping channels

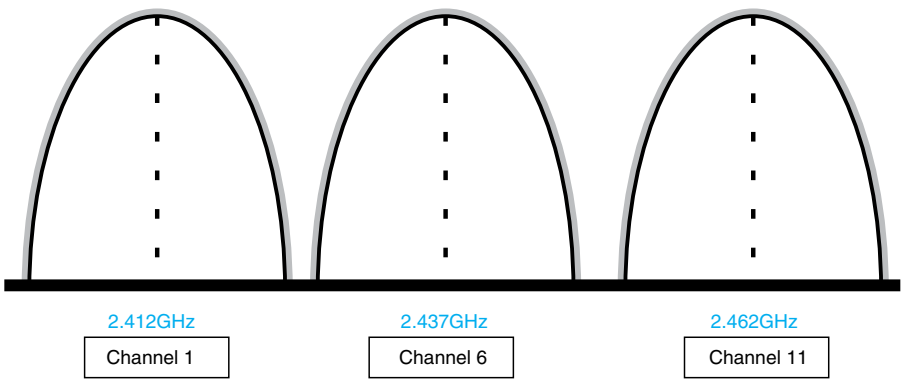


FIGURE 13.49 2.4 GHz channel IDs 1, 6, and 11

Figure 13.50 shows how the three nonoverlapping channels can be used to attain extended coverage even with multiple access points.

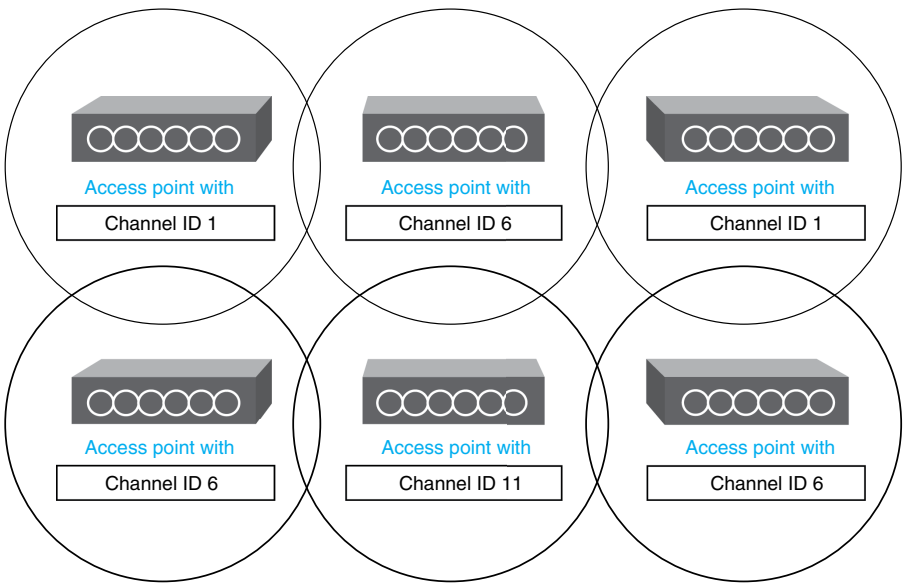


FIGURE 13.50 802.11b/g/n nonoverlapping channel IDs

With 802.11a, 12 20 MHz channels are available in the 5 GHz range. 802.11n supports 20 and 40 MHz channels. 802.11ac supports 20, 40, 80, and 160 MHz channels. The 5 GHz range has three subranges called Unlicensed National Information Infrastructure (UNII): UNII-1, UNII-2, and UNII-3. All bands can be used for indoor and outdoor usage. Figure 13.51 shows the 5 GHz channels.

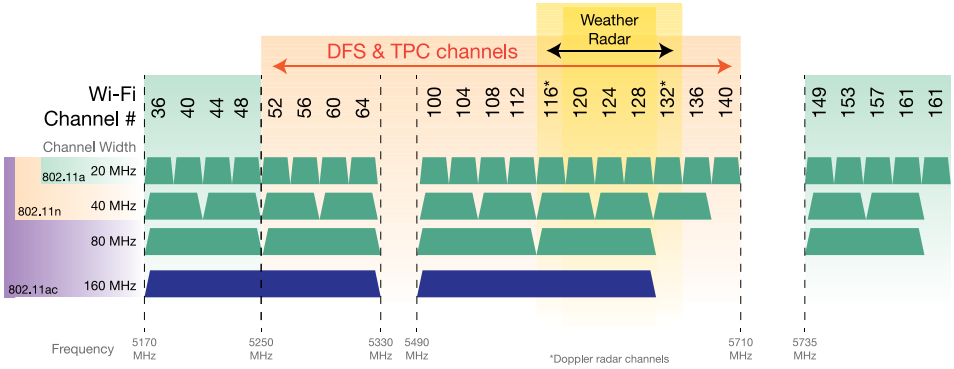


FIGURE 13.51 802.11 a/n/ac 5 GHz channel IDs

Devices that work in the UNII-2 frequency ranges must support dynamic frequency selection (DFS) and transmit power control (TPC) to avoid interference with radar systems. These two terms are most often shortened to simply *DFS channels*. Most wireless routers can automatically configure themselves with the best channel, but if the surrounding area has interfering devices, this may need to be manually planned and configured. Figure 13.52 shows how you can select a specific 2.4 or 5 GHz channel on a TP-Link wireless router (and the transmit power is the option below that).

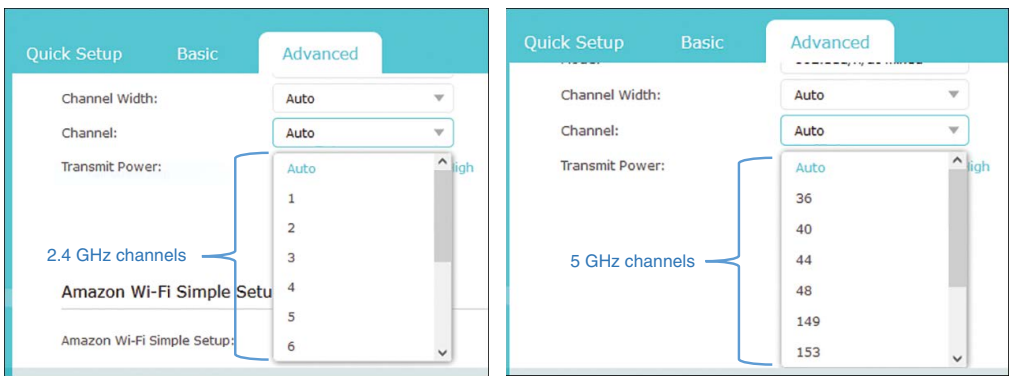


FIGURE 13.52 2.4 and 5 GHz channel selection

With 802.11ax (Wi-Fi 6) and 802.11be (Wi-Fi 7), the 6 GHz band can be used. With these two standards, there is a Low Power Indoor (LPI) standard and a standard power standard. The standard power has fewer channels available, as shown in Figure 13.53.

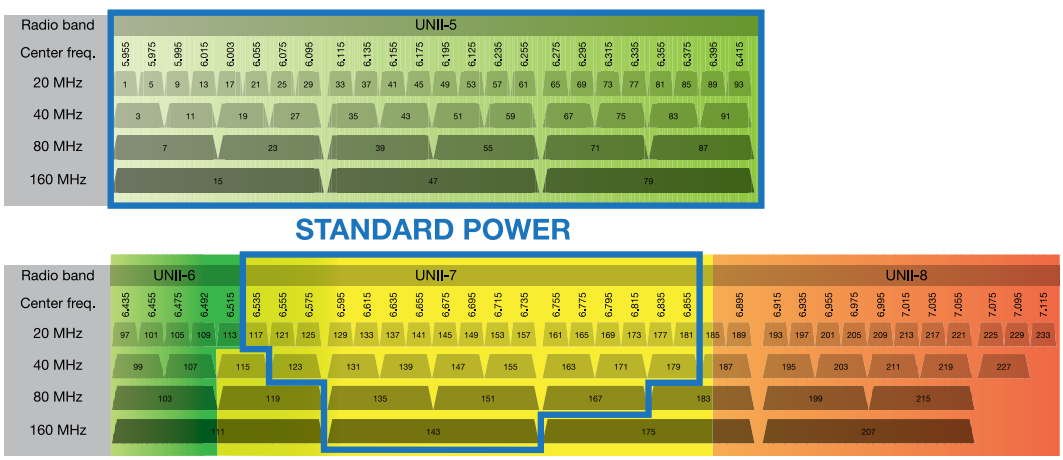


FIGURE 13.53 6 GHz channels

TECH TIP

Know your channel widths

For the A+ certification, know the channel widths. For example, in the 2.4 GHz band, each channel width is 20 MHz; 802.11n and higher allow 40 MHz. In the 5 GHz and 6 GHz ranges, each channel can be 20, 40, 80, or 160 MHz. Increasing the channel width may allow extra speed but could potentially mean interference from other devices operating at the same frequency (but not on that particular wireless network).

An important point to make is that the frequency ranges, channel ID, number of channels, subchannel range, and so on must adhere to a country's **wireless regulations**. Most countries also regulate maximum wireless power levels that differ for indoor networks and outdoor networks and that change often. The good news is there is some consistency in the 2.4 GHz, 5 GHz, and 6 GHz ranges so that a laptop used in the United States will work on the wireless networks in other countries.

Antenna Basics

Wireless cards and access points can have either external or built-in antennas. An antenna radiates or receives radio waves. Some access points also have integrated antennas. Wireless NICs and access points can also have detachable antennas, depending on the make and model. You can simply move an external antenna to a different angle to obtain a better connection. With some antennas, you must turn the antenna to a different angle to get a stronger signal (and, therefore, faster transfers). Antenna placement is important in a wireless network.

TECH TIP

Where is the wireless antenna on a laptop?

For laptops with integrated wireless NICs, the wireless antenna is usually built in to the laptop display for best connectivity. This is because the display is the tallest point of the laptop and therefore closest to the wireless receiving antenna. The quality of integrated antennas is diverse.

There are two major categories of antennas: omnidirectional and directional. An **omnidirectional antenna** radiates energy in all directions. Integrated wireless NICs use omnidirectional antennas. Refer to Figure 10.59 in Chapter 10 to see how the antenna wires attach to two posts on the wireless NIC. These wires connect the antenna to the wireless NIC. If a laptop always has low signal strength, ensure that these two wires are attached.

A **directional antenna** radiates energy in a specific direction. Directional antennas are frequently used to connect two buildings together or to limit wireless connectivity outside a building. Each antenna has a specific radiation pattern (sometimes called a propagation pattern), which is the direction(s) the radio frequency is sent or received. It is the coverage area for the antenna that is normally shown in a graphical representation in the antenna manufacturer's specifications. Figure 13.54 shows the difference in radiation patterns between omnidirectional and directional antennas.

A wireless network installer must be familiar with an antenna's radiation pattern so that the appropriate type of antenna can be chosen for the installation. As a signal is radiated from an antenna, some of the signal is lost. Attenuation, which is sometimes called path loss, is the amount of signal loss for a radio wave as it travels through air. Attenuation is measured in decibels (dB), which represent the ratio between two signal levels.

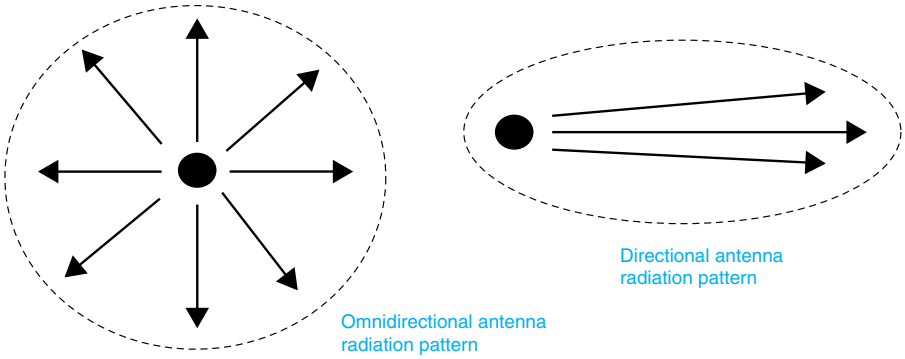


FIGURE 13.54 Basic antenna radiation patterns

Factors that affect an antenna's attenuation are the distance between the transmitting antenna and the receiving antenna, any obstructions between the two antennas, and how high the antenna is mounted. Another factor that affects wireless transmission is interference, including radio frequencies being transmitted using the same frequency range and external noises. Other wireless devices, wireless networks, cordless phones, and microwave ovens are common sources of interference.

TECH TIP

What is the maximum distance of a wireless network?

The maximum distance of a wireless network depends on the wireless network standard used, the antenna attached to the AP, and the attenuation experienced.

Antenna power levels are described as *antenna gain*. Gain is measured in dBi, which is a measurement of decibels in relationship to an isotropic antenna. (The *i* in DBi is for *isotropic*.) Some antennas are shown with the measurement dBd instead of dBi. 0 dBd equals 2.14 dBi. More gain means more coverage in a particular direction. A technician must sometimes reduce the transmit power (that is, lower the signal strength) in order for multiple wireless access points to function in the same building or area.

TECH TIP

You might need to reduce power levels

If an open wireless network is being used by adjacent businesses, reduce the power level of the antenna to reduce the wireless network coverage area.

A **site survey** is an examination of an area to determine the best wireless hardware placement. To conduct such a survey, temporarily mount an access point (or use a telescoping pole to place the AP at different heights). With a laptop that has a wireless NIC and site survey software, walk around the wireless network area to determine the coverage range. Some vendors provide site survey software with their wireless NICs.

A site survey can also be conducted by double-clicking the network icon on the taskbar. The signal strength is shown in the window that appears. Move the access point as necessary to avoid attenuation and obtain the ideal coverage area. Radio waves are affected by obstructions such as walls, trees, rain, snow, fog, and buildings, so for a larger project, a site survey may need to be done over a period of time. Radio waves are also affected by **external interference** from other devices and other wireless networks operating in the same frequency range causing **intermittent wireless**

connectivity. You can see the wireless antenna signal strength in the notification area part of the taskbar. You can also see it from within the wireless NIC properties window. Figure 13.55 shows a wireless antenna signal strength display on a laptop.

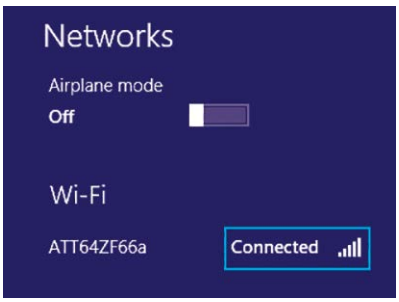


FIGURE 13.55 Signal strength

TECH TIP

Attenuation matters

The type of radio antenna and antenna gain affect the signal strength. However, no matter how good the antenna, as a wireless device is moved farther away from an access point or another wireless device, the more attenuation occurs. Walls, trees, obstacles, and other radio waves can cause attenuation.

A **Wi-Fi analyzer** or wireless locator can determine whether there are wireless networks or hotspots in the area. It can also locate wireless devices that can be attached to pets, people, keys, remotes, and so on. A phone or mobile device app can also locate a powered mobile device or locate a person who has a mobile device with this enabled.

Multiple input/multiple output (**MIMO**) uses multiple 2.4 GHz, 5 GHz, and 6 GHz antennas. Figure 13.56 shows an example of MIMO transmissions. Note that although each client that attaches to an AP using MIMO can have multiple data streams, the AP handles one client at a time.

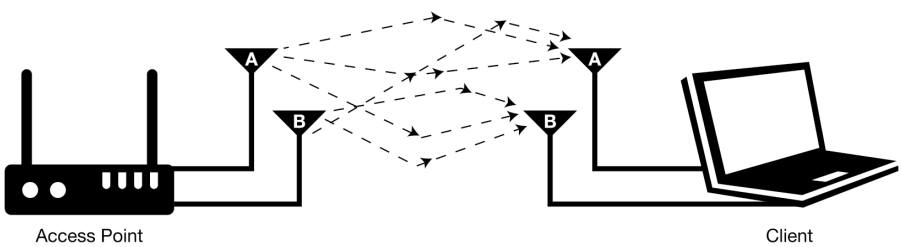


FIGURE 13.56 MIMO transmissions

MIMO antennas may be external or built in to a wireless device. Greater wireless speeds can be achieved by using multiple antennas. 802.11n and higher radios are defined by how many antennas can transmit and receive, as well as by the number of data streams supported. The documentation commonly shows a number formatted like 2x2:1 or 4x4:4, where the first number is the maximum number of antennas that can transmit, the second number is the number of antennas that can receive data, and the last number is the number of data streams supported. 802.11ac and 802.11ax use multi-user MIMO (**MU-MIMO**) and allow up to 8 simultaneous streams, whereas 802.11be can have up to 16 simultaneous streams. MU-MIMO serves multiple devices simultaneously, whereas with pre-802.11ac implementations, an AP serves only one wireless device at a time.

Wireless Data Transfer Speeds

The data transfer speed between a wireless NIC and an access point or another wireless device is automatically negotiated for the fastest transfer possible. The farther away from an access point a wireless device is located, the lower the speed (see Figure 13.57). A low radio frequency signal (or **low RF signal**) could simply mean the device is too far from the access point and result in **slow network speeds** as well as intermittent wireless connectivity. Move closer or change the angle of the device to get a better signal.

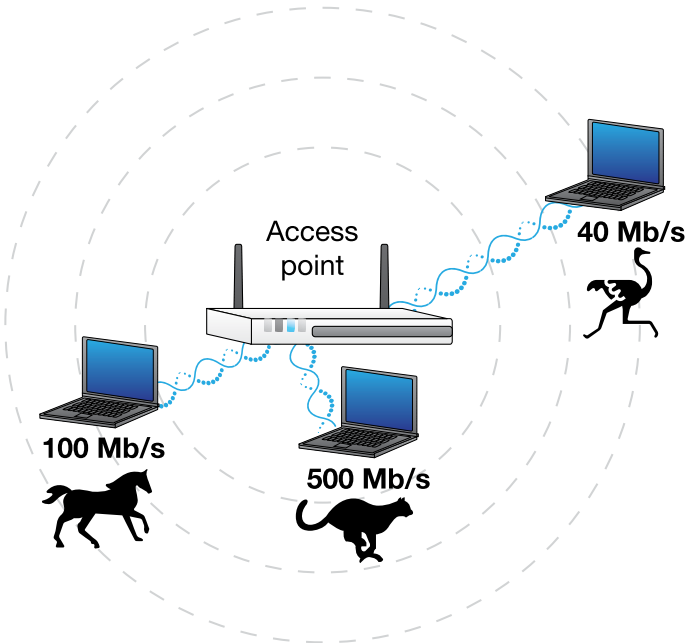


FIGURE 13.57 Wireless connectivity speed ranges

External interference can also influence wireless connectivity and wireless transfer speeds. Check the area for devices or other wireless networks using the same frequency. Don't forget that walls, structures, and other objects also affect wireless reception/speeds.

Wireless and Wired Client Device Configuration Overview

When you are connecting a device to a wired or wireless network, many things might have to be done, such as the following:

- Configure IP addressing.
- If the computer wants to share a printer or folders, file and print sharing might need to be enabled.
- If the device is on a corporate network, the device might have to be put on the domain with a unique name.
- If a wireless device is being configured, the SSID and possibly security parameters need to be entered.

TECH TIP

How to name a computer

In Windows, name a computer using the *System* section of the Control Panels or use the *Settings > System* option. Each device on the same network must be given a unique name.

Configuring an End Device: IP Addressing

No matter what device connects to a wired or wireless network, the device must have an IP address so that it is uniquely identified on the network. Every device on a wired or wireless network needs three important pieces of information: an IP address, a subnet mask, and a default gateway. The IP address and subnet mask are what make the network device unique and allow it to be reached by other devices. There are two ways to get IP addressing information:

> Use a **static IP address**, which means manually defining the IP address and subnet mask
> Use a **dynamic IP address**, which means obtaining the address/mask using DHCP

The device also needs a default gateway IP address in order to communicate with other networks.

TECH TIP

My computer's IP address changes

A computer's IP address can change each time the computer boots because with DHCP, the DHCP server issues an IP address for a specific amount of time.

Statically Configure an IP Address

When an IP address is statically defined, someone manually enters an IP address and mask into the computer using *Settings* > *Network & Internet* > *Change adapter options* link. Most support staff do not statically define IP addresses except for devices that are network infrastructure devices, such as web servers, database servers, other network servers, routers, or switches. Instead, DHCP is used. However, in wired home networks, IP addresses are sometimes statically assigned. Figure 13.58 shows the window that appears when you right-click a particular adapter and select *Properties* > *Internet Protocol Version 4 (TCP/IPv4)* > *Properties* button.

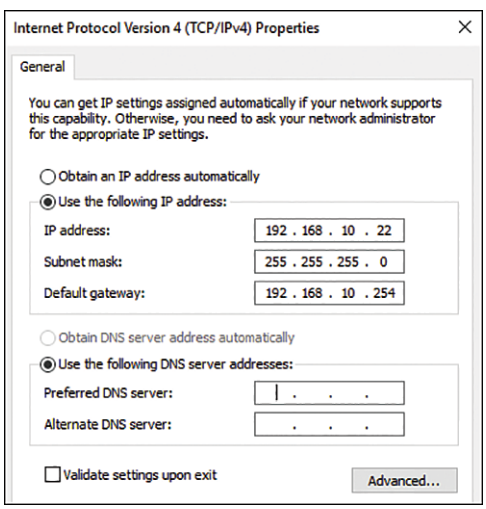


FIGURE 13.58 IP address configuration using a NIC's Properties window

In Windows *Settings* >*Network & Internet*, you select either *Ethernet* or *Wi-Fi* from the left menu and then select the Ethernet connection shown in the pane on the right. Scroll to the *IP settings* section and select *Edit*. In the *Edit IP settings* dialog box, use the arrow to select *Manual* > *IPv4* (see Figure 13.59).

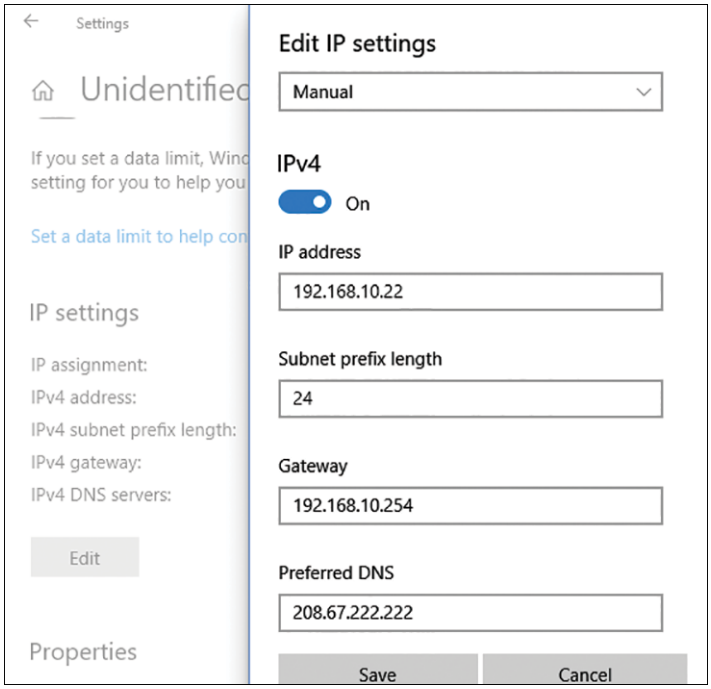


FIGURE 13.59 IP address configuration using Windows Settings

TECH TIP

What happens if you assign the same IP address to two devices?

Entering an IP address that is a duplicate of the address for another network device renders the new network device inoperable on the network and could affect the other device's traffic as well.

Another place that you might need to configure a static IP address is on a wireless router. Most of the time you automatically get an IP address when connecting a router to the internet, but sometimes if a router connects to another router or if you request a static address from the internet service provider, you need to go into the wireless router's configuration and select a static WAN IP address. This is commonly done through the *WAN* or *Internet* option and selecting *Static IP*, as shown on the TP-Link wireless router configuration screen in Figure 13.60. The *Dynamic IP* option is the default and is used when the address is one from the internet provider.

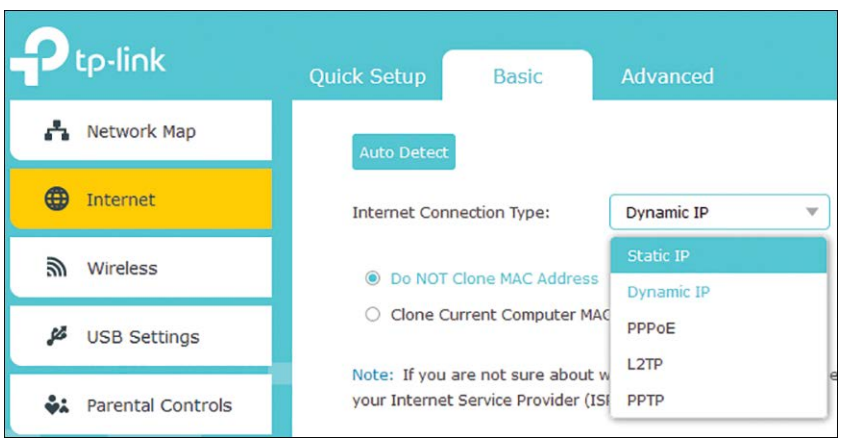


FIGURE 13.60 Static WAN IP address configuration on a wireless router

Using DHCP

Dynamic Host Configuration Protocol (**DHCP**) is a protocol used to assign IP addresses to network devices. A **DHCP server** (software configured on a network server, router, or wireless router) contains a pool of IP addresses known as a **DHCP scope** that defines the starting and ending IP addresses that can be issued to network devices. Commonly on servers or routers, you have to give the DHCP pool/scope a name before entering the range of IP addresses, but on a wireless router used for a home or small business, you just enter the IP addresses and ensure that the DHCP server option is enabled, as shown in Figure 13.61.

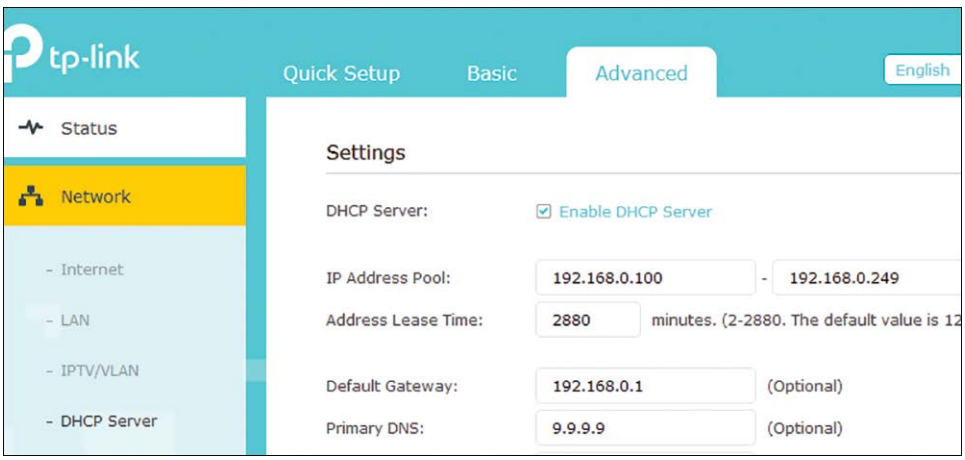


FIGURE 13.61 DHCP configuration on a wireless router

When a network device has been configured for DHCP and it boots, the device sends out a DHCP request for an IP address. A DHCP server responds to this request and issues to the network device an IP address that may be used for a specific period of time, such as a day or longer, depending on the **DHCP lease time** configured on the DHCP server. For example, TP-Link has the lease time in minutes, with a max of 2880, or 2 days (refer to Figure 13.61). DHCP makes IP addressing easy and prevents network devices from being assigned duplicate IP addresses.

An important configuration on a DHCP server is a DHCP reservation, which is an IP address reserved for a particular device, such as a server or printer. Instead of statically assigning an IP address to a device, a technician enters the physical address (the MAC address) of the device, such as a network printer, into the DHCP server and the IP address to be assigned to the device. No other device will get that IP address, and the device will always get the reserved IP address. On the DHCP server, each network is configured with a starting IP address and an ending IP address. A technician can also create a range of reserved IP addresses known as **DHCP exclusions** that will not be issued to network devices by the DHCP server but that can be statically configured on the device as an alternative to making an individual reservation on the DHCP server for each device (see Figure 13.62).

To configure client-side DHCP in Windows, access the *Network and Sharing Center* Control Panel > access the *Change Adapter Settings* link > right-click or tap and briefly hold on the wired and wireless NIC and select *Properties* > double-click or double-tap on the *Internet Protocol Version 4 (TCP/IPv4)* option > ensure the *Obtain an IP address automatically* radio button is enabled (refer to Figure 13.58). In Windows *Settings* >*Network & Internet*, you select either *Ethernet* or *Wi-Fi* from the left menu and then select the Ethernet connection shown in the pane on the right. Scroll to the *IP settings* section and select *Edit*. In the *Edit IP settings* dialog box, use the arrow to select *Automatic (DHCP)*.

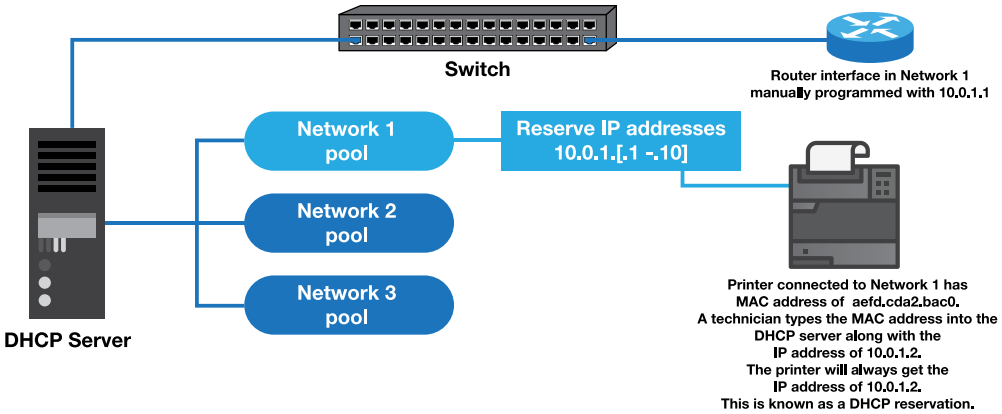


FIGURE 13.62 DHCP reservations

TECH TIP

Watch out for duplicate IP address messages

If a device displays a message related to a duplicate IP address, check the device to see if a static IP address has been assigned (and to see if the DHCP server issued the same address to a different device or vice versa). If a computer cannot communicate on a network, use the `ipconfig` command to verify that the computer received an IP address. If a computer cannot communicate on a remote network, use the `ipconfig` command to verify that the computer received a default gateway.

APIPA

Windows computers support automatic private IP addressing (**APIPA**), which assigns an IP address and mask to the computer when a DHCP server is not available but continues trying to contact the server at five-minute intervals. The IP addresses assigned are 169.254.0.1 to 169.254.255.254. No two computers get the same IP address. If you can connect to other computers on your local network but cannot reach the internet or other networks, it is likely that the DHCP server is down and Windows has automatically used APIPA to assign an address. To determine if APIPA is configured, open a command prompt window and type `ipconfig /all`. If you see the words *Autoconfiguration Enabled Yes*, APIPA is turned on. If the last word is *No*, APIPA is disabled.

Configuring an Alternative IP Address

An alternative configuration is used when a DHCP server cannot assign an IP address, such as when there are network problems or the DHCP server is down. An alternative IP address could also be used on a laptop when DHCP is used at work but addresses are statically assigned at home, for example. Figure 13.63 shows the *Alternate Configuration* tab settings. Note that this tab appears only if you have the *Obtain an IP address automatically* radio button enabled on the *General* tab of the *Internet Protocol Version 4 (TCP/IPv4) Properties* window.

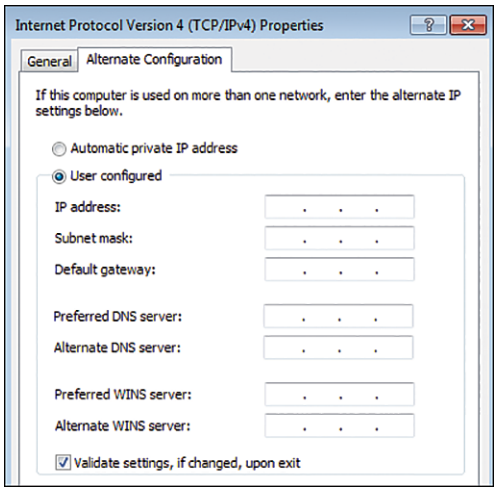


FIGURE 13.63 Alternate Configuration tab

Default Gateway

Another important concept that relates to IP addressing is a default gateway. A **default gateway** (sometimes called *gateway of last resort* or simply **gateway**) is an IP address assigned to a network device that tells the device where to send a packet that is going to a remote network. Default gateway addresses are important for network devices to communicate with network devices on other networks. The default gateway address is the IP address of the router that is directly connected to that immediate network. Keep in mind that the primary job of a router is to find the best path to another network. Routers send traffic from one network to another throughout the internet. Your router at home might be used to get traffic from your wireless network and your wired network out to the internet. Consider Figure 13.64, which shows a router moving traffic from the network on the left to the network on the right (or vice versa).

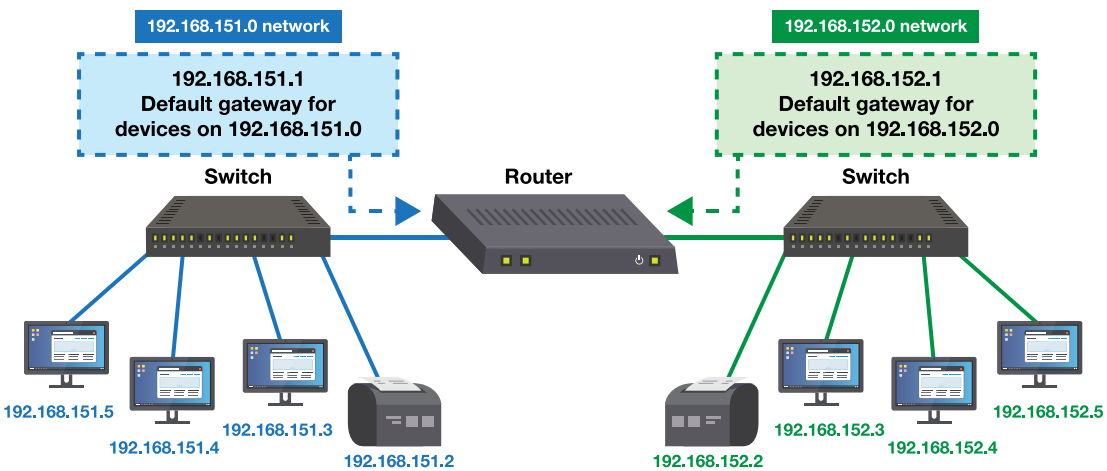


FIGURE 13.64 Default gateway addresses for two different networks

In the network shown in Figure 13.64, network devices on the 192.168.151.0 network use the router IP address 192.168.151.1 as a default gateway address. When a network device on the 192.168.151.0 network wants to send a packet to the other network, the device sends the packet to the default gateway, which is the router. The router, in turn, looks up the destination address in its routing table and sends the packet out the other router interface (192.168.152.1) to the device on the 192.168.152.0 network.

The default gateway address for all network devices on the 192.168.152.0 network is 192.168.152.1, which is the router's IP address on the same network. Any network device on 192.168.152.0 sending information to another network sends the packet to the default gateway address.

TECH TIP

How do I assign a default gateway?

If you are statically assigning an IP address, the default gateway address is configured using the *Network and Sharing Center* Control Panel or *Network & Internet* Settings link. Your computer can automatically receive a default gateway address through DHCP just as it receives an IP address and mask.

DNS

DNS server IP addresses may need to be configured or provided through DHCP. Domain Name Service (**DNS**) is a protocol that runs on a network server (sometimes called a domain name server, or **DNS server**) and translates internet names into IP addresses. DNS is used on the internet so that you do not have to remember the IP address of each site to which you connect. For example, DNS would be used to connect to Pearson Education, Inc. by translating the uniform resource locator (URL) https://www.pearson.com into the IP address 23.197.24.193. Figure 13.65 shows how DNS is organized. An organization can register a second-level domain, but all DNS web address lookups start at the root level.

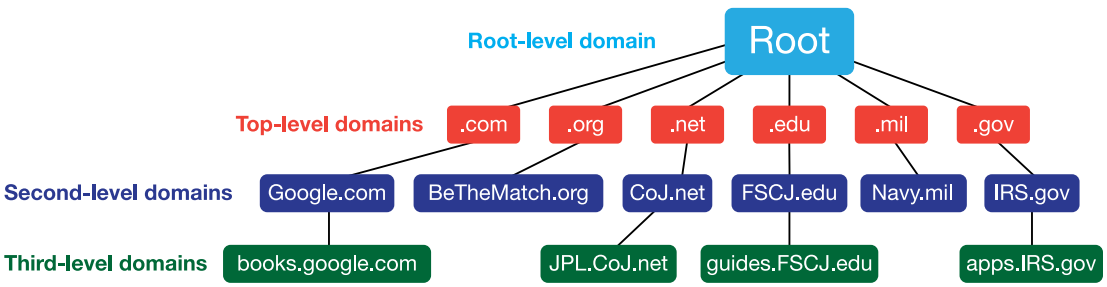


FIGURE 13.65 DNS address hierarchy

Table 13.18 shows common terms associated with DNS.

TABLE 13.18 DNS terminology

Term	Explanation
A record	An address record that holds the IPv4 address of a particular web address. When the A record contains an at (@) symbol, it means the record is for the root domain.
AAAA record	The DNS record that stores a domain's IPv6 address of a particular website.
MX record	A type of DNS record that forwards email to a mail server in another domain. MX stands for mail exchange.
CNAME record	A canonical name (CNAME) record makes managing domains easier by mapping an alias to a specific domain name. For example, www.pearson.com can be mapped to pearson.com.
TXT record	A text record used by administrators for documentation and security (such as email spam prevention and domain verification). Chapter 18, "Computer and Network Security," covers this in more detail.

TECH TIP

DNS servers provide name resolution

If a Windows computer is on an Active Directory domain, Active Directory automatically uses DNS to locate other hosts and services using assigned domain names.

If a DNS server does not know a domain name (that is, if it does not have the name in its database), the DNS server can contact another DNS server to get the translation information. Common codes used with DNS (three letters used at the end of a domain name) are `.com` (commercial sites), `.edu` (educational sites), `.gov` (government sites), `.net` (network-related sites), and `.org` (miscellaneous sites).

Client-side DNS involves configuring a computer to use one or more DNS servers. A computer can be programmed for one or more DNS server IP addresses by using DHCP. The DHCP server must be configured for this. Otherwise, a technician can manually configure the system for one or more DNS server IP addresses through the *Network and Sharing Center* Control Panel or *Network & Internet* Settings link. Refer to Figures 13.58 and 13.59 to see where to enter the information.

Wired and wireless adapters require IP addresses, default gateways, and DNS configuration, but before any wired or wireless adapters are installed or configured, the basic configuration parameters should be determined.

Adding a Computer to a Windows Domain

In a corporate environment, computers are in a network domain. This means that all the network devices are registered with (that is, joined to) one or more network servers, called *domain controllers*, as shown in Figure 13.66.

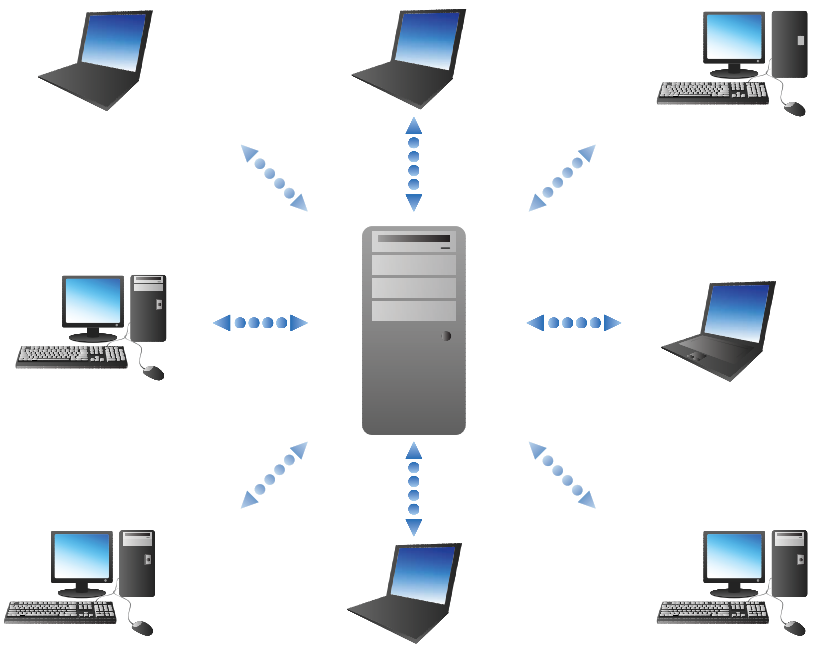


FIGURE 13.66 Corporate computers joined to a domain controller

A technician who has a domain user account that has the appropriate permission can add devices to the domain. On a Windows computer, use the *System* Control Panel to access the *Change Settings* link. In the *Computer Name, Domain, and Workgroup Settings* section > from the *Computer Name* tab, select *Network ID* button > *This computer is part of a business network*

radio button > *Next* > *My company uses a network with a domain* > *Next* > *Next* > enter a domain user account name that has permission to add a computer to the domain and password > enter a computer name and the domain name > *Next*. Restart the computer. You can also use the *Settings* > *System* link and click the *Join a domain* button.

With macOS, use the *System Preferences* option by clicking the *Apple* icon in the top-left corner > *Accounts* > select *Lock* > *Join* button > *Open Directory Utility* button > select *Lock* > highlight *Active Directory* and select the pencil icon > enter the domain name and a unique computer ID > *Bind* button > enter the domain user account name/password that has permission to add a computer to the domain.

Wireless NIC–Specific Settings

Not all computers in a wireless network need the same type of wireless NIC, but each NIC does require configuration to join a wireless network. After a wireless adapter is installed, SSID and security options can be entered. Specific security options are covered in Chapter 18. Wireless parameters can be configured through a utility provided by the wireless NIC manufacturer or through Windows by selecting the wireless network icon in the notification area, selecting the wireless network shown, and entering the required security information.

If the SSID is not being broadcast (that is, if you see **SSID not found** in the list of available wireless networks), a wireless network can be manually entered using the following procedures for Windows: *Network and Sharing Center* Control Panel > *Set up a new connection or network* link > *Manually connect to a wireless network* option (see Figure 13.67).

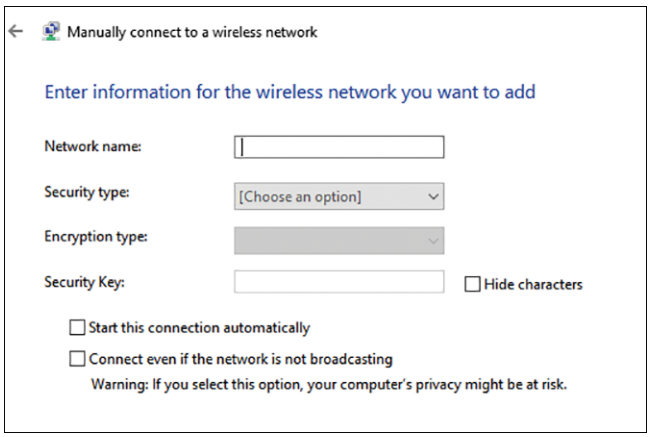


FIGURE 13.67 Manually entering wireless network configuration information in Windows

TECH TIP

Ensure that a laptop's wireless NIC is enabled

If a laptop cannot connect to a wireless network, make sure the wireless NIC is enabled. It can be enabled/disabled through the use of a Fn key.

Another common setting for wireless NICs is the type of encryption used. (Encryption is covered in Chapter 18, along with other wireless security measures.) The following types of encryption can be chosen and must match what is configured on the wireless AP/router (see Figure 13.68):

- **Wireless Encryption Protocol (WEP):** 64- and 128-bit versions
- **Temporal Key Integrity Protocol (TKIP):** May be seen in combination with Wi-Fi Protected Access (WPA) and/or WPA2

> **WPA:** Might be seen with Preshared Keys (PSK), meaning a passphrase and/or TKIP
> **WPA2:** Uses the Counter Mode Block Chaining Message Authentication Code Protocol (CCMP) for added security (might be seen as PSK and/or TKIP)
> **WPA2 with Advanced Encryption Standard (AES):** Uses a block cipher and has key lengths of 28, 192, or 256 bits, with the longer key lengths being the stronger
> **WPA3:** Uses 128-bit (in Personal mode) or 192-bit (in Enterprise mode) encryption and a four-way handshake called Simultaneous Authentication of Equals (SAE) for authentication

FIGURE 13.68 Wireless security options

Wireless NICs are easy to install. Be sure to follow the manufacturer's instructions. All the screens and configuration utilities have the same type of information. Understanding what the configuration parameters mean is important. The hardest part about configuring wireless NICs is obtaining the correct parameters before installation begins. Incorrectly inputting any one of the parameters prevents the wireless NIC from joining the wireless network. Planning is critical for configuring wireless NICs.

Advanced NIC Properties

Both wired and wireless NICs have some optional parameters that can be manually configured. These options are shown in Figure 13.69 and discussed in Table 13.19. Access these parameters by right-clicking the NIC from within the *Networking and Sharing Center* Control Panel > *Properties* > *Configure* button > *Advanced* tab.

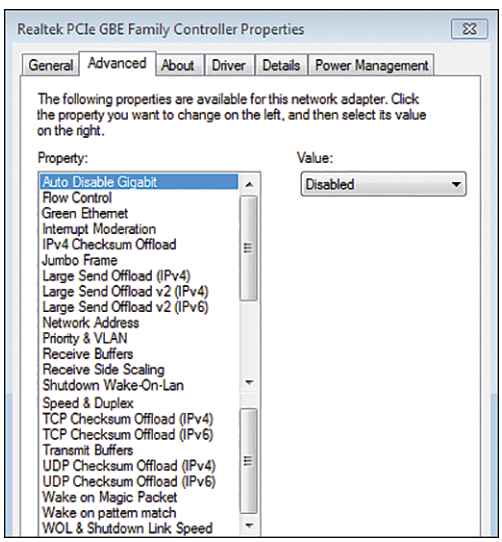


FIGURE 13.69 NIC advanced properties

TABLE 13.19 Network card properties

Configuration property	Description
Duplex	Options include half duplex, full duplex, and auto. The default is auto or auto negotiation. Duplex might be combined with the Speed configuration option. Speed and Duplex should be manually configured on an important device such as a server or checked if the device is experiencing high latency.
On-board NIC (BIOS/UEFI)	If a wired or wireless NIC is integrated into the motherboard or mobile device, you might have to access BIOS/UEFI to configure some of the settings related to the NIC.
Quality of service (QoS)	Some NICs have the capability to have QoS features enabled. This allows tagging certain packets for priority transmission. Other similar options might be Priority and VLAN or Tagging.
Speed (NIC property)	Speed is normally automatically configured, but manual options include 10 Gb/s, 1 Gb/s, 100 Mb/s, and 10 Mb/s.
Wake-on-LAN	This setting allows the computer to be brought out of a low power mode to have configuration changes or updates made. It is usually enabled through the BIOS but can also be set through the NIC properties *Advanced* tab.

NIC Configuration When Using Virtualization

Virtualization allows a single computer to host multiple operating systems that share hardware resources. When you configure a computer for virtualization, part of that virtualization is a virtual network interface card, or **virtual NIC**. One virtual NIC is standard in a virtual machine. More virtual NICs can be assigned. A physical network device has at least one NIC, but if the device is a server, it has more than one NIC.

Each virtual NIC has its own MAC address and can have an IP address assigned. If more than one virtual machine is installed, each can communicate with the other machine(s) based on the NIC settings configured. Furthermore, the virtual NIC can go through the physical NIC and have internet access in the virtual environment. If the virtual machine doesn't have network connectivity, but the host workstation does, verify the virtual NIC settings. Figure 13.70 illustrates three virtual machines (one Linux, one Windows, and one Microsoft Server) in one physical machine connecting to the one physical NIC even though each virtual machine has its own virtual NIC.

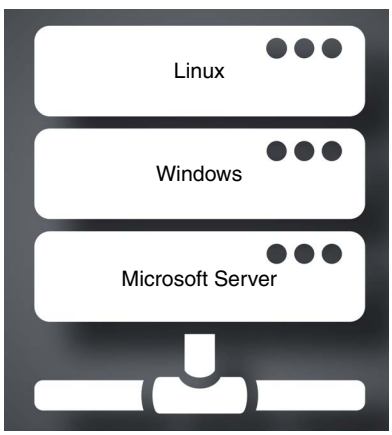


FIGURE 13.70 VMs connecting to a network

Rather than go into all of the different virtualization vendors' products, let's examine VMware Workstation's NIC settings. Other vendors have similar configurations. In VMware Workstation, a NIC can be configured for bridged, network address translation (NAT), host-only, or custom mode. Table 13.20 describes these modes.

TABLE 13.20 Virtualized NIC modes of operation

Mode	Description
Bridged	The NIC is normally manually configured and has access to the host machine's NIC (which normally is connected to the internet and provides internet access to the virtual machine).
Custom	This option allows you to select the VM network that the NIC is assigned to.
Host-only	Other virtual machines configured with an IP address on the same network can see and communicate with one another. DHCP is supported.
NAT (network address translation)	The private IP address assigned to a VM cannot be seen by other virtual machines but a VM can use the host machine's NIC for internet access. DHCP is also supported.

Wireless AP/Router Configuration

A wireless router frequently has the capability to route. This type of device is made for a small office/home office (SOHO) environment. The graphical environment used to configure a SOHO AP varies by vendor, but the process is common. Some of the specific configuration tasks have already been shown such as DHCP configuration, but the generic steps for configuration follow:

Step 1. Connect an Ethernet cable between the wireless AP and another device that has a web browser.

Step 2. Open a web browser and in the address textbox, enter the default IP address of the AP, such as `http://192.168.1.1`.

Step 3. Enter the default username (if needed) and default password.

TECH TIP

Change the default username/password

When an access point or wireless router is purchased, a default username and/or password is assigned. Because default passwords are available on the internet, the password needs to be changed immediately so that unauthorized access is not permitted. Manufacturers recognized this weakness, and as a result, many newer devices enable you to create a password during the initial setup.

Typical AP configuration menu options are shown in Table 13.21.

TABLE 13.21 Common AP configuration options

Option	Description
Wireless	Used to configure basic wireless settings, such as the SSID. Also includes a link to security options such as MAC filtering, authentication, and encryption (covered in Chapter 18).
Security	Used to enable/disable a firewall and configure firewall features such as a VPN or allow particular network ports to be opened to allow certain types of traffic through. A **firewall** is a device or software that can inspect data for security purposes and filter traffic based on configured rules.

Option	Description
Storage	Allows monitoring and control of an attached storage device and can even support a File Transfer Protocol (FTP) server.
Maintenance	Allows viewing of the current status of the various components as well as access to any logging that is enabled.
Administration	Allows configuration of the device, such as **secure management access** (password and remote capabilities), IP address assignment, and event logging. Could also include configuration of features such as VoIP or QoS. QoS allows one type of traffic such as voice to take priority over another type of traffic.

Wireless SOHO access points/routers frequently include network functions such as a demilitarized zone (**DMZ**), also known as a **screened subnet**, QoS, a DHCP server (sometimes seen as the DHCP on/off setting), a router, integrated switch ports, and a port to add a hard drive and support network-accessible storage. Chapter 18 provides explanations and configuration details related to wireless security, and Table 13.22 introduces some common configuration features.

TABLE 13.22 Common wireless network device configuration settings

Option	Description
Basic QoS	Used to enable QoS so that traffic such as gaming traffic or VoIP traffic is prioritized over other data types.
IP filtering	Uses lists to control which users, websites, IP addresses, protocols, and apps can be used on a device. A deny setting blocks, whereas an allow setting specifically permits network traffic.
Content filtering	Blocks access to specific web pages. Might also include a date/time range. Also called URL or web filtering.
Channel ID	Used to specify a particular 2.4 GHz or 5 GHz channel.
Demilitarized zone (DMZ)	A separated corporate network that allows a server to be accessed from a remote location. Also called DMZ host or **screened subnet**.
DHCP	Used to enable or disable DHCP as well as the specific network number, mask, and range of addresses to use.
Firmware	Used to update the embedded code within a device. Frequently contains security, performance, and software updates.
Network address translation (NAT)/ destination NAT (DNAT)	NAT, which is used to translate from private IP addresses to a public address, is enabled by default. DNAT maps a public IP address to a specific private IP address and is used in a home or small business network.
Port forwarding	Provides an alternative to using a DMZ in which specific port numbers, ranges of port numbers, and applications are allowed to be used instead of opening all ports. One example of this is when a small company has a web server inside the company, and the server needs to be accessed by external users. Also called port mapping. A similar concept is port triggering which allows data through on a limited basis when a specific/ configured situation occurs.
SSID	Used to name a wireless network. An SSID cannot contain spaces. There is commonly an option to enable or disable SSID broadcasting.
Universal Plug and Play (**UPnP**)	Used as an alternative to port forwarding to allow peer-to-peer (P2P) gaming applications to function without further configuration. Could be a security risk for other devices on the network.

WWAN Cellular Configuration

Another type of wireless device that you might configure is a wireless broadband device or a WWAN (cellular) connection. A wireless broadband (WWAN cellular) device can be a USB device, it can be integrated into a mobile device, or it can be an external device that serves as a hotspot. A USB device commonly has a phone number/account number associated with the broadband card. Figure 13.71 shows the type of information provided for a wireless broadband USB device.

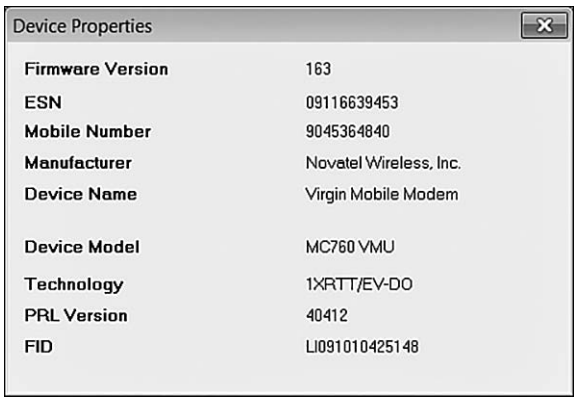


FIGURE 13.71 WWAN cellular properties

IoT and Smart Devices

Internet of Things (**IoT**) is a term that describes the interconnectivity of sensors and devices that connect to a network (usually a wireless one). The IoT has affected all industries, and home devices are particularly common. Smart homes (see Figure 13.72) are becoming popular, and even older existing homes can be made smart.

FIGURE 13.72 Smart home controls

Smart homes include devices that can monitor water consumption, air and heat, and electricity. In addition, it is possible to control locks, lights, thermostats, garage doors, computers, sound systems, TVs, and refrigerators—and the list keeps growing. Smart devices are controlled through an app on a phone, tablet, laptop, or computer. These devices can connect to a wired Ethernet network, an 802.11-based wireless network, or using other standards, such as LoRa, MQTT, Zigbee, and Z-Wave.

IoT devices are very susceptible to security breaches because of the lack of standardization within the industry; in addition, IoT devices are incapable of supporting security due to the lack of hardware. They also provide an easy target if they connect to other networks, such as 802.11 or Ethernet networks. Here are some security suggestions for implementing IoT devices:

- Research the company and protocol(s) used to connect the devices. Make a selection based on a good security track record.
- Encrypt the IoT data sent between the devices and the systems that receive the data.
- Require user authentication to access the IoT devices.
- Secure the IoT network. Industry security leaders offer IoT solutions.
- Ensure that any communication between an IoT device and an app uses proven security methods.

Network Troubleshooting

A network has a lot of moving parts, and so there are a lot of different ways to set about troubleshooting it. Some traditionalists would say to use the OSI model and start troubleshooting at either Layer 1 or Layer 7. One quick method is to check the network status of a particular machine. Let's start there.

Network Status

Windows has an icon in the bottom-right corner of the taskbar that shows internet connectivity as either Connected (Wired), Connected (Wireless), or Connected (No internet). You can also use the *Network & Internet* Settings link to get a quick look at whether your network connection is up and whether you have internet connectivity (see Figure 13.73).

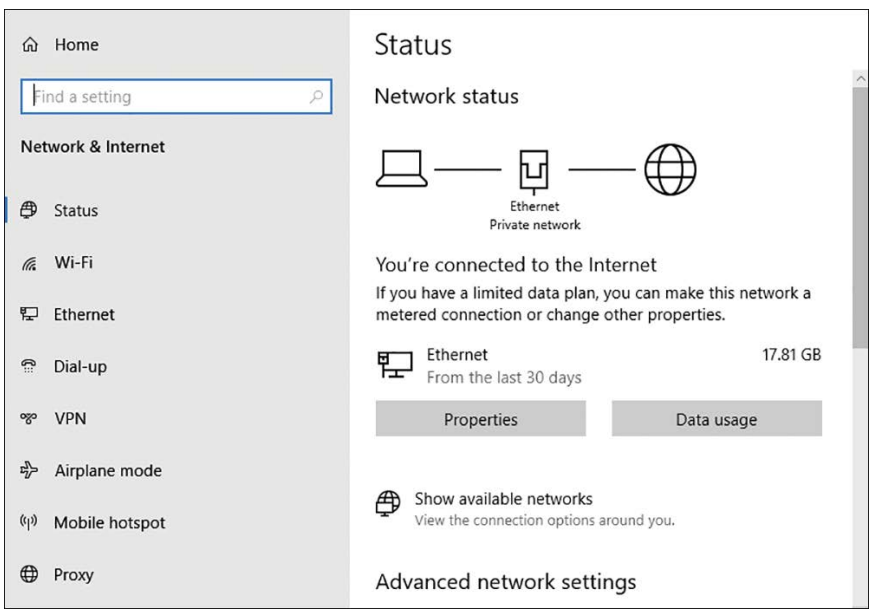


FIGURE 13.73 Windows Network & Internet Settings window

From this screen you can see whether you have a wired Ethernet connection or a wireless connection. You can select the *Properties* button and scroll to the *Properties* section to see IP and MAC address information. Other options you might see include the following:

- **No internet access:** Check your internet router. Reboot it. Check for an outage in the area.
- **Limited connectivity:** The computer knows it is connected to a network, but it cannot fully connect. You can try rebooting the computer and internet router. Check cabling. See if your NIC is enabled (as discussed shortly). Use the `ipconfig` command to see if your computer has an IP address assigned to it.
- **Identifying:** The computer is trying to get an IP address from a DHCP server. If this continues, try restarting the PC and the internet router.

You could also use the Windows network troubleshooter to help with these issues.

Another method of network troubleshooting is to determine how many devices are affected. For example, if only one computer cannot communicate across a network, it will be handled differently than if several (or all) computers on the network cannot communicate. If a computer cannot get on a network at all, it might not have appropriate IP addressing information, or it may not be joined to a domain. If a network port is suspect, ensure that the interface is enabled, try another cable, or use a loopback plug to test the port. The easiest way to determine how many devices are having trouble is by using the `ping` command.

The `ping` Command

The `ping` command can be used to check connectivity from one network device to another device (if you suspect **no connectivity**, **no internet connectivity**, or **intermittent connectivity/limited connectivity**). Figure 13.74 shows the sample network used here to illustrate how `ping` is used to check various network points.

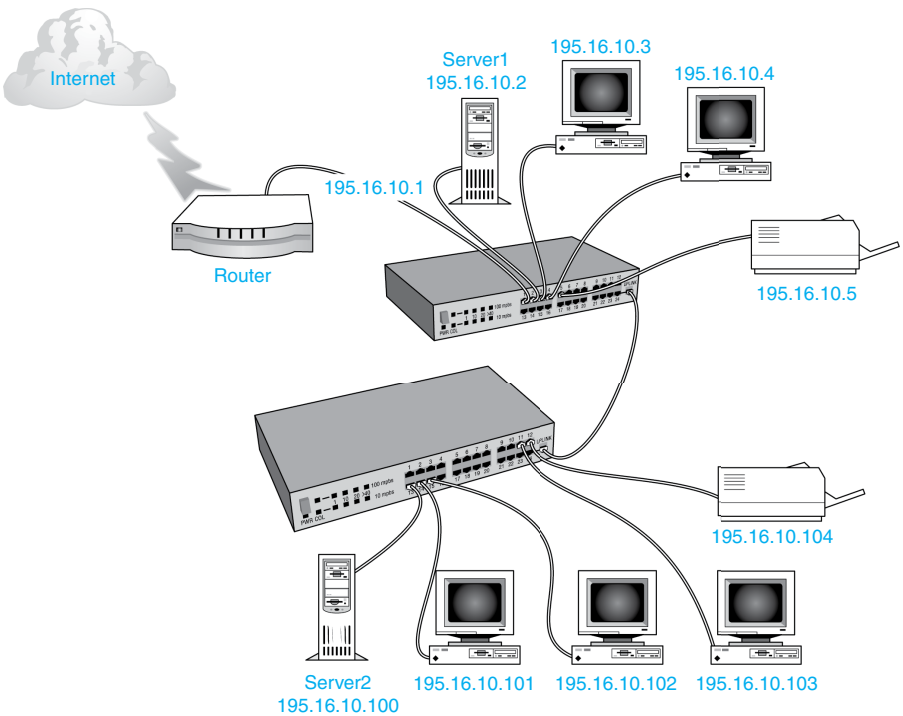


FIGURE 13.74 Sample network troubleshooting scenario

TECH TIP

What does `ping` do?

The `ping` command can be used to determine whether a network path is available, whether there are delays along the path, and whether a remote network device is reachable. `ping` sends a packet to an IP destination (that you specify), and a reply—indicated by an exclamation point (!)—is sent back from the destination device if everything works fine. A series of dots show when there is an issue.

The network shown in Figure 13.74 consists of various network devices, including two servers and two laser printers. The devices connect to one of two switches that are connected using the uplink port via an Ethernet cable or a fiber cable. A router connects to the top switch, and the router connects to the internet.

If the 195.16.10.3 workstation cannot access a file on Server2 (195.16.10.100), the first step in troubleshooting is to ping Server2 from the workstation. If this ping is successful, you know the problem is with Server2 or the file located on the server.

If the ping is unsuccessful, you know there is a problem somewhere between the workstation and the server or on the server. To test this, ping another device that connects to the same switch; for example, from workstation 195.16.10.3, ping Server1 (195.16.10.2). A successful ping tells you the connection between the 195.16.10.3 workstation and the switch is good, the switch is working, the cable connecting to Server1 is fine, and Server1 is functioning. If the connectivity is intermittent (that is, if you get one or two out of numerous pings), this could be a result of a **port flapping** (that is, a port going up and then down) due to faulty cabling or a faulty port.

What Resources Are Unavailable?

One of the first signs of network issues is a user complaining about **unavailable resources**. This might mean the user can't reach the internet or can't reach local resources within the company, such as network shares, printers, or email. Troubleshooting each of these problems helps you narrow down where you should ping and verify exactly what network resource(s) cannot be reached.

Pinging devices on the same network is a good check of local connectivity. The term *local connectivity* describes devices on the same network, including the default gateway. If a network device can ping other devices on the same network as well as the default gateway, the network device (and all its components and basic settings) are configured correctly.

TECH TIP

Use `ping -t`

Use `ping x.x.x.x -t` (where you replace `x.x.x.x` with an IP address or a URL) to issue a continuous ping to a remote location. When you do, the ping does not stop until you press Ctrl+c.

Now check connectivity to workstation 195.16.10.101 (a device other than the server on the remote switch) by typing `ping 195.16.10.101`. If the ping is successful, you know that (1) the uplink cable is operational; (2) the second switch is operational; (3) the cable that connects workstation 195.16.10.101 to the switch is good; and (4) the 195.16.10.101 workstation has been successfully configured for TCP/IP. If the ping is unsuccessful, you know that one of these five items is faulty. The problem could be (1) the Server2 cable, (2) the switch port to which the server connects, (3) the server NIC, (4) the server configuration, or (5) the file on Server2.

TECH TIP

How can I check the TCP/IP protocol stack on my own NIC?

The `ping` command can be used to test a NIC as well as the TCP/IP protocol running on the NIC, with the command `ping 127.0.0.1` (IPv4), `ping ::1` (IPv6), or `ping localhost`, where *`localhost`* is a hostname that is translated to an IP address known as a private IP address, or loopback address, which means it cannot be used by the outside world.

Use the `ping` command followed by the name of the device (or website) being tested (for example, `ping www.pearson.com`). A DNS server translates the name (pearsoned.com) to an IP address (23.197.24.193). If you can reach the site by pinging the IP address, but not the name, there is a problem with the DNS server.

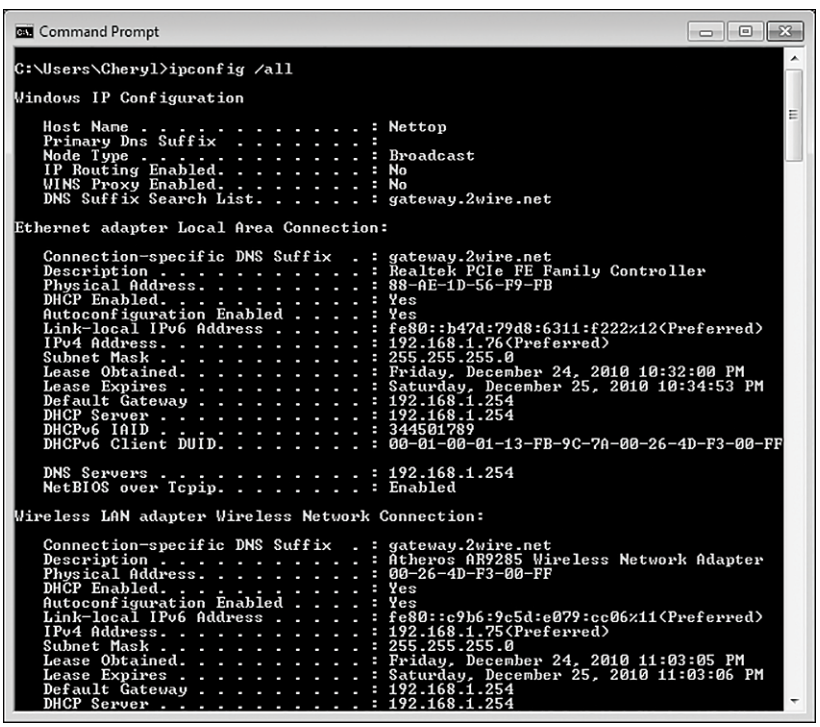
TECH TIP

What the `ping localhost` results mean

If a ping is successful (that is, if you get a message indicating that a reply was received from 127.0.0.1 or ::1), you know the TCP/IP protocol stack works correctly on the NIC. If the ping response is nothing (appears to hang) or a 100% packet loss error, you know that TCP/IP is not properly installed or is not functioning correctly on that particular device.

The `ipconfig` Command

To see the current IP configuration on a Windows computer, use the `ipconfig` command from a Windows command prompt or the `ifconfig` or `ip addr` command with Linux or macOS. The `ipconfig /all` command can be used to see both wired and wireless NICs if both are installed, as shown in Figure 13.75. The `ipconfig /all` command also allows you to view MAC addresses.



```
Command Prompt
C:\Users\Cheryl>ipconfig /all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : Nettop
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Broadcast
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No
   DNS Suffix Search List. . . . . . : gateway.2wire.net

Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . : gateway.2wire.net
   Description . . . . . . . . . . . : Realtek PCIe FE Family Controller
   Physical Address. . . . . . . . . : 88-AE-1D-56-F9-FB
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::b47d:79d8:6311:f222%12(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.1.76(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Friday, December 24, 2010 10:32:00 PM
   Lease Expires . . . . . . . . . . : Saturday, December 25, 2010 10:34:53 PM
   Default Gateway . . . . . . . . . : 192.168.1.254
   DHCP Server . . . . . . . . . . . : 192.168.1.254
   DHCPv6 IAID . . . . . . . . . . . : 344501789
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-13-FB-9C-7A-00-26-4D-F3-00-FF

   DNS Servers . . . . . . . . . . . : 192.168.1.254
   NetBIOS over Tcpip. . . . . . . . : Enabled

Wireless LAN adapter Wireless Network Connection:

   Connection-specific DNS Suffix  . : gateway.2wire.net
   Description . . . . . . . . . . . : Atheros AR9285 Wireless Network Adapter
   Physical Address. . . . . . . . . : 00-26-4D-F3-00-FF
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::c9b6:9c5d:e079:cc06%11(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.1.75(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Friday, December 24, 2010 11:03:05 PM
   Lease Expires . . . . . . . . . . : Saturday, December 25, 2010 11:03:06 PM
   Default Gateway . . . . . . . . . : 192.168.1.254
   DHCP Server . . . . . . . . . . . : 192.168.1.254
```

FIGURE 13.75 `ipconfig /all` command output

A network device may not properly get an IP address from the DHCP server. A symptom of this problem is a device getting an APIPA (IPv4) or link-local (IPv6) address because a DHCP server is unavailable. When this occurs, use the `ipconfig /release` and then issue the `ipconfig /renew` command. Also ensure that the device is specifically configured for DHCP. A message appears on Windows-based devices when two devices have been manually assigned the same IP address. Check any device that has a manually configured IP address for any duplicate IP addresses that are causing an IP address conflict.

The `tracert` and `pathping` Commands

The `tracert` command is a commonly used tool in Microsoft, macOS, and Linux environments. The `tracert` command is used to display the path a packet takes through the network. The benefit of using the `tracert` command is that you can see where a fault is occurring in a larger network. It also allows you to see the network latency. Network latency is the delay measured from source to destination; **high latency** can mean slow network speeds. The `tracert` command is also useful when you have intermittent connectivity. An example of output from the `tracert` command is provided in Figure 13.76.

```
C:\Users\Cheryl>tracert comptia.org
Tracing route to comptia.org [198.134.5.6] over a maximum of 30 hops:
 1 <1 ms <1 ms <1 ms vankman1 [192.168.1.1]
 2 8 ms 7 ms 8 ms 10.126.208.1
 3 10 ms 8 ms 7 ms 72-31-92-20.net.bhntampa.com [72.31.92.20]
 4 11 ms 14 ms 12 ms ten0-6-0-11.tamp27-car1.bhn.net [71.44.3.186]
 5 17 ms 16 ms 19 ms hun0-4-0-3.tamp20-car1.bhn.net [72.31.117.170]
 6 22 ms 19 ms 18 ms ten0-8-0-0.orld71-CAR1.bhn.net [71.44.1.211]
 7 17 ms 16 ms 19 ms 72-31-217-88.net.bhntampa.com [72.31.217.88]
 8 23 ms 19 ms 14 ms 10.bu-ether15.orldfljo00w-bcr00.tbone.rr.com
[66.109.6.98]
 9 36 ms 31 ms 31 ms bu-ether18.atlngamq47w-bcr01.tbone.rr.com [66.109.1.72]
 10 23 ms 23 ms 24 ms 0.ae2.pr1.atl20.tbone.rr.com [107.14.17.188]
 11 26 ms 29 ms 23 ms 67.106.215.89.ptr.us.xo.net [67.106.215.89]
 12 50 ms 51 ms 50 ms 207.88.13.54.ptr.us.xo.net [207.88.13.54]
 13 52 ms 56 ms 49 ms 207.88.12.174.ptr.us.xo.net [207.88.12.174]
 14 50 ms 51 ms 51 ms 207.88.12.31.ptr.us.xo.net [207.88.12.31]
 15 49 ms 57 ms 55 ms ae0d0.mcr1.chicago-il.us.xo.net [216.156.0.162]
 16 54 ms 52 ms 53 ms 216.55.11.62
 17 52 ms 60 ms 52 ms 198.134.5.6
Trace complete.
```

FIGURE 13.76 Sample output of `tracert`

A similar command available in the Windows environment is `pathping`, which is sort of a combination of the `ping` and `tracert` commands. The `ping` command checks for connectivity between one network device and another device, and `tracert` displays the IP addresses of the routers between the source and destination addresses. `pathping` provides additional information, including the network latency and loss between the source and destination. `pathping` takes longer to execute than the ping or tracert commands. Sample output is provided in Figure 13.77.

High latency in wireless networks is caused by interference from devices operating in the same frequency range, obstacles such as walls and concrete, and distance from the access point. High latency in wired networks is typically caused by poor or faulty cabling and/or security issues.

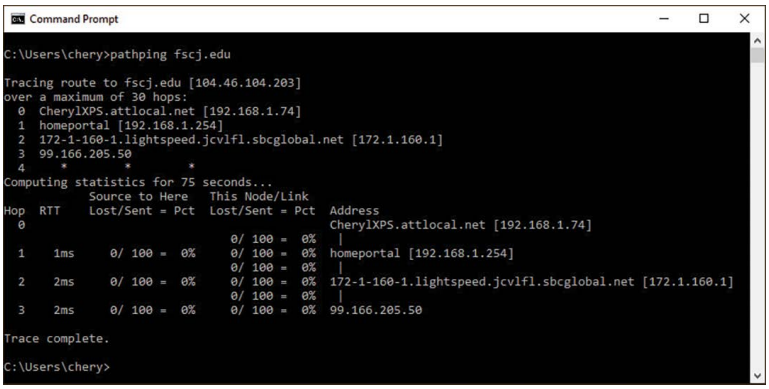


FIGURE 13.77 Sample output of `pathping`

The `nslookup` Command

The `nslookup` command is a tool that helps with DNS server troubleshooting. `nslookup` enables you to see domain names and their associated IP addresses. When an internet site (server) cannot be contacted by its name but can be contacted using its IP address, there is a DNS problem. The `nslookup` command can make troubleshooting these types of problems easier. To see this tool in action, bring up a command prompt, type `nslookup pearson.com`, and press Enter. The IP address of the Pearson web server appears. Note that if the `nslookup` command shows a domain name such as a computer, but the domain name cannot be used to contact the device, the `ipconfig /flushdns` command can be used to clear the DNS cache.

The `net` Command

The `net` command is used to manage just about everything on a network from a command prompt. The `net` command is followed by other options, and each option has different parameters. Here is the command syntax:

```
net [ accounts | computer | config | continue | file | group | help
| helpmsg | localgroup | name | pause | print | send | session |
share | start | statistics | stop | time | use |user | view ]
```

Table 13.23 lists some of the most commonly used `net` command options.

TABLE 13.23 `net` command options and descriptions

Command	Description
`net help`	Used to get help for the `net` commands. You can also use `net help computer` or `net computer /help` or `net computer /?`.
`net computer`	Used to add or remove a computer in a Microsoft domain.
`net config`	Used to display information about a server or workstation service.
`net share`	Used to create, remove, or view network share resources.
`net start`	Used to start a network service.
`net stop`	Used to stop a network service.
`net use`	Used to map a drive letter to a network resource.
`net user`	Used to manage user accounts.
`net view`	Used to view network devices.

The `netdom` Command

The `netdom` command, which is similar to `net`, is used to manage workstations in a domain environment. Use the `netdom /?` command to see all the options. Table 13.24 shows some of the most popular `netdom` command options.

TABLE 13.24 `netdom` **command options and descriptions**

Command	Description
`netdom add`	Used to add a workstation account to a domain
`netdom join`	Used to join a workstation to a domain
`netdom remove`	Used to remove a workstation from a domain
`netdom renamecomputer`	Used to rename a computer and its domain account
`netdom reset`	Used to reset the connection between a workstation and a network domain controller
`netdom resetpwd`	Used to reset the computer account password
`netdom verify`	Used to verify the connection between a workstation and a Microsoft domain controller

NIC Troubleshooting

The following methods can help with NIC troubleshooting:

- In a command prompt window, use `ping localhost` to test the NIC.
- Ping another device on the same network. If the ping is successful, you know the NIC, device, cable, switch, and hub are all working.
- Ping the default gateway. If the ping is successful, you know connectivity and configuration of the device for communication on the local network work, and the device has the potential to communicate with other networks.
- Ping a device on a remote network. If the ping is successful, you know the Layer 3 device serving as the default gateway is working.
- Use the `tracert` command to determine the location of the fault (such as whether the problem is inside or outside the company).
- Check the status light(s) on the NIC (see Figure 13.78) to see if the physical connection is good. Different NICs have lights of different colors, but the two most common colors used with status lights to indicate a good connection are green and orange. Some status lights indicate the speed at which the NIC is operating (10 Mb/s, 100 Mb/s, or 1 Gb/s).
- Check the status light on the hub or switch (see Figure 13.79) that is used to connect the workstation NIC to the network. Green is a common color for a good connection on these devices.

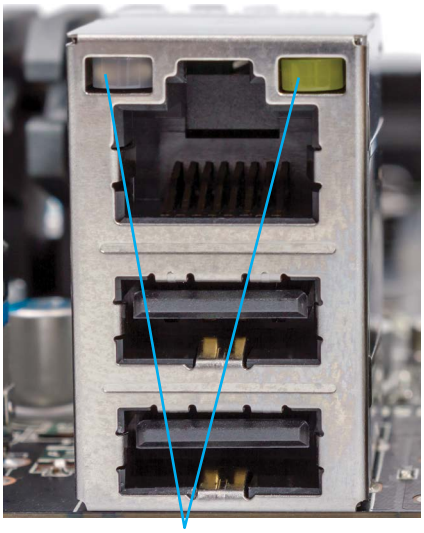


FIGURE 13.78 NIC status lights

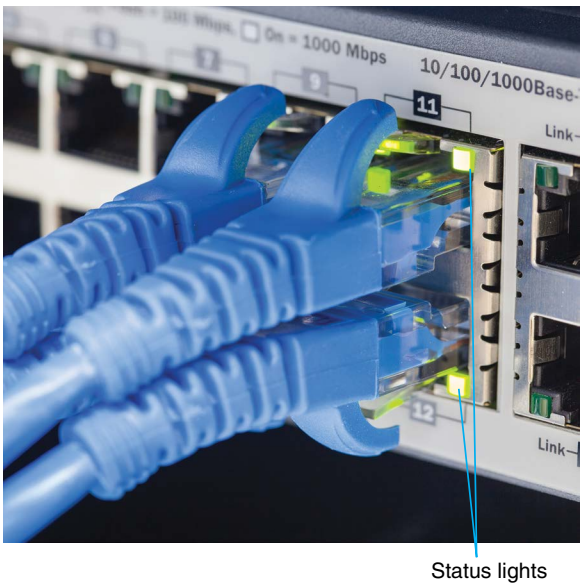


FIGURE 13.79 Switch or hub status lights

- Check cabling. Even if the status lights indicate that the connection is good, the cabling may still be faulty.
- Update the device driver by obtaining a newer one from the NIC manufacturer's website.
- Check the IP addressing used. Use the `ipconfig` command from a prompt to ensure that the NIC has an IP address assigned. If you get a duplicate IP address error message, change the IP addressing to DHCP or another statically assigned address (that has not already been used).
- On a mobile device, ensure that wireless is enabled and that the wireless NIC is enabled. Look for a button or a keystroke combination that re-enables the wireless antenna and ensure that the NIC is not disabled in the *Network and Sharing Center* Control Panel.
- If your network connection on the desktop or from within the *Network and Sharing* section of the Control Panel shows limited connectivity (see Figure 13.80) or if you cannot reach the internet at all, try rebooting the PC (because of a 169.254.*x.x* address) or the router (if in a home or small business network). With a wireless connection, check security settings, the

wireless button that controls the wireless antenna, or a wireless key that toggles the wireless NIC. If on a wired network, the cable could be an issue.

> If the network connection is intermittent or slow on a wireless connection, move closer to the AP, change the position of the wireless device, or add another AP in the area to extend the wireless network. On a wired connection, check cabling and duplex settings. Replace a hub with a switch.

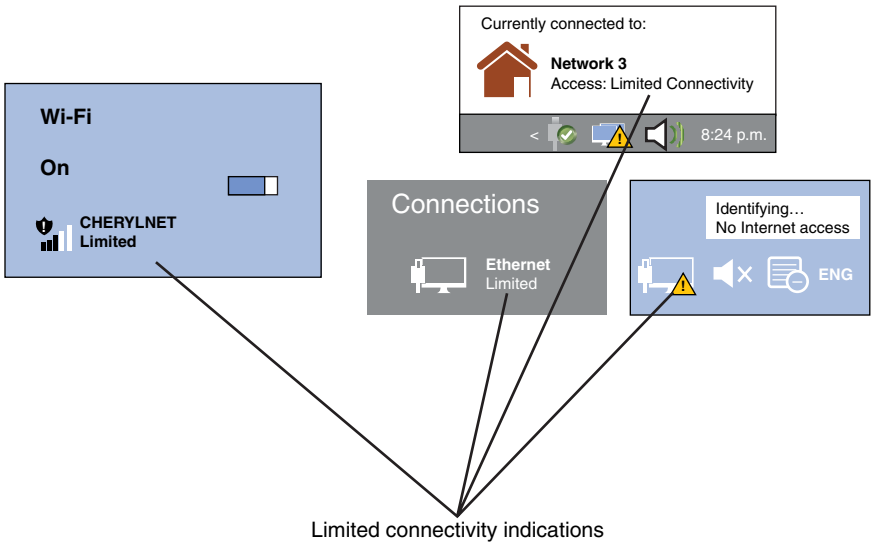


FIGURE 13.80 Windows limited connectivity network indications

Troubleshooting Cable and DSL Modems

Because most cable and DSL modems are external, the best tools for troubleshooting connectivity problems are the lights on the front of the modem (see Figure 13.81). The lights vary from vendor to vendor, but common ones are listed in Table 13.25.

FIGURE 13.81 Cable/DSL modem lights for troubleshooting

TABLE 13.25 Cable/DSL modem lights and troubleshooting*

Light	Explanation
Cable, Data, or D/S	Usually blinks to indicate connectivity with internet provider
ENET, E, or Ethernet	Usually indicates connectivity between the PC and the modem; if unlit, ensure that you are using Ethernet (though if using USB, this will be unlit), check cabling, and check PC network card settings
Internet, Ready, or Rdy	Stays lit when the modem has established an internet connection

Light	Explanation
Link Status	Usually flashes when acquiring a connection with a provider and is steadily on when a link is established
PC	Used instead of Ethernet or USB lights to show the status of the connection between the modem and the PC
Power	Indicates power to the modem
USB or U	Usually indicates connectivity between the PC and the modem; if unlit, ensure that you are using USB (though if using a NIC, this light will be unlit), check cabling, and check *Device Manager* to see if the modem is recognized

* Refer to the modem documentation for the exact status of the lights.

After you have checked lights and possibly checked cables, if you still have a problem, power off the modem, wait two minutes, power the modem back on, and reboot the computer. Give the modem a couple minutes to initialize. Most modems have a reset button that can also be used, but when you use that button, you wipe all the configuration information; powering off and powering back on works without wiping that information. If a modem is still not working after you take these steps, contact the service provider.

Networking Multifunction Devices

Chapter 9, "Printers/Multifunction Devices," describes how to share a printer or multifunction devices across a network as well as how to access a wired or wireless network printer. Now that you know a bit more about networking, the processes outlined in Chapter 9 might be easier to understand.

Printer sharing is commonly done in a home or small business environment. In a corporate environment, a **print server** is used, and printers are published or visible to users and devices on the network. A network printer will definitely have an IP address assigned. Users can perform network printer mapping, which enables network users to add a printer to their computer by using the domain printer name or the printer's IP address. To find printers by name in a corporate network domain, use *File Explorer* to explore the network for printers.

You can also use a Control Panel or Windows Settings link to add a network printer:

- Access the *Add Printer* Control Panel link > enable the *Select a shared printer by name* radio button and enter the domain name (an example might be the domain name SchmidtCo, in this format: \\SchmidtCo\) and select from the printers that are listed.
- Add the printer by using the printer's IP address. A network printer commonly has a front panel that is used to access network configuration settings. A printer that connects directly to the network through a wired or wireless connection has a statically configured IP address, mask, and default gateway. Many times technical support staff attach a label to the printer that shows the IP address. You could access the network settings from the *Devices and Printers* > *Printers* section of the Control Panel to view the assigned IP address. Refer to Chapter 9 for how to connect using a printer's IP address.
- Use the *Printers & scanners* Settings link > *Add a printer or scanner* > *Add device* box. If you don't see the printer listed, select *Select a shared printer by name* and enter the network share name.

Network Printer/Scanner Services Configuration

Networked printers, copiers, scanners, and multifunction devices might include network services that provide the ability to copy/scan a document and email it to someone or to put a copied/scanned document in a network folder. Typically when configuring a device to be able to email a document, you must provide the following information:

- IP address of the email server (which might be listed in the settings as the Simple Mail Transfer Protocol [SMTP] gateway)
- The port number used for the server, obtained from the network administrator who manages the email server
- The email account created by the administrator for the printer
- On some devices, a standard subject line for any documents emailed from the device

Devices might also be able to store a copied or stored document in a network folder. Make sure you know the network path to the shared folder and ensure that the folder permissions are set to allow new files to be placed into the folder. (Directions on how to share a folder are given later in this chapter.) An example of a network path is `\\CherylXPS\ScannedDocs`, where the first part is the network device name and the second part is the name of the shared folder. Configuration on the network device used to scan/copy the document typically requires the following:

- A name that appears in the device's address book. This name should be descriptive so that anyone who wants to store a document in the network folder will recognize it. An example is Shared Scanned Documents.
- The protocol used by the device to send the document to the folder. The most common one used is Server Message Block (**SMB**), though you might also see Common Internet File System (**CIFS**).
- The IP address of the SMB server or the device that holds the shared folder.
- The network path to the shared folder.
- The username/password used to put files in the shared folder. This may have to be obtained from the network administrator of the SMB server.

Network Printer/Scanner Troubleshooting

To begin troubleshooting a network printer, do all the things that are normally done when troubleshooting a local printer (refer to Chapter 9) and check the obvious things first. Does the printer have power? Is the printer online? Does the printer have paper? Are the printer's connectors secured tightly? Is the correct printer driver loaded? If all these normal troubleshooting steps check out correctly, try the following:

- Print a test page and see if the printer's IP address outputs or see if the printer is labeled with its IP address. If so, ping the printer's IP address to see if there is network connectivity between the computer and the printer. Use the `tracert` command to see if there is a complete network path to the printer.
- Check the printer's *Properties* page to see if the printer has been paused.
- Cancel any print jobs that are in the print queue and resubmit the print job.
- Reset the printer by powering it off and back on. If it connects to a print server device, reset that, too.
- Be sure the print job has been sent to the correct printer. Companies commonly have several network printers to use.

> If a network printer fails and a user has a USB-attached printer, share the USB printer. (Chapter 9 shows how to share a printer across a network.)
> If the printer has never worked, try a different version of the print driver.

Network Servers

Servers are an important part of networking and provide different functionality. One server may provide more than one function. For example, a corporate server might act as a web server and also as a DHCP server. In addition, each physical box could contain several virtualized servers. Figure 13.82 shows several network servers mounted in a rack.

FIGURE 13.82 Network servers

Table 13.26 describes the most common servers on a network.

TABLE 13.26 Server types and descriptions

Server type	Description
Authentication server	Used to verify credentials (usually username and password), such as when someone logs in to a domain workstation. Sometimes called an authentication, authorization, and accounting server (**AAA server**).
Database server	Holds data for applications and users in an organized way so that the data can be stored, organized, managed, and analyzed for business operations.
DHCP server	Used to issue IP-related information, including IP address, subnet mask, default gateway, DNS server, and domain name. Commonly has a block of addresses that are in a pool to be assigned to common devices such as PCs and IP phones. A few addresses are reserved for statically assigned devices such as routers, switches, APs, and printers.
DNS server	Used to translate domain names to IP addresses.
End-point management server	Used as a centralized solution for discovering devices, distributing software, provisioning, updating, configuring, managing security, managing profile, imaging/re-imaging computers, and managing inventory.
File server	Used to store files that can be accessed and managed from a remote location. Sometimes called a **fileshare server**.

Server type	Description
Mail server	Used to maintain a database of email accounts, store (email) messages sent and received, communicate with other mail servers, and use the DNS protocol to locate other servers. Also known as an email server.
NTP server	Used to synchronize time across network devices, based on Network Time Protocol (NTP). This is important for logs, especially when problems occur.
Print server	Used to manage one or more network printers. See Chapter 9 for more information.
Proxy server	Used as a go-between between an application such as a web browser and a physical server. Details on how to configure a network device for a proxy server are provided in Chapter 18.
Syslog server	Used to receive information from multiple network devices and used as a historical record of events such as devices losing power, a particular interface going down, and logins or logouts on a particular device. Also called a logging server.
Web server	Used to provide web-based content that is accessed through a web browser that commonly requests the information through TCP port 80 or secure port 443.

Authentication Issues

Whether you are trying to get onto a network or using a network resource such as a printer, you must provide credentials via a username and password or code. The most common **authentication failure** issue is forgotten user ID and/or password, but there can be other issues as well. The authentication server could be down, or a network issue may be causing the server to be unreachable. Or the server may have been misconfigured. Some authentication types have expiration dates and may need to be renewed in some way that causes additional steps. Finally, an account may have been hacked or had its credentials stolen.

No matter the cause of an authentication issue, a technician must try to eliminate some of the "what ifs" by determining whether others can get onto the same network. Can someone else who has the appropriate permission access the same file or resource? Document as much information as possible and then, if the problem is indeed a network problem, escalate it to the network team.

Embedded, SCADA, and Legacy Systems

An **embedded system** is a computer that has a specific function within a larger system. Embedded systems have many of the same components as desktop or mobile computers: processor, RAM, flash memory, and ports. Embedded systems can be found in many places, including airports, manufacturing plants, medical equipment, electrical systems, mechanical systems, and telecommunication systems. Embedded systems tend to be self-contained, but they commonly attach to wired or wireless networks and may be part of an IT person's responsibility.

Closely related to an embedded system is a supervisory control and data acquisition (**SCADA**) system. These systems are used in just about every industry you can think of, including power, water, manufacturing, oil/gas, mass transit, and food/beverage production. SCADA uses a wide variety of networks, servers, and software to handle industrial processes, provide 24/7 monitoring, and supply data in real time (see Figure 13.83). Frequently a SCADA system automates tasks in an attempt to eliminate human error, increase productivity, reduce risks, and improve management by

providing real-time data and alerts. One concern about these types of systems is the security risk because of the complexity of hardware, software, protocols, and systems used.

FIGURE 13.83 SCADA example

A **legacy system** is an outdated computer system or piece of network equipment that in an ideal world would be replaced or updated with something new but that is kept because it might cost too much to replace it, it is used with a particular system that can't be replaced, or it provides a functionality that will not be needed much longer. A legacy system might contain ports that require converters to be attached to the newer equipment, require outdated access methods, or use proprietary cables that might not be easy to obtain or find. Legacy systems are challenging for technicians because of the lack of support and documentation, but they may still be part of the job requirements.

Software-Defined Networking

Traditional networking involves hardware and software to move information from one place to another. Software-defined networking (SDN) is like ramped-up virtualization. With SDN, network hardware can be virtualized and centrally controlled. Advantages of SDN include the following:

- Provides centralized management and control
- Makes applying security policies across the entire network easier
- Makes it possible to expand and contract the network by quickly and effortlessly adding or removing devices as needed
- Enables fine-tuning of the network for a specific application, time, or purpose

Two basic concepts associated with SDN are the control plane and data plane. The **control plane** is the part of SDN that is involved with getting the data ready to move, whether that means building a routing table for the routing function or a MAC address table for a switch. The **data plane** is where all the work is done to move or forward traffic from the source to the destination, such as sending the data out a specific router or switch port. By splitting up these areas, it is easy to virtualize network equipment.

Let's look at switches as an example. You may remember that switches build a MAC address table, which enables the network to efficiently send data based on the destination MAC address out a specific port. The process of learning the MAC addresses, storing them, and deciding which port to send the data to could be confined to the control plane area, and the transmission of data could be part of the data plane to allow for SDN switches to be used (see Figure 13.84).

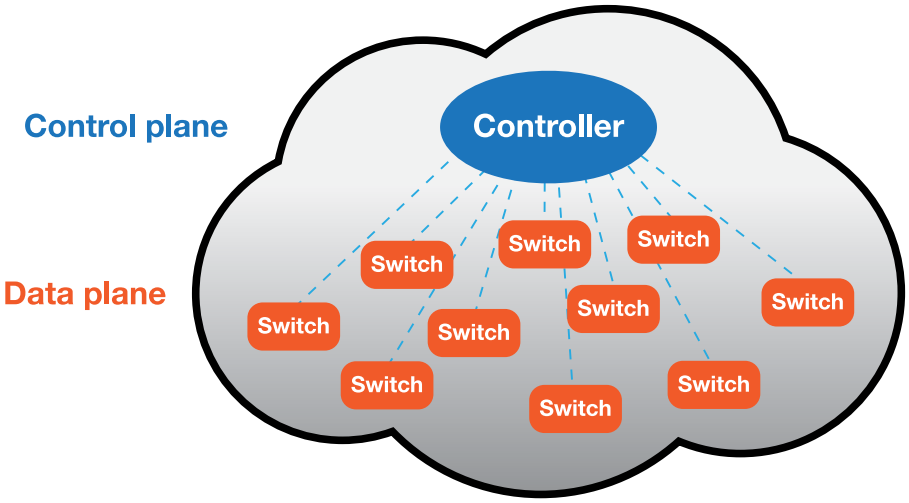


FIGURE 13.84 SDN network switching example

SDN started in the data center but has moved into other areas, including WANs and cloud connections, and it affects every part of network functionality today.

Network Terminology

In the networking field, you must be familiar with many acronyms and terms. Table 13.27 shows a few of the most common of them.

TABLE 13.27 Common network terms

Term	Description
Address Resolution Protocol (ARP)	A protocol used to discover MAC addresses. To send a message, a computer needs four key addresses: source IP, source MAC, destination IP, and destination MAC addresses. The computer sending the message knows its own source IP and MAC addresses. When the computer does not know the destination MAC address (but knows the destination IP address), ARP is used to discover that destination MAC address.
Bandwidth	The width of a communications channel, which defines its capacity for data. Examples include up to 56 kb/s for analog modems and up to 100 Gb/s for an Ethernet network.
Broadband	Cable bandwidth that is divided into multiple channels, on which simultaneous voice, video, and data can be sent.
Internet Control Message Protocol (ICMP)	A Layer 3 protocol used when troubleshooting or evaluating networks. The `ping`, `pathping`, and `tracert` commands use ICMP.
Network address translation/port address translation (NAT/PAT)	A method of conserving IP addresses. NAT uses private IP addresses that are translated to public IP addresses. PAT does the same thing, except it uses fewer public IP addresses by "overloading" one or more public IP addresses and tracking port numbers.
Secure Sockets Layer (SSL)	A protocol used to transmit internet messages securely. This protocol is used with HTTPS and online shopping websites to secure credit card information. Transport Layer Security (TLS) is the successor of SSL, which is now considered deprecated.

Term	Description
Transmission Control Protocol (**TCP**)	A connection-oriented protocol that ensures reliable communication between two devices. TCP and UDP are the two most common transport layer protocols. TCP is used when a connection needs to be made, and if the data is not received, the data is re-sent. Website connections and some file transfer protocols use TCP.
User Datagram Protocol (**UDP**)	A Layer 4 connectionless protocol that applications use to communicate with a remote device. TCP and UDP are the two most common transport layer protocols. UDP is used when a connection is not very important, when low overhead is needed (that is, when the UDP header is a lot smaller than a TCP header), or when speed is of the essence. VoIP and DHCP use UDP.

The TCP/IP Model in Action

To see the TCP/IP model in action, imagine opening a web browser with two separate windows: `https://www.pearsoned.com` and `https://www.google.com`. Two separate packages of data would be formed. For example, because HTTPS data is sent, HTTPS specifies how the data is to be formatted at the application layer. So, web page 1 gets HTTPS data at the application layer and moves down to the transport layer (inside the computer). At the transport layer, TCP is used for HTTPS traffic, and TCP adds a source port number 51116 and a destination port number 443 as part of building the transport layer header. All this HTTPS and TCP information moves down to the internet layer, where IP adds source and destination IP addresses. Because Pearson Education's web server has the IP address 23.197.24.193, that is the destination IP address. The packet continues moving down the model to the network access layer, and because the LAN is an Ethernet LAN, a source MAC address and destination MAC address are added. The data and all the headers are placed onto the Ethernet cable and sent on their way. The same thing happens with the second web page, except that at the transport layer, TCP adds port number 51117 and destination port number 443.

TECH TIP

Use `netstat` to view current connections

To see current connections and associated port numbers, bring up a command prompt and type `netstat`.

When the Pearson Education web server delivers the web page to the computer, the data is, of course, from the web server, but the TCP port numbers are reversed. The web server places port number 443 as the source port number and port number 51116 as the destination port number. The source and destination IP addresses and MAC addresses are reversed as well. When the original computer gets the message, it knows which browser window generated port number 51116, and it places the Pearson Education information from the web server into the correct browser window. The same is true when the Google request comes back from the Google web server.

TCP/IP-based protocols are required to send and receive data through the internet. Table 13.28 describes some of the most popular protocols and lists the TCP/IP port numbers that are commonly used for various protocols. Table 13.29 lists some of the common protocols or network standards and the TCP/IP model layers at which they operate.

TABLE 13.28 TCP/IP protocols and port numbers

Protocol	Common port number(s)	Description
Dynamic Host Configuration Protocol (DHCP)	67/68	Issues IP addressing information, such as IP address, subnet mask, default gateway, and DNS server address, to network devices.
Domain Name System (DNS)	53	Translates internet names and URLs into IP addresses.
File Transfer Protocol (**FTP**)	20/21	Sends/receives files from one computer to another network device; actually requires two port numbers: one to issue commands and the other one for data. Port 20 is sometimes but not always used for data. FTP sends data in cleartext and is not considered secure.
Hypertext Transfer Protocol (**HTTP**)	80	Provides browser-based internet communication. HTTP is not considered secure.
HTTP over SSL/TLS (Secure Sockets Layer/Transport Layer Security) Protocol (**HTTPS**)	443	Provides encrypted HTTP communication through an SSL/TLS session.
Internet Message Access Protocol (**IMAP**)	143	Supports email retrieval. Allows synchronization from multiple devices. The latest version is IMAP4.
Lightweight Directory Access Protocol (**LDAP**)	389	Provides records related to directory services (any type of network resource, such as users, printers, phone numbers, files, access points, and so on)
NetBIOS over TCP/IP (**NetBT**)	137–139	Supports outdated applications that rely on the NetBIOS API to use a TCP/IP-based network. Also known as NBT.
Network Time Protocol (NTP)	123	Synchronizes time between network devices.
Post Office Protocol version 3 (**POP3**)	110	Supports email retrieval and stores email on a single network device. (Contrast with IMAP.)
Remote Desktop Protocol (**RDP**)	3389	Connects a Windows computer to a remote Windows computer.
Secure File Transfer Protocol (SFTP)	22	Supports file transfer using the SSH protocol suite.
Secure Shell (**SSH**)	22	Supports secure connectivity to a remote device and allows secure file transfer.
Server Message Block (SMB)/Common Internet File System (CIFS)	445	Provides access to shared network devices, files, and printers, especially in a mixed environment, such as a network consisting of Mac and Windows computers. CIFS is a version of SMB. SMB/CIFS can use TCP port 445, but when used with the NetBIOS API, UDP ports 137 and 138 as well as TCP ports 137 and 139 are used. (See NetBT.)

Protocol	Common port number(s)	Description
Service Location Protocol (SLP)	427	Announces and discovers services in a LAN.
Simple Mail Transfer Protocol (**SMTP**)	25	Transmits email and is commonly used with MIME (Multipurpose Internet Mail Extensions) to include non-ASCII character sets and other rich media content within email.
Simple Network Management Protocol (**SNMP**)	161/162	Used to monitor, communicate with, and manage network devices.
Telnet	23	Supports connecting to a remote network device; is not secure.

TABLE 13.29 TCP/IP layers and associated protocols/standards

Layer	Protocols
Application	HTTP, HTTPS, Telnet, SSH, FTP, SFTP, DNS
Transport	TCP, UDP
Internet (Internetwork)	IP, DHCP, ICMP
Network access	ARP, 802.3 (Ethernet), 802.11a, 802.11b, 802.11g, 802.11n, 802.11ac, and 802.11ax (wireless)

Networking protocols can seem overwhelming at times, but remember that each one is just a set of rules for a specific purpose.

One more aspect of protocols that you need to understand is how TCP and UDP differ. What they have in common is that they both operate at the transport layer of the TCP/IP model, and they both work on port numbers. What is different is that TCP has a bigger header that contains features that let it do a lot more things, like make sure the destination connection is available and stay in constant contact with the destination during the data transfer. This is called being **connection-oriented**. Most of the TCP/IP protocols are connection-oriented, including HTTP, HTTPS, and SSH. Another feature of TCP is that if any data is lost along the way, it is re-sent.

In contrast, UDP is considered a **connectionless** protocol. I think of this as throwing a baseball (the data) and just hoping it gets to the destination. There are no "do overs," and data is not re-sent. UDP transfers are faster than TCP transfers. Some application layer protocols that use UDP are DHCP and TFTP. The voice data in VoIP calls is sent using UDP because VoIP cannot tolerate delay. DNS servers can actually use both TCP and UDP.

More Windows Network Settings

When you first configure a computer, you have to specify whether the computer is on a private network, such as your home or corporate network, or on a public network. This can be changed using the Windows *Network & Internet* Settings link. From the *Network Status* link (refer to Figure 13.73), use the *Properties* button for whatever type of network connection you are using to select whether the computer has a public or private network profile, as shown in Figure 13.85.

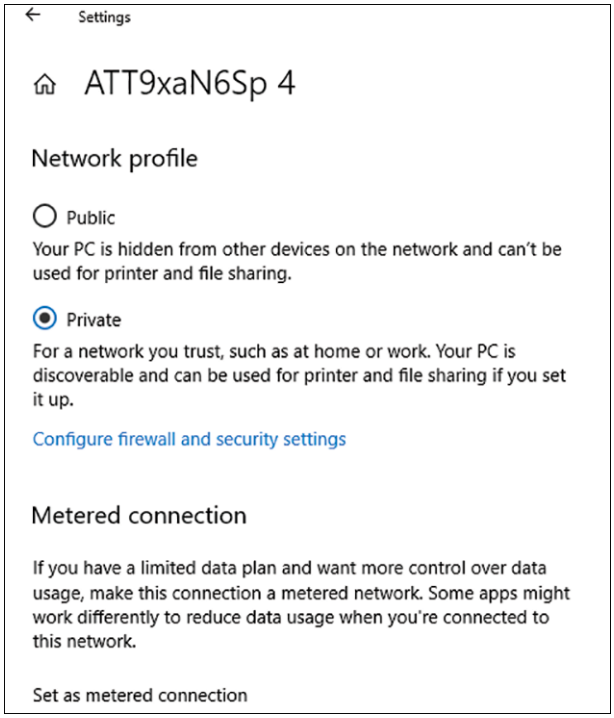


FIGURE 13.85 Windows public or private network profile

Notice the section for a metered connection at the bottom of Figure 13.85. A **metered connection** is an internet connection that has a data limit imposed by the internet provider. You may be familiar with this because of your cell phone and cellular plan. Wi-Fi and Ethernet network connections can also be configured to be metered (but normally are not by default).

Even though you can control many things from the notification area or from some of the Windows Settings options, many network configuration settings are still done through the *Network and Sharing Center* Control Panel. The *Network and Sharing Center* Control Panel has been used both in this chapter and in Chapter 12, "Internet Connectivity, Virtualization, and Cloud Technologies," but knowing the details and purposes of the options is important for IT personnel. Figure 13.86 shows the *Network and Sharing Center* window.

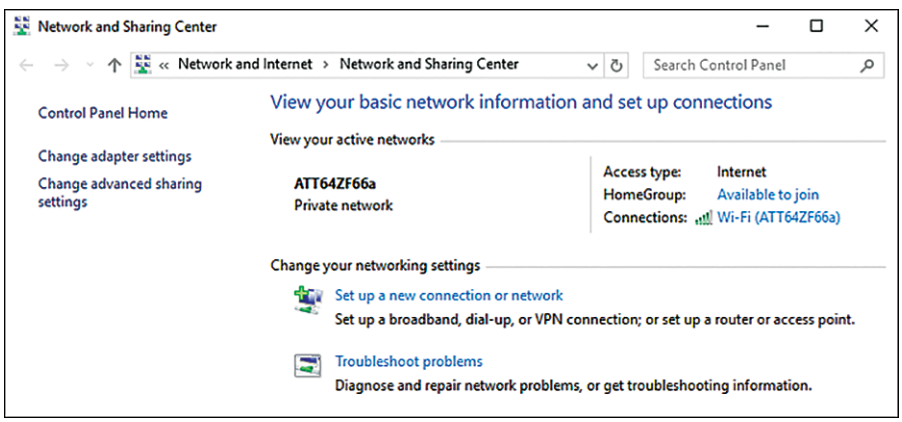


FIGURE 13.86 Windows Network and Sharing Center window

Notice in the main portion of the screen that you can see what network is currently being used. You can see whether the connection is wired or wireless and the name of the network. You can also tell in home or small business networks if the computer can share files with other devices (as discussed in the next section).

There are two important links in the left pane: *Change adapter settings* and *Change advanced sharing settings*. The *Change adapter settings* link enables you to access the network adapters that are installed, as shown in Figure 13.87. If a network adapter that is installed in the computer is not listed, use *Device Manager* to troubleshoot and ensure that the device is enabled through UEFI/system BIOS.

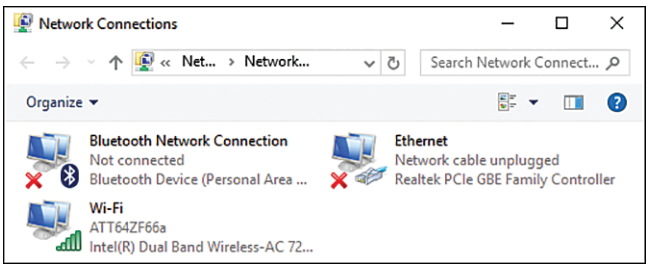


FIGURE 13.87 Windows Network Connections window

The *Network Connections* window is important when configuring an adapter. In it you can perform some of the following tasks:

- Double-click or tap the adapter icon to view device information. A wireless NIC shows wireless connectivity (see Figure 13.88), a wired NIC shows the wired network information (see Figure 13.89), and a Bluetooth adapter shows any Bluetooth pairs. At the bottom of each of the wired and wireless NIC windows, you can see the number of sent and received bytes.
- Click the *Details* button in the wireless or wired NIC windows (that is, the *Wi-Fi Status* window or *Ethernet Status* window) to see information similar to that provided by the `ipconfig /all` command (see Figure 13.90).

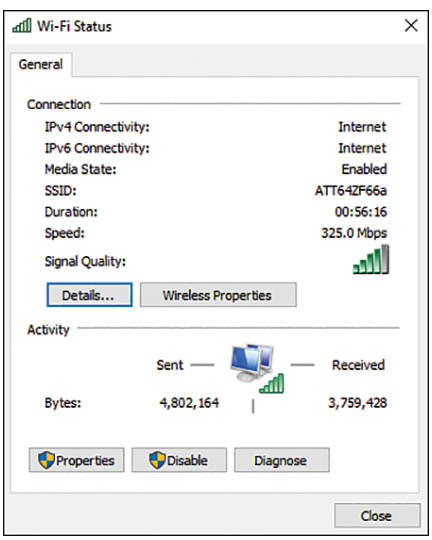


FIGURE 13.88 Wireless NIC window

- Click the *Wireless Properties* button in the wireless NIC window (that is, the *Wi-Fi Status* window) to view information about the specific type of wireless network. Use the *Security* tab to view the type of security applied.
- In both the wireless and wired NIC windows, click the *Properties* button to manually configure the NIC properties or modify a connection, such as the TCP/IPv4 or TCP/IPv6 parameters (see Figure 13.91).
- Double-click the *Internet Protocol Version 4 (TCP/IPv4)* (or *TCP/IPv6*) link to configure the adapter for DHCP or statically assign an IP address (refer to Figure 13.58).
- Click or tap the *Configure* button to set wired or wireless NIC-related settings, such as speed and duplex.

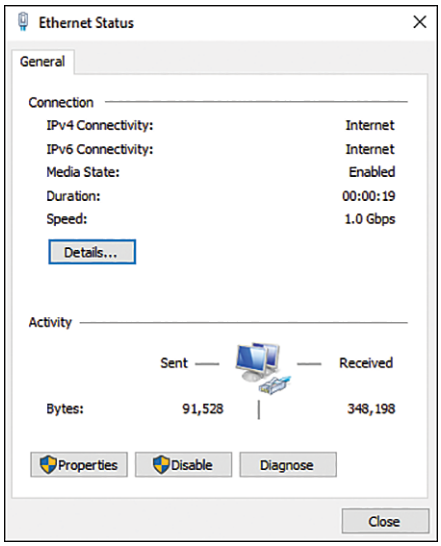


FIGURE 13.89 Wired NIC window

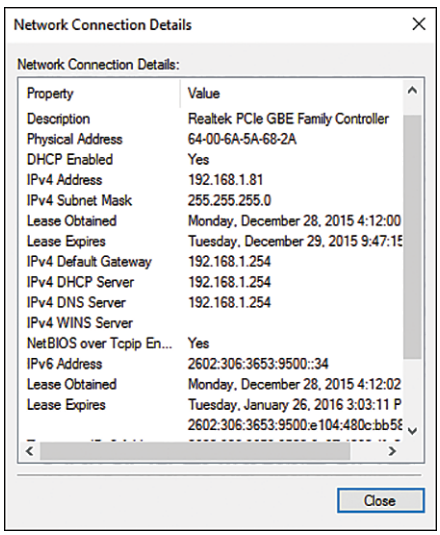


FIGURE 13.90 Wired or wireless NIC details

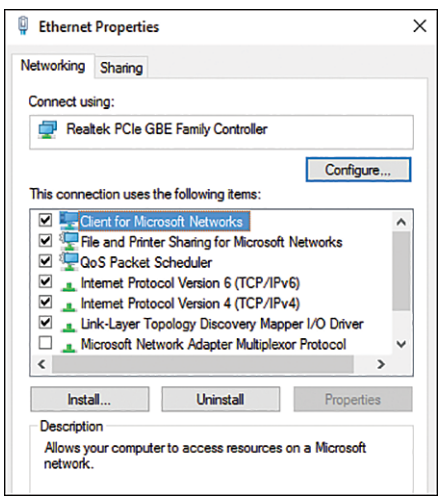


FIGURE 13.91 Wired or wireless networking properties window

> Manually configure the wireless NIC for a specific nonbroadcasting wireless network (refer to Figure 13.67).

> Set up a new Bluetooth connection. In Windows, access the *View Devices and Printers* Control Panel > *Add a device* link. Ensure that the Bluetooth device is turned on and visible in the *Add a device* window (see Figure 13.92). Select the device and click *Next*. Sometimes, a PIN or passcode must be verified in Windows and on the device.

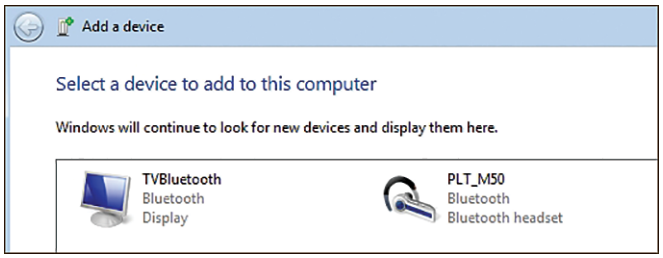


FIGURE 13.92 View Bluetooth devices in the Add a Device window

> From the *Network and Sharing Center* Control Panel, select *Change advanced sharing settings*. These settings relate to what the next section covers: sharing information across the networks you are now familiar with. Figure 13.93 shows the *Advanced sharing settings* window. Notice in the figure that there are three distinct and expandable sections: Private, Guest or Public, and All Networks. In the figure, the Private section has been expanded so you can see the available options.

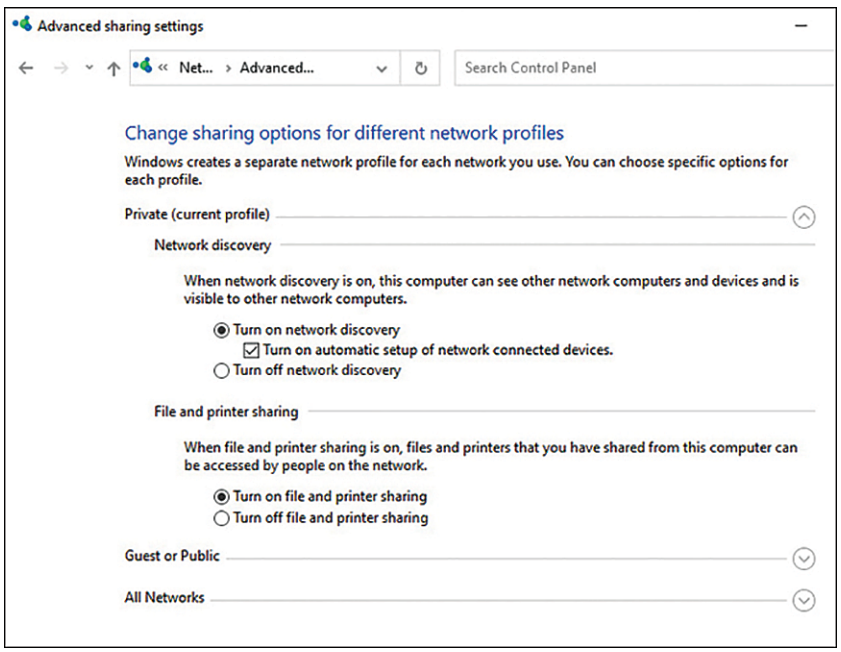


FIGURE 13.93 Advanced Sharing Settings window

Introduction to Shared Folders

When you double-click the *Network* option in File Explorer, you can view other network devices by their assigned names. You can also view network device names by typing `nbtstat -n` at a command prompt. Knowing a network device name is important when accessing a network share across the network. A **network share** is a folder or device that has been shared and is accessible from a remote network device.

Using the *Sharing* Tab > *Share* Button

You can set up any Windows computer as a file server and share files with other network devices. If you right-click on any folder and select *Properties* > *Sharing* tab, you can share documents within a folder two different ways. The most common way is with the *Share* button (see Figure 13.94).

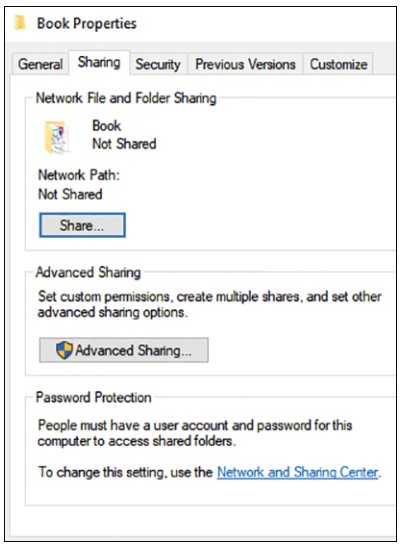


FIGURE 13.94 Sharing tab > Share button

Once you click on the *Share* button, you must choose the username to share the document with by selecting the down arrow, selecting a name or creating a new user, and selecting the *Add* button > *Share* button (se in Figure 13.95).

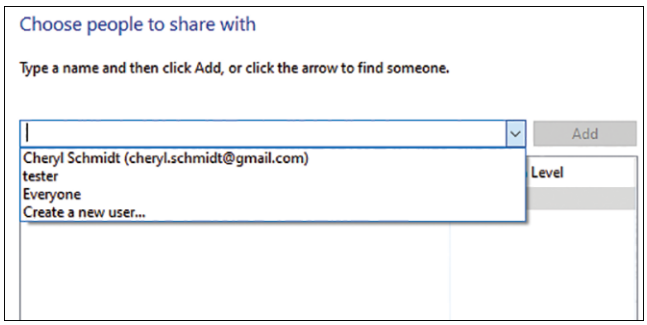


FIGURE 13.95 Adding the name of a user to share the folder with

Once you select the *Share* button, the network path appears in the properties window, as shown in Figure 13.96.

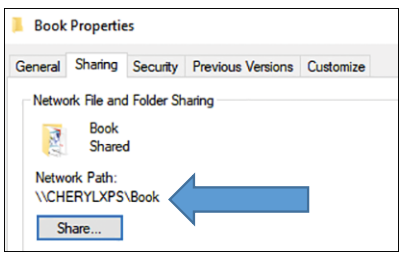


FIGURE 13.96 Network path

The network path is important to have and to give to others who want to access the share. The **network path** is similar to the driving route to a restaurant except that it is how to get to something

shared on the network from a remote device. The network path can be used from the command prompt or File Explorer to access the folder quickly. The network path can be the full path to get to the document or shown using the Universal Naming Convention (UNC). For example, say that a computer called CSchmidt has a network share called *TESTS*. By typing `\\CSchmidt\TESTS` at the command prompt, you can access the network share. Or you can type the IP address of the computer instead of the computer UNC. For example, if the CSchmidt computer had IP address 192.168.10.5, you could use `\\192.168.10.5\TESTS` from the command prompt instead. The problem with this method is that computer IP addresses are commonly provided by DHCP and could change. Next week, the CSchmidt computer could have the IP address 192.168.10.77, and the command would have to be adjusted. The *Advanced Sharing* button can also be used to create a network share (see Chapter 18).

Once someone or everyone no longer needs access to a shared resource, you can remove a share by right-clicking the shared file or folder > *Give access to* > *Remove access*. Another way is to select *Sharing* tab (refer to Figure 13.96) > *Remove access*. Be sure to click the *OK* and *Close* buttons to apply the change; do not use the *x* in the upper-right corner.

Mapping to a Share

In a network, it is common to map a drive letter to a frequently used network share. To map a drive letter to a network share in Windows 10/11, use File Explorer to locate and right-click *This PC* > *Map network drive* (note that in Windows 11, you might have to select *Show more options* to see) > select a drive letter in the *Drive* box > in the *Folder* textbox type the UNC for the network share or click the *Browse* button to select the network share. The *Reconnect at logon* checkbox allows you to connect to the mapped drive every time you log on. Figure 13.97 shows the windows to map drive letter `Z:` to the shared folder on the computer called CHERYL-PC. Expand the CHERYL-PC option to see the shared folders on this computer.

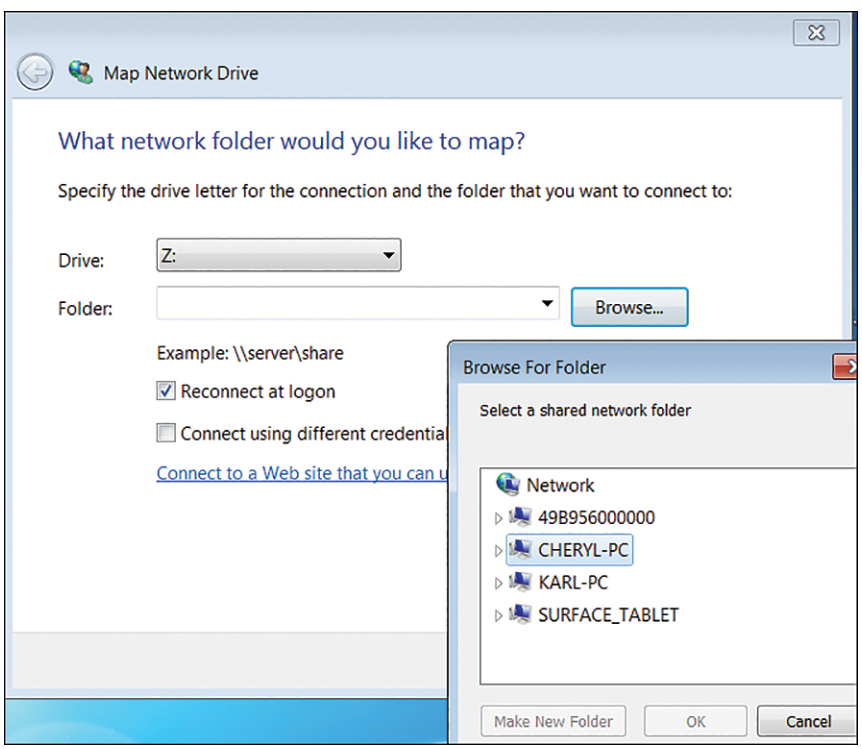


FIGURE 13.97 Windows Map Network Drive window

TECH TIP

Seeing a mapped drive path in File Explorer

Select *This PC* and expand *Network locations*. Double-click the mapped drive to see the network path.

TECH TIP

Mapping from a prompt

A drive can be mapped from a command prompt. Use the `net /?` command to get help. For example, say that a computer with the name *TECH01* has a share called *Cheryl*. The following command can be used to attach to it using the drive letter `M:`

```
net use m: /persistent:yes \\TECH01\Cheryl
```

Computer users commonly have frequently used network shares mapped to drive letters. It is faster to access a network share by drive letter than by searching around for the share through the File Explorer *Network* option.

SOFT SKILLS: BEING PROACTIVE

A good technician is **proactive**, which means the technician thinks of ways to improve a situation, anticipates problems, and fixes problems before being told to. A proactive technician follows up after a service call to ensure that a repair fixed the problem rather than waiting for another help desk ticket that states that the problem is unresolved. When something happens or a problem with a customer occurs, a proactive technician provides a list of recommended solutions or procedural changes to the supervisor rather than waiting for the supervisor to delineate what changes must occur.

For example, consider a technician at a college. The technician is responsible for any problems logged by computer users through the help desk. The technician is also responsible for maintaining the computer classrooms used by various departments. Each term, the technician reloads the computers with software updates and changes requested by the teachers. A proactive technician checks each machine and ensures that the computers boot properly and that the load is successful.

Another example involves checking new software. When the computers are reloaded each term, a faculty member is asked to check the load. A proactive technician has a list of "standard" software loaded on the computer, such as the operating system, service pack level, and any applications that are standard throughout the college. A separate list would include the changes that have been applied to the computer. Then the faculty member can simply look at the list and verify the load. Being proactive actually saves time for both the technician and the faculty member.

The opposite of proactive is *reactive*. A reactive technician responds to situations only when problems are reported. A reactive technician does not look for ways to avoid problems. For example, a proactive technician ensures that a computer is configured with automatic updates of virus scanning software. A reactive technician waits until a help desk ticket is created for a computer that exhibits unusual behavior (for example, it has a virus) even though the technician notices the unusual behavior when installing a second monitor.

As a student, practice being proactive. Start an assignment a day before you would normally start it. Talk to your teacher about your grade in advance (before the day preceding the final). Bring to school something to write with and paper. Finally, take this practice into your IT career: Be proactive as an IT professional and increase the level of service and professionalism in the field.

Chapter Summary

- Networks are created to share data and devices and connect to the internet. Types of networks include PANs, LANs, MANs, SANs, WANs, and WMNs.
- Networks can be wired or wireless.
- A workgroup network is composed of a small number of computers, whereas larger companies use a domain environment. A domain environment has a server that provides authentication to resources with a centralized user ID and password. A workgroup network manages the usernames on a computer-by-computer basis; this system grows less secure and more difficult to manage as the network grows.
- An Ethernet LAN, which is the most common type of LAN, is wired in a star or extended star topology. A switch is used to connect the devices. Each network connects to a router for communication with other networks. The router's IP address is the default gateway for all network devices on a particular LAN.
- Computers must have IP addresses to participate in a TCP/IP-based network (and gain access to the internet). IPv4 is the most common addressing used on computers today, but IPv6 addresses are slowly being assigned and used by corporate devices and internet providers.

- IP addresses are grouped by classes, with a particular subnet mask for each class. Each default mask can be changed to further subdivide a network for more efficient and manageable addressing. DHCP can provide addresses to network devices, or static addresses can be assigned. Public addresses are routable on the internet. Private addresses are used within homes and companies.
- TCP/IP is a suite that includes the following important protocols: FTP, Telnet, SMTP, DNS, DHCP, HTTP, HTTPS, POP3, IMAP, RDP, LDAP, SNMP, SSH, SFTP, SMB/CIFS, TCP, UDP, IP, and ICMP.
- The OSI model is a networking model that has seven layers: application, presentation, session, transport, network, data link, and physical. The TCP/IP model is a working model that contains four layers: application, transport, internet (or internetwork), and network access. The devices and protocols that work at Layer 3 (network layer or internet layer) include routers, IP, and ICMP. The devices and protocols that work at Layer 2 (data link layer or network access layer) include switches, access points, and ARP. Keep in mind that Ethernet has Layer 2 specifications, which is why a MAC address is a Layer 2 address. The devices that work at Layer 1 (physical layer or network access layer) are cables, connectors, hubs, and wireless antennas.
- 802.11 and Bluetooth are wireless network technologies. Bluetooth is used in PANs, and 802.11 is used in wireless LANs. 802.11 wireless NICs include 802.11a, 802.11b, 802.11g, 802.11n, 802.11ac, and 802.11ax. 802.11a, 802.11n, 802.11ac, and 802.11ax work in the 5 GHz range; 802.11b, 802.11g, 802.11n, and 802.11ax work in the 2.4 GHz range. 802.11ax also functions in the 6 GHz range using Wi-Fi 6E. 802.11 antennas are either directional or omnidirectional.
- The key tools for troubleshooting a networked computer are the `ipconfig`, `ping`, `pathping`, `nslookup`, and `tracert` commands and a cable tester.
- A technician should be proactive as opposed to reactive, preventing problems and situations whenever possible.

A+ CERTIFICATION EXAM TIPS

- ✓ This chapter provides information related to both the 220-1201 and 220-1202 exams. The information related to the 1202 exam includes the *Network and Sharing Center* Control Panel, Network & Internet settings, and network client configuration (including IP addressing scheme, DNS settings, subnet mask, gateway, static and dynamic addressing, wired network connection, wireless, wireless WWAN [cellular], network-related commands—`ipconfig`, `ifconfig`, `nslookup`, `tracert`, `netstat`, `net use`, `net user`, `pathping`, and `ping`—NIC properties, network shares, and drive mapping).
- ✓ Know the difference between a LAN, WAN, PAN, MAN, SAN, WLAN and WWAN.
- ✓ Know the purposes of these network devices: hubs, routers, access points, firewalls, patch panels, cable/DSL modems (see Chapter 12), repeaters, PoE devices (injectors and switches), and switches (both managed and unmanaged). Also be able to describe how software-defined networking (SDN) uses software to handle functions normally provided in hardware by dividing a network into the control and data planes.
- ✓ Know the purposes of key networking protocols, port numbers used by the protocols, and the differences between TCP and UDP.
- ✓ Know when to use a particular type of networking tool, whether it is a physical tool or a command. Physical tools include crimpers, cable strippers, Wi-Fi analyzers, toner probes, punchdown tools, cable testers, loopback plugs, and network taps.
- ✓ Know what a VLAN is and how it is configured on a switch.

- ✓ Know what to do when one or more computers cannot connect to the internet or when computers have an IP address conflict. Know how to tell whether the problem is an internet connection problem and what specific network resources the device can't reach, such as network shares, printers, or email.
- ✓ Know how to manually configure an IP address on a network device such as a computer, an AP, or a printer.
- ✓ Know the different types of wireless networks and their compatibility with each other.
- ✓ Be able to configure a wireless network and 2.4 GHz and 5 GHz channels so multiple wireless APs can coexist as well as other parameters, such as an administrator password and DHCP.
- ✓ Know the purpose of an IP address, a default gateway, and a subnet mask.
- ✓ Know the difference between an IPv4 address and an IPv6 address.
- ✓ Recognize when an address is a private IP address and understand the difference between a public IP address and a private IP address.
- ✓ Be familiar with DHCP terminology, including leases, reservations, and scope.
- ✓ Know the different types of network cabling and connectors.
- ✓ Recognize when a computer gets assigned an IP address by APIPA.
- ✓ Know the port numbers and purposes of the following protocols as well as the differences between TCP and UDP: 20/21 (FTP), 22 (SSH), 23 (Telnet), 25 (SMTP), 53 (DNS), 67/68 (DHCP), 80 (HTTP), 110 (POP3), 143 (IMAP), 443 (HTTPS), 3389 (RDP), 137–139 (NetBIOS/NetBT), 161–162 (SNMP), 389 (LDAP), and 445 (SMB/CIFS).
- ✓ Know the purposes of different servers, including web, fileshare, database, print, DHCP, DNS, mail, NTP, syslog, and authentication (AAA) servers.
- ✓ Review the section on troubleshooting network printer problems.
- ✓ If a wireless laptop cannot get on a wireless network, you might have to forget the network, reconnect, and provide credentials. You can also check to see if wireless has been disabled.
- ✓ Be able to recognize and troubleshoot problems with IP addressing information that comes from a DHCP server (including IP address, exclusions, default gateway, subnet mask, and DNS server address).
- ✓ Be able to troubleshoot wireless problems by, for example, moving a device to a different location and making sure a wireless NIC is turned on.
- ✓ Be able to use the `ipconfig` command and review the options available (by using `ipconfig /?`).
- ✓ Be able to use the Network Status link to view or configure public or private networks, IP addressing information, and the MAC address of a NIC.
- ✓ Review the different DNS message types: A, AAAA, MX, CANME, and TXT.
- ✓ Know what might cause an authentication failure.
- ✓ Be able to describe the services provided by IoT devices and legacy/embedded systems like SCADA systems.

Key Terms

2.4 GHz, 5 GHz, 6 GHz, 802.11a, 802.11ac (Wi-Fi 5), 802.11ad, 802.11ax (Wi-Fi 6), 802.11b, 802.11be (Wi-Fi 7), 802.11e, 802.11g, 802.11i, 802.11n, A record, AAA server, AAAA record, access point, AES, APIPA, authentication failure, Bluetooth, broadcast address, cable management system, cable stripper, cable tester, Cat 5e, Cat 6, Cat 6a, Cat 7, channel, CIDR, CIFS, client-side DNS, CNAME record, connection-oriented, connectionless, content filtering, control plane, crimper, crossover cable, data plane, database server, default gateway, DHCP, DHCP exclusion, DHCP lease time, DHCP scope, DHCP server, direct burial cable, directional antenna, DMZ, DNS, DNS server, domain, dynamic IP address, embedded system, Ethernet, Ethernet over Power, external interference, FC, fileshare server, firewall, firmware, frequency band, FTP, gateway, high latency, host address, HTTP, HTTPS, hub, `ifconfig`, IMAP, intermittent connectivity, intermittent wireless connectivity, IoT, IP address, IP addressing scheme, IP filtering, `ipconfig`, IPv4, IPv6, iSCSI, LAN, LDAP, legacy system, limited connectivity, link-local address, loopback plug, low RF signal, MAC address, mail server, MAN, managed switch, metered connection, MIMO, MU-MIMO, MX record, `net`, `net use`, `net user`, NetBT, `netstat`, network number, network path, network protocol, network share, network tap, no connectivity, no internet connectivity, `nslookup`, NTP server, omnidirectional antenna, OSI model, PAN, patch panel, `pathping`, physical address, `ping`, plenum-rated cable, PoE, PoE injector, PoE switch, POP3, port flapping, port forwarding, port mapping, print server, printer sharing, private IP address, private network, proactive, proxy server, public IP address, public network, punchdown block, punchdown tool, PVC, RDP, RJ11, RJ45, router, SAN, screened subnet, secure management access, site survey, slow network speed, SMB, SMTP, SNMP, SSH, SSID, SSID not found, static IP address, STP, straight-through cable, subnet mask, switch, syslog server, T568A, T568B, TCP, TCP/IP, Telnet, TKIP, tone generator, toner probe, `tracert`, twisted pair cable, TXT record, UDP, unavailable resources, unmanaged switch, UPnP, UTP, virtual NIC, VLAN, WAN, web server, WEP, Wi-Fi analyzer, wireless extender, wireless regulations, WLAN, WMN, workgroup, WPA, WPA2, WPA3, WWAN

Review Questions

1. Match the network type on the left with the scenario on the right. Note that even though an answer may be valid for more than one answer, only one answer will allow all answers to be used. No term is used twice.

____ MAN	**a.** Home network of four PCs
____ SAN	**b.** City of Schmidtville network
____ PAN	**c.** Hewlett-Packard corporate network
____ WAN	**d.** Bluetooth network of two devices
____ LAN	**e.** Data storage for a company

2. Match the following. Note that even though an answer may be valid for more than one answer, only one answer will allow all answers to be used. No term is used twice.

a. Cat 8	____ Common type of LAN cable
b. Cat 6a UTP	____ 1 Gb/s over UTP
c. 1000BaseT	____ Can only use STP
d. 1000BaseSX	____ 1 Gb/s over fiber

3. Which network device would be best to use to connect wired client devices and can send data directly to the destination device without sending the data as a broadcast to every connected device?

   [access point | hub | router | switch]

4. Match each TCP/IP model layer to the description. Note that a layer can be used more than once.

a. Application	____ HTTP	____ a straight-through cable	____ a NIC
b. Transport	____ a router	____ UDP	____ DNS
c. Internet	____ a switch	____ IP	____ TCP
d. Network access	____ ICMP	____ MAC address	____ a wireless antenna

5. Some computers (both wired and wireless) in a specific area of the building are having problems connecting to printers, servers, and the internet. What should the technician do?

   a. Use a tone generator.

   b. Check the access point.

   c. Check the router that connects to the internet.

   d. Check problem computers for a DNS server address.

6. Software-defined networking splits tasks into which two major areas?

   a. Data plane and control plane

   b. 2.4 GHz and 5 GHz

   c. UTP and STP

   d. Network and transport

7. Which network device works at Layer 1 and sends received data out all its ports (except the port that received the data)?

   [switch | antenna | router | hub]

8. What is the most common network protocol suite and the protocol suite required to communicate on the internet?

   [LTE | TCP/IP | Bluetooth | ISO]

9. Which type of address is 48 bits long and is hard-coded into a NIC?

   [IP | TCP | MAC | NAT]

10. Which type of address is called a Layer 3 address and needed to get to the internet?

[IP | TCP | MAC | NAT]

11. Which type of IP address uses 128 bits? [IPv4 | IPv32 | IPv6 | IPv64]

12. Draw a vertical line between the network number and the host number for each of the following IP addresses (assuming the default subnet mask):

130.5.15.177	130.5.| 15.177
192.168.13.15	192.168.13.| 15
10.12.17.18	10.| 12.17.18

13. What protocol could be used to issue an IP address and the IP address of the DNS server to network devices?

[DNS | DHCP | ICMP | ARP]

14. What protocol is used to convert URLs to IP addresses?

[HTTP | SSH | SSL | UDP | DNS]

15. Two access points connect and extend *the same* wireless network. List the SSIDs for each access point in the following chart.

Access point	SSID
Access Point 1	
Access Point 2	

16. Two access points (AP1 and AP2) operating in the 2.4 GHz range have overlapping coverage areas. List the two channel IDs to assign to each access point by filling in the following chart.

Access point	Channel ID
AP1	
AP2	

17. Which connectors are commonly used on network ports that connect to a SAN? (Choose two.)

[RJ11 | RG-59 | FC | SATA | iSCSI]

18. A user has shared a folder with her corporate team. What information will the user need to give co-workers to enable them to easily access the shared documents across the network?

[UNC | IP address of the computer that has the shared folder | MAC address of the computer with the shared folder | network path for the shared folder]

19. Match each technology to the appropriate definition. Note that not all of the definitions are used.

____ 802.11a	**a.** Operates in the 2.4 GHz range, with speeds up to 54 Mb/s
____ 802.11b	**b.** Operates in the 2.4 GHz range, with speeds up to 2 Mb/s
____ 802.11g	**c.** Operates in the 2.4 GHz range, with speeds up to 11 Mb/s
____ 802.11i	**d.** Security specification
____ 802.11n	**e.** Operates in the 5 GHz range, with speeds up to 54 Mb/s
____ 802.11ac	**f.** Specifies interoperability between access points
____ 802.11ax	**g.** Standard for quality of service
	h. Standard for wireless interference
	i. Backward compatible with 802.11a, b, and g
	j. Allows eight simultaneous data streams
	k. Allows access to 6 GHz range with Wi-Fi 6E

20. In Figure 13.98, what IP address is the default gateway for host 203.145.15.2?

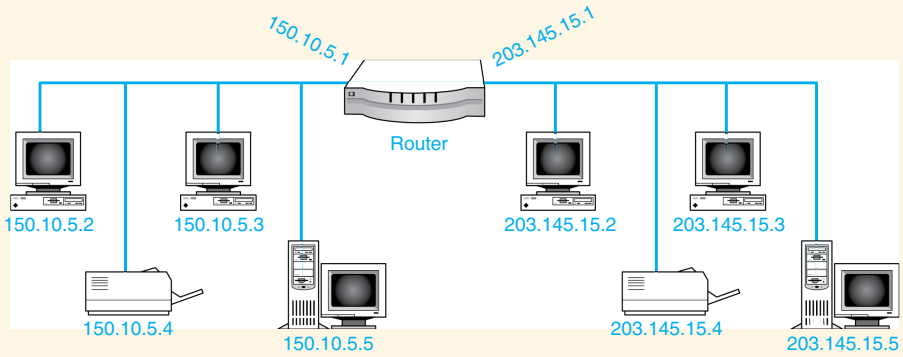


FIGURE 13.98 Review question network scenario

21. Which command determines whether another network device is reachable?

[`ping` | `ipconfig` | `ipconfig /all` | `arp -a`]

22. On which network device would VLANs be configured?

[hub | switch | router | firewall]

23. Which port numbers are used by a protocol whose purpose is to allow remote connectivity to a network device such as a server or router in order to make changes to the device? (Choose two.)

[21 | 22 | 23 | 53 | 69 | 80 | 443]

24. What command can be used to see a computer's MAC address?

[`netdom` | `net` | `netstat` | `ipconfig /all`]

25. A technician is setting up a new printer and notices that the computer is running unusually slowly. The technician decides to not only do the job that was logged (install the new printer) but also investigate the computer issue. Is the technician being reactive or proactive?

[proactive | reactive]

Exercises

Exercise 13.1 Understanding Wireless AP Paper Configuration

Objective: To determine what menu items would be used for specific functions

Procedure: Use the given menu options to determine which one would be used to perform a common configuration task on a wireless AP.

Note: Many times an IT professional must deal with a device or a particular model that is unfamiliar. Many wireless AP menus are similar, so practicing which menu option might be the one chosen is a good activity.

Wireless AP sample menu and submenu options:

a. Setup: Language, Date/Time

b. Wireless: Basic Wireless Settings, Wireless Security, Wireless MAC Filter, Advanced Wireless Settings

c. WAN/LAN: Internet Setup and Network Setup

d. Administration: Management, Access, Security, Factory Defaults, Firmware Upgrade

e. Status: Access Point, Wireless Network, About

Select which menu option would be used to do each of the following tasks:

____ **1.** Change the password used to access the AP menu.
____ **2.** Configure UPnP.
____ **3.** Configure to allow only 802.11n 2.4 GHz devices to attach (not 802.11b or 802.11g).
____ **4.** Check connectivity with another device.
____ **5.** Change the SSID.
____ **6.** Disable SSID broadcasting.
____ **7.** Configure the device as a DHCP server for wireless clients.
____ **8.** Set the year.
____ **9.** Reset the device.
____ **10.** Determine how many wireless hosts are currently attached to the AP.

Exercise 13.2 Understanding T568B Color Sequence

Objective: To articulate the proper colored order of a T568B straight-through cable

Procedure: Use the given graphic to denote which color of cable goes into the connector from left to right.

Use Figure 13.99 to designate which colors of vinyl insulator should go into making a T568B connector.

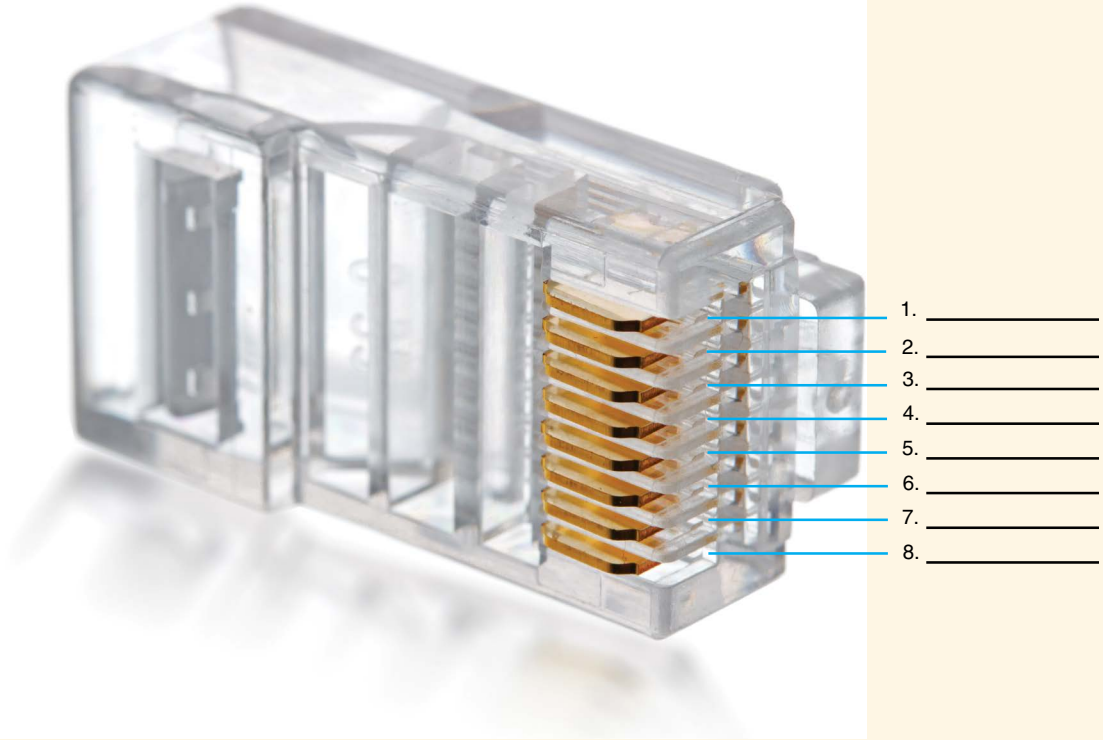


FIGURE 13.99 RJ45 connector/cabling exercise

Exercise 13.3 Recognizing Network Devices

Objective: To recognize a network device on sight

Procedure: Use Figure 13.100 to identify each network device.

Note: Possible answers could include the following.

Possible devices:

Cable modem	Termination plate	Switch
Hub	Patch panel	Repeater
Bridge	Wireless router	Firewall

Note that not all devices are used. No device is shown twice.

A

B

C

D

E

FIGURE 13.100 Network device identification

Exercise 13.4 Identifying Basic Wireless Network Parts

Objective: To identify basic parts of a wireless network and determine the type of wireless network used

Procedure: Using Figure 13.101, identify the major parts of a wireless network. For the number 5 blank, document whether this network would most likely be for a home network or a corporate network and explain why.

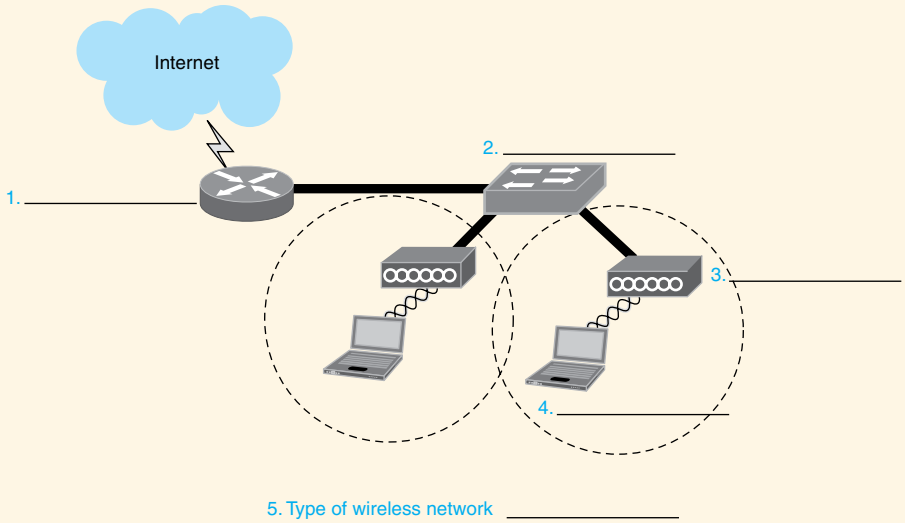


FIGURE 13.101 Wireless network components

1. _____
2. _____
3. _____
4. _____
5. _____

Exercise 13.5 Wireless Network Case Study

Objective: To design and price a wireless network based on the parameters given

Parts: Computer with internet access

Note: The instructor or lab assistant can speak on behalf of the faculty members if any design questions arise.

Scenario: A building has just been renovated to include corporate offices, as shown in Figure 13.102. The only wired network connections are the two stations in the reception area and the plotter in the left-most office area. All other connections are wireless.

FIGURE 13.102 Building floor plan for wireless design

Tasks:

1. Design a 2.4 GHz wireless network plan that will cover the reception area and all office stations to the right. Draw a circle over each coverage area and label each circle with a 2.4 GHz channel ID.
2. Design a 5 GHz wireless network plan that will cover the conference room and all the other office areas. Draw a circle over each coverage area and label each circle with a 5 GHz channel ID.
3. Provide a detailed list of wireless network parts, part numbers, and prices, as well as a web link where the prices were obtained. Be sure to include the antenna type, a printout of the wireless antenna radiation pattern, and antenna coverage range.
4. Provide the instructor with a typewritten list of policies and configuration settings for the wireless network you have designed. You are the designer and implementer, and what you decide goes.

Exercise 13.6 Practicing with Network Numbers and Broadcast Addresses

Objective: To determine the subnet numbers, broadcast addresses, and IP addresses that can be assigned to network devices

Procedure: Complete the following procedure and answer the accompanying questions.

1. Determine the network address for each of the following IP addresses, assuming that the default subnet mask is used.

   210.141.254.122 _____

   206.240.195.38 _____

   14.130.188.213 _____

   129.89.5.224 _____

   110.113.71.66 _____

2. Determine the broadcast address for each of the following IP addresses, assuming that the default subnet mask is used.

   166.215.207.182 _____

   198.94.140.121 _____

   97.57.210.192 _____

   133.98.227.36 _____

   14.89.203.133 _____

Exercise 13.7 Practicing with CIDR Notation

Objective: To determine the appropriate CIDR notation based on a given subnet mask

Procedure: Complete the following procedure and answer the accompanying questions.

For each subnet mask given in dotted decimal notation, determine the equivalent CIDR notation.

255.255.255.0 ___

255.255.255.224 ___

255.255.255.252 ___

255.255.254.0 ___

255.255.0.0 ___

255.255.255.128 ___

255.255.255.192 ___

255.0.0.0 ___

255.255.240.0 ___

255.255.255.240 ___

Exercise 13.8 Determining the Default Gateway

Objective: To determine the appropriate default gateway for a PC in a given situation.

Procedure: Complete the following procedure and answer the accompanying questions.

1. Determine the appropriate IP address, subnet mask (in dotted decimal notation, *x.x.x.x*), and default gateway for PC 1 shown in Figure 13.103.

   IP address: _____

   Subnet mask: _____

   Default gateway: _____

2. Determine the appropriate IP address, subnet mask (in dotted decimal notation, *x.x.x.x*), and default gateway for PC 2 shown in Figure 13.103.

   IP address: _____

   Subnet mask: _____

   Default gateway: _____

3. Determine the appropriate IP address, subnet mask (in dotted decimal notation, *x.x.x.x*), and default gateway for PC 3 shown in Figure 13.103.

   IP address: _____

   Subnet mask: _____

   Default gateway: _____

4. Determine the appropriate IP address, subnet mask (in dotted decimal notation, *x.x.x.x*), and default gateway for PC 4 shown in Figure 13.103.

   IP address: _____

   Subnet mask: _____

   Default gateway: _____

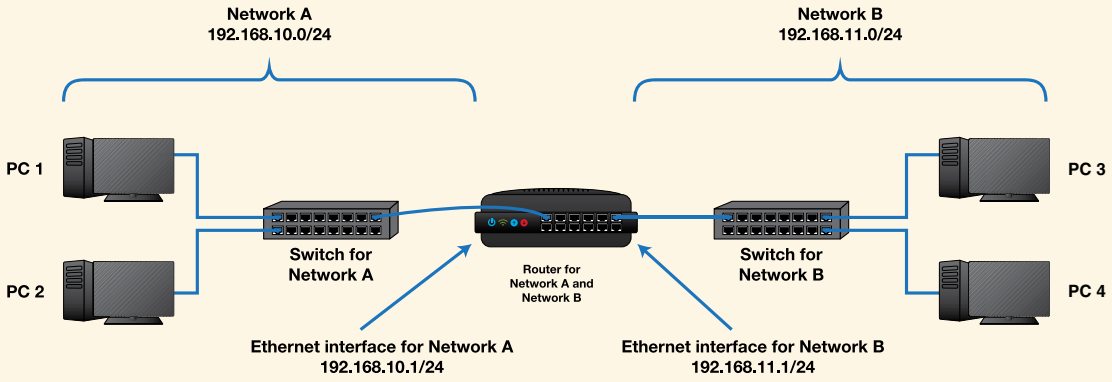


FIGURE 13.103 Network Topology 1

5. Determine the appropriate IP address, subnet mask (in dotted decimal notation, *x.x.x.x*), and default gateway for PC 1 shown in Figure 13.104.

   IP address: _____

   Subnet mask: _____

   Default gateway: _____

6. Determine the appropriate IP address, subnet mask (in dotted decimal notation, *x.x.x.x*), and default gateway for PC 2 shown in Figure 13.104.

   IP address: _____

   Subnet mask: _____

   Default gateway: _____

7. Determine the appropriate IP address, subnet mask (in dotted decimal notation, *x.x.x.x*), and default gateway for the printer shown in Figure 13.104.

   IP address: _____

   Subnet mask: _____

   Default gateway: _____

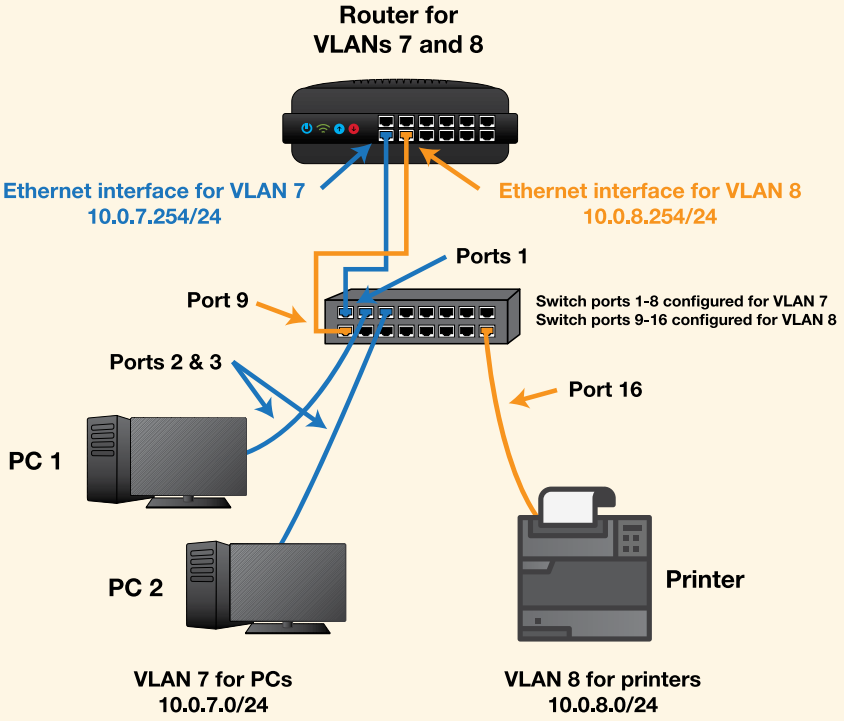


FIGURE 13.104 Network Topology 2

Activities

Internet Discovery

Objective: To obtain specific information regarding a computer or its associated parts on the internet

Parts: Computer with internet access

Procedure: Complete the following procedure and answer the accompanying questions.

1. On an HP ProBook 650 Windows 10 laptop, you cannot get the wireless NIC to attach to the wireless network. What are some steps you can take, as recommended by HP, to help in this situation?

   Write at least three solutions as well as the URL where you found each solution.

   _____

   _____

   _____

   _____

   _____

   _____

2. A Windows 11 laptop is showing limited connectivity on its Wi-Fi status. List three things to recommend to the user as well as the URL(s) where you found this information.

_____

_____

_____

_____

3. Locate a website that describes how to reserve an IP address on a Netgear router. Write the one router model the answer applies to, the menu option used to configure it, and the URL where you found this information.

_____

_____

_____

_____

4. Find a website that allows you to check your internet speed. Document your current speed, any other information provided as part of the test, and the URL where you found the information.

_____

_____

5. Find a website that explains the differences between Cat 5e and Cat 6a UTP cable. Write which standard you would recommend to the CIO and why. List the URL where you found this information.

_____

_____

_____

_____

Flip the CLASSROOM

Soft Skills

Objective: To enhance and fine-tune a technician's ability to listen, communicate in both written and oral forms, and support people who use computers in a professional manner

Activities:

1. Using the internet, find and access a utility that tests your soft skills. Compare your scores with those of others in the class and determine how you might improve in specific weak areas.

_____

_____

2. In groups of two, one person inserts a network problem in a computer while the other person is out of the room. When the other person comes back, they troubleshoot the problem by asking questions of the user (as if they were on the phone helping them). The person performing the troubleshooting cannot touch the computer. Discuss strategies for improving this troubleshooting process better before swapping roles.

_____

3. In groups of two or three, brainstorm three examples of a technician being reactive rather than proactive. List ways the technician could be more proactive for each example. Share your findings with other teams.

_____

Critical Thinking Skills

Objective: To analyze and evaluate information as well as apply learned information to new or different situations

Activities:

1. A home user connects to the internet. The ISP provides hard drive space for the user's web page. Is this a network? Why or why not? Write your answer in a well-written paragraph using good grammar, capitalization, and punctuation.

   _____

   _____

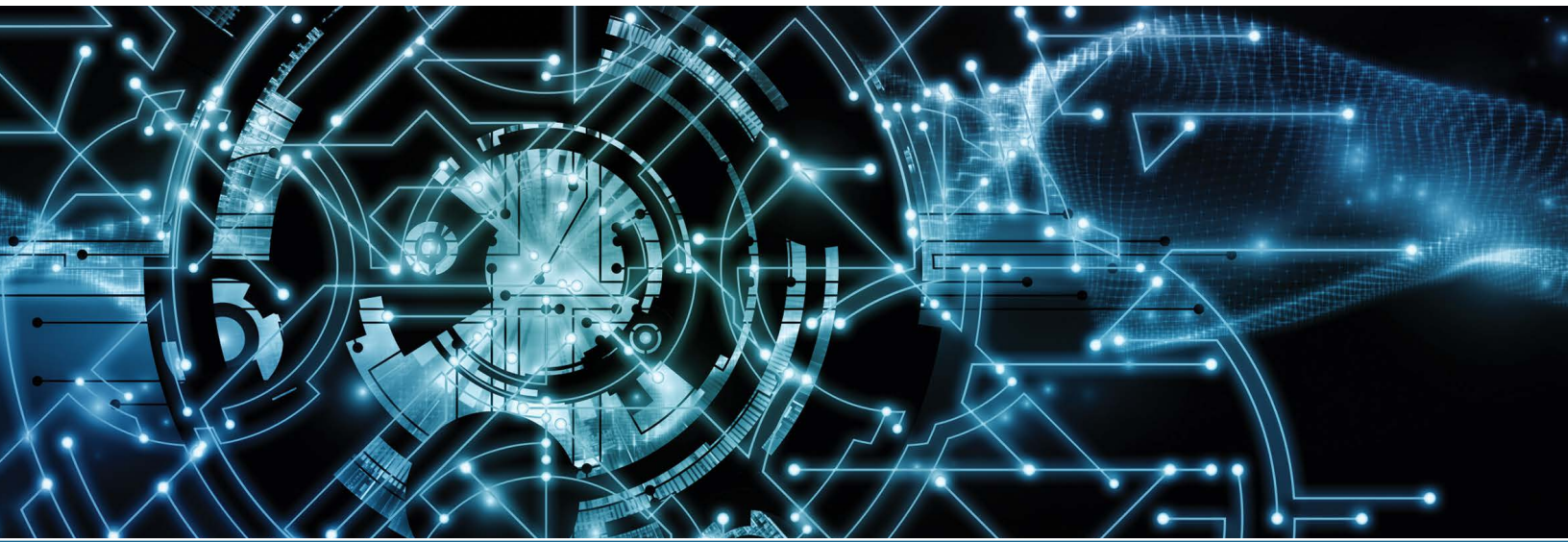
2. Use the internet, magazines, newspapers, or books to find a network installation case study. Make a table of terms the case study uses that were introduced in this chapter. On the left side, list the term, and on the right side, define or describe how the term relates to the network installation. Analyze the installation and discuss with a team. Make a checklist of approved processes and of recommended changes to implemented processes. Share your team findings with the class.

   _____

3. In a team environment, design a wired and wireless network for a small business that has 10 computers. Name the business, provide a design and implementation plan, and provide a list of items for which you should do more research. Share your plan with the class.

   _____

14 Introduction to Operating Systems



In this chapter you will learn:

- To identify the basic features and functions of an operating system
- To explain common types of operating systems and their purposes: desktop, workstation, and mobile device operating systems
- To apply application installation and configuration concepts
- To identify concerns related to identifying end-of-life, compatibility, and updating operating system
- To identify specific corporate needs
- To identify basic features of Microsoft Windows editions
- To identify and use common desktop icons in Windows 11
- To manage files and folders in Windows
- To use the appropriate Microsoft Windows 11 Settings utility
- To work with the Windows registry
- To create backups and to create a system image
- To apply techniques to stay current in the field

CompTIA Exam Objectives:

- ✓ 1202-1.1 Explain common operating system (OS) types and their purposes.
- ✓ 1202-1.3 Compare and contrast basic features of Microsoft Windows editions.
- ✓ 1202-1.4 Given a scenario, use Microsoft Windows operating system features and tools.
- ✓ 1202-1.6 Given a scenario, configure Microsoft Windows settings.

Operating Systems Overview

The operating system (OS) is the most important piece of software on a computer because without it, no application can run, and the hardware cannot work. While today's operating systems provide many services, the basic service of an **operating system** is to provide the interface between the user and the various components of the computer (the physical hardware and the digital applications).

You might be wondering what kind of things the operating system can do. An operating system does many tasks, but some that really affect you as a student are recognizing what you type on the keyboard (or do using a mouse or a touchpad) and bringing that information into the computer as input. The operating system controls output to the display, keeps track of files and folders, manages and keeps track of open applications, and controls peripherals such as printers. Figure 14.1 shows that the operating system is the coordinator of all hardware and software. The operating system is the software that any computer device needs to function.

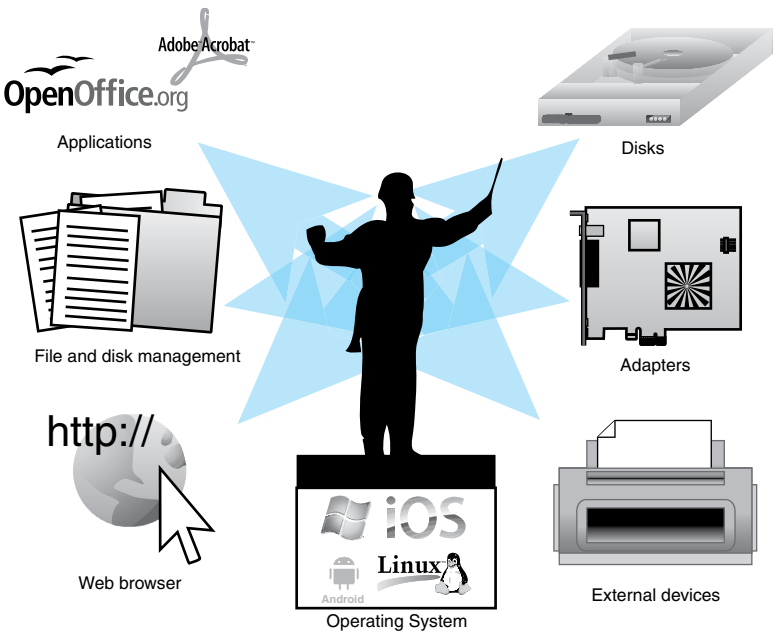


FIGURE 14.1 The operating system coordinates everything on a computer

The **boot process** is the steps a computer device (desktop, laptop, cell phone, tablet, etc.) goes through when it is first turned on. The central processing unit (CPU) initializes itself. It looks to the system's basic input/output system (BIOS or UEFI BIOS) for its first instruction. The BIOS runs the power-on self-test (POST), which makes sure the hardware is functioning properly. When this is complete, the BIOS looks for an operating system to load.

At this point, the operating system takes control of the boot process. The operating system loads the necessary device drivers to control devices such as a printer, CD/DVD drive, mouse, and keyboard. Once drivers are loaded, the user can access the system's applications and begin to work.

Virtually everything today's users do with their computers is done through an application, and every application must run through the operating system. The list of applications is endless, and new applications are being developed daily. The operating system allows a computer to communicate with almost anything—from the baby monitor installed by new parents, to the tablet a hospital nurse uses to enter patient information, to the security system that protects a home, to another computer a microbiologist is using to analyze data.

Each application must be written to communicate with a specific operating system because each operating system has its own specific code and syntax. Therefore, the choice of operating system largely determines the applications a computer can run. Many applications today are developed for multiple operating systems, and this requires that multiple versions of the application be created.

TECH TIP

Buy an application for a particular operating system

When buying or installing an application, you must be careful to get the version created for your operating system.

User Interaction with Operating Systems

When you click on something or type something in a search box, you are interacting with the operating system. The operating system therefore has to be programmed to respond based on what you do. At the most basic level, an operating system responds to a set of commands. The commands are accepted and processed by the operating system's command processor. Today's operating systems allow most commands to be entered by clicking on something through the graphical user interface (**GUI**) or by entering a command through the command-line interface. The **command-line interface** is not graphical and is only used to enter or view commands. For example, you can use the command-line interface to rename a file as shown on the left side of Figure 14.2, or you can use the GUI, as shown on the right side of the figure.

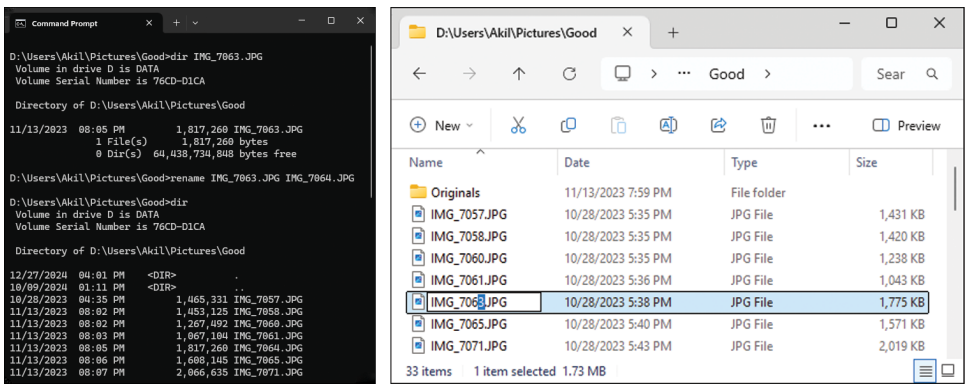


FIGURE 14.2 Command-line interface (left) and GUI (right)

The operating system is also responsible for handling file and disk management. Figure 14.3 shows File Explorer on a Windows 11 computer.

A **file** is an electronic container that holds computer code or data. Another way of looking at a file is to think of it as either a box of bits or an electronic piece of paper with information on it. A **folder** holds files and can also contain other folders. In Figure 14.3, *Potential Graphics* is a folder. With File Explorer, you can create, copy, or move files and folders.

The command prompt environment, also called the command-line interface, is an alternative environment that a technician can use to resolve a problem. From a command prompt, you can enter commands that are specific to the operating system. For example, say that you type the word `hop` at the command prompt. The word "hop" is not a command that the computer has been programmed to understand, so an error message appears because the computer does not know what to do. However, if you type `dir` at a command prompt, the computer recognizes the command and displays a *directory*, which is a listing of files.

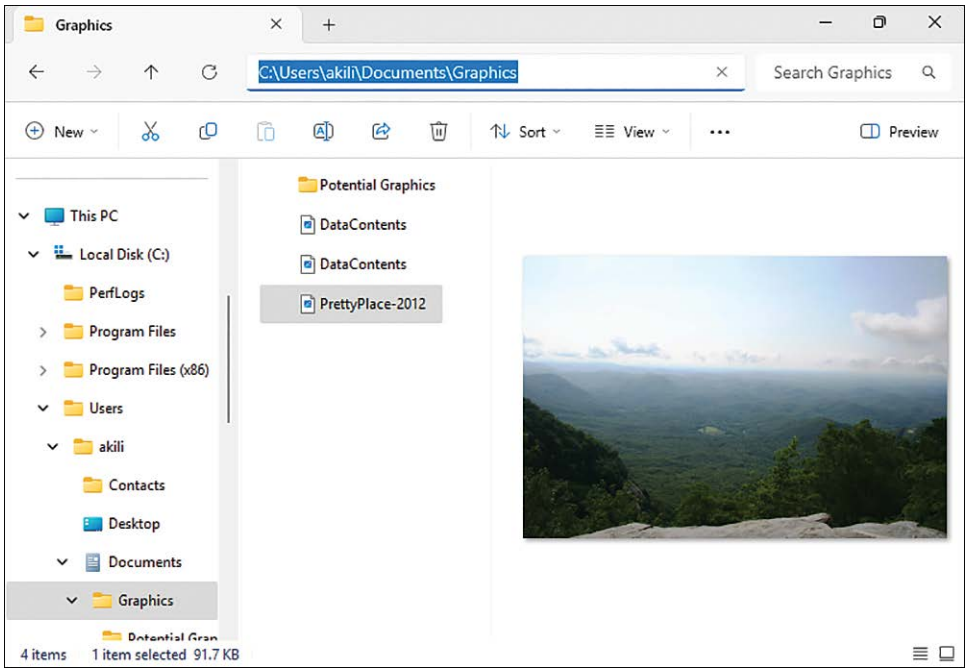


FIGURE 14.3 Windows 11 File Explorer

To access the command prompt from within Windows, you can right-click *Start* > select *Command Prompt* or *Command Prompt (Admin)*, but keep in mind that there are several ways of accomplishing almost anything in the Windows environment.

Chapter 15, "Introduction to Scripting," covers using the command prompt in greater depth.

Technicians must be familiar with the GUI environment and must also be able to function from a command prompt because sometimes the only way to execute a fix is by typing a command at a command prompt. Not only must technicians be familiar with the tools and environments of Microsoft operating systems, they must know multiple operating systems. This makes for a challenging and ever-changing career.

Overview of Popular Operating Systems

Some of the most common operating systems today are Microsoft's Windows, Apple's macOS, Linux, Chrome OS, Android, and Apple's iOS and iPadOS. The last three are specifically used for mobile devices, such as cell phones and tablets.

As of late 2024, it was estimated that about 73% of all personal computers use some version of Windows, and the remainder primarily use Linux or macOS. These numbers reflect worldwide usage.

The **Microsoft Windows** operating system dominates the personal computer world and remains the most popular operating system for home and office computers. Microsoft Windows was announced by Bill Gates in November 1983. Since then, there have been numerous versions and updates.

macOS is only intended to be run on computers manufactured by the Apple corporation. DOS 3.1 was used as the first operating system for Apple computers in 1978. The **Apple Macintosh OS** was introduced in 1997 as Mac OS 8. At the time of writing, the latest version is macOS 15.2, also known as macOS Sequoia. **macOS** is an example of a proprietary operating system. **Proprietary systems** generally are designed and sold by one company (the proprietor). No other companies or individuals are expected to contribute to the code or to alter the code, except under a business agreement with the proprietor.

In 1991 a Finnish student, Linus Torvalds, began work on a personal project: to build a new free operating system kernel known as Linux. The kernel is the core of a computer's operating system. People from all over the world continue to collaborate on the Linux **open source** code to submit tweaks to the central kernel. Open source systems are generally available for free; thus, they may or may not come with support. Open source systems such as Linux and Android (which is based on Linux) can be modified without permission from the creator.

The Windows operating system can be used on a wide variety of computers manufactured by many different companies. Apple computers, on the other hand, are the only computers that can use macOS. **Linux** has maintained its original goal of being a free and open source operating system.

When you purchase an operating system license, there are several types available: (1) an open and free license, such as when you download and install Linux, (2) a personal license, such as when you buy the rights to use the operating system on one computer (for example, a home computer or a small business computer), (3) a corporate license, where you get a discount for a specific number of Microsoft Windows installations, for example, and (4) an enterprise license, which might include more security, cloud, and virtualization options.

32-Bit vs. 64-Bit Operating Systems

Operating systems can use either a **32-bit architecture** or **64-bit architecture**. The number of bits is determined by the processor. Some versions of Windows and macOS are available in both 32-bit and 64-bit options. The main difference between the two is the type of processors that can be supported. A 64-bit operating system supports 64-bit processors. A 64-bit processor features multiple cores, and the more cores, the more processing power a CPU has. This makes a 64-bit operating system better suited to handling tasks such as video editing and image rendering.

It is also significant to note that a 32-bit operating system can run only programs and use only drivers that are written specifically for a 32-bit operating system's instruction set. However, a 64-bit operating system supports software written for 64-bit architecture and also allows the computer to run 32-bit applications. Table 14.1 lists the differences between 32-bit and 64-bit Windows.

TABLE 14.1 32-Bit and 64-Bit Windows

32-Bit Windows	64-Bit Windows
32-bit or 64-bit processor	64-bit processor
4 GB **RAM limitation** (that is, the operating system can view no more than 4 GB even if more RAM is installed)	Up to 2,048 GB RAM supported, depending on the version of Windows used
32 bits processed at a time	64 bits processed at a time
32-bit drivers required	64-bit device drivers required, and they must be digitally signed
32-bit applications and some support for older 16-bit applications	32- or 64-bit application support; 16-bit application support using the compatibility troubleshooter
Use of DEP (Data Execution Prevention), which prevents a specific type of security attack by using both hardware and software technology	"Always-on" DEP support for 64-bit processes
N/A	Protection for the operating system kernel (the core of the operating system)
N/A	Better support for multiple processors

Windows 11 Versions

The Microsoft Windows operating system was introduced in 1985. Since then, there have been several versions of Windows, including Windows 3.1, Windows 95, Windows 2000, and Windows XP. The most recent families of the Windows operating system are **Windows 10** and **Windows 11**. Windows 10 is a mixture of its predecessors Windows 7 and Windows 8. Both Windows 10 and its successor Windows 11 were designed from the beginning to be used across all platforms: desktops, laptops, and mobile devices. Windows 11 includes several new features, such as a redesigned graphical interface, a centered taskbar, and compatibility with Android applications.

Both Windows 10 and Windows 11 update device drivers automatically through Windows Update. Table 14.2 shows the various versions of Windows 10 and Windows 11 that can be purchased and briefly describes each one. Each version of Windows 10 can be 32- or 64-bit, except where noted. Windows 11 is only available for 64-bit systems. At the time of writing, support for Windows 10 was due to end on October 14, 2025.

TABLE 14.2 Windows 10/11 editions

Windows edition	Description
Home	Home is designed for home use on PCs and tablets; it comes with Microsoft Edge, Pen & Touch, and Cortana. It also features mobile and voice capabilities and a battery save mode. Some security features include device encryption, internet protection, and Windows Defender antivirus. BitLocker and Windows Information Protection are not available in Home. Home supports peer-to-peer networks but not domain networks. It does not support Remote Desktop. By default, Group Policy Editor (`gpedit.msc`) is not available, but it can be installed to facilitate the configuration of local software, network, and security settings.
Pro and Pro Education	Pro and Pro Education are designed for computers in the workplace. They include all features of Home, as well as features to support business networks. Local software, network, and security settings can be configured via Group Policy Editor (`gpedit.msc`), which is available by default. These editions include BitLocker and Windows Information Protection, which provide additional protection. Domain connectivity simplifies user and device administration. Remote Desktop facilitates configuration and troubleshooting. The Pro Education version provides additional management controls that are needed in schools.
Pro for Workstations	This edition is designed for people with advanced workloads or data needs, such as data scientists, CAD professionals, researchers, media production teams, graphic designers, and animators. Features include faster network file transfers, automatic repair of corrupted data, and persistent memory. This edition supports up to 4 CPUs and 6 terabytes (TB) of RAM.
Enterprise	Enterprise offers the same features as Pro, as well as additional security and management tools. Features include advanced credential protection and threat detection and response. This edition is not sold through retail centers but to corporate and educational institutions using bulk licensing.
N versions	The N versions of Windows are special editions created for European markets that lack certain media-related features (including Windows Media Player) to comply with EU antitrust rulings. Users can install a Media Feature Pack to restore most of the missing functionality, if needed.

The following links provide a detailed comparison of Windows 10 Pro and Windows 11 Pro and a comparison of Windows 11 Home, Pro, and Pro for Workstations:

> https://www.microsoft.com/en-us/windowsforbusiness/compare
> https://www.microsoft.com/en-us/windows/business/compare-windows-11

Workstation Operating Systems

A workstation is a computer used by one or more users. It normally includes one or more high-resolution displays and a fast processor that is designed to handle complex manipulation of data, such as data analysis, video editing, animations, or mathematical plots. Sometimes, however, the term is applied to any individual computer location that is hooked up to a mainframe.

Microsoft has a Windows 11 Pro for Workstations operating system, which is a higher-end version of Windows 11 Professional. It includes features that were already available on Windows Server and were brought over to a desktop version of Windows. macOS and Linux are also operating systems used on workstations.

Operating Systems for Mobile Devices

A mobile operating system is an operating system for phones, tablets, smartwatches, and other mobile devices. Mobile operating systems tend to require less memory and combine features of a personal computer operating system with features needed on mobile devices, such as a touch screen, Bluetooth, GPS navigation, speech recognition, and more. Some specialized mobile devices need specialized operating systems. For example, drones use Robot Operating System (ROS).

Android OS, developed by Google, Inc., is based on the Linux kernel. Worldwide, Android dominates the field; in the third quarter of 2024, about 70% of the 7.21 billion phones sold worldwide used Android OS. Android's early releases (before 2.0) were used exclusively on mobile phones. Android version 4.0 was the first version to be used by both smartphones and tablets.

Chrome OS is an operating system designed by Google that is also based on the Linux kernel. It was conceived as an operating system that would allow both applications and user data to reside in the cloud, and it uses the Chrome browser as its principal user interface. It is available only on hardware from Google manufacturing partners. Even though primarily used on laptops and tablets, Chrome OS can be used on desktops. Chromebooks (and other Chrome OS devices) are generally less expensive, lighter, and easier to transport than traditional laptops. In addition, they usually offer long battery life. Furthermore, viruses and malware pose less risk to Linux-based devices than to Windows devices.

The **iOS** mobile operating system was created and developed by Apple, Inc. to run only on Apple devices such as the iPhone and iPad. It is the second-most-popular mobile operating system worldwide. Although it's gaining in popularity worldwide, iOS is still a distant second after Android, with about 28.6% of the market (at the time of press).

As stated earlier, iOS was initially used on both iPhone and iPad devices. Over time, the version of iOS for the iPad required significant differences due to the iPad's larger screen, faster processor, increased memory, and optional devices such as keyboards. In 2019, Apple rebranded the variant of iOS for the iPad as iPadOS. **iPadOS** offers features such as improvements in the home screen, multitasking, and the Safari web browser. It also allows for use of external storage, a mouse, or a trackpad. In addition, with iPadOS, an iPad can be used as a second monitor for a macOS computer via a feature called Sidecar.

End-of-Life (EOL) Concerns

End-of-life (EOL) software is software that its vendor no longer supports or software that has reached the end of its usefulness. There can be serious consequences associated with using software that has reached its end of life. To avoid these issues, most IT departments replace their workstations, servers, and cell phones regularly in a replacement cycle. They also upgrade their software applications and their operating systems after thorough testing and careful planning. In some cases, they may be forced to move on when software companies stop issuing updates or when a warranty ends.

Some of the issues associated with using software past its end of life are listed here:

- **Security threats:** When an operating system's vendor stops issuing updates to address new forms of cyber attacks, the operating system becomes far more vulnerable to **security threats**. Also, older operating systems cannot take advantage of security enhancements such as Trusted Platform Module (TPM) or artificial intelligence (AI).
- **Software incompatibility:** Software vendors often cannot guarantee that new applications will be compatible with older operating systems, so **software incompatibility** is an issue.
- **Compliance issues:** Regulated industries, such as healthcare and financial technology, deal with sensitive data. It is dangerous to entrust critical information to an outdated and possibly insecure system.
- **Operating costs:** It costs a lot to maintain and fix bugs in unsupported software. For example, the expense of paying a company to patch an operating system that has reached its end of life can exceed the price of updating to a new system.
- **Performance and reliability:** As it ages, software can become slow or may fail to always perform as expected. Also, old software is normally installed on old hardware, which is prone to breaking down.

Update Limitations

The process of updating an operating system may cause problems. Some potential problems are listed here, along with possible solutions or ways to avoid the problems:

- **Insufficient hardware:** Normally, a new operating system requires better hardware than the previous version. Hardware requirements should be checked before doing an upgrade. Insufficient hardware may cause a new operating system to run slowly. Often a faster processor and more memory are required, but other components may also need to be upgraded.
- **Setup errors and freezes:** Such problems could be caused by insufficient disk space or RAM or by incompatible drivers.
- **Drivers:** Drivers often cause trouble related to operating system upgrades. Unfortunately, sometimes vendors don't update their drivers to work with the newest systems, and this might make it necessary to buy a new expansion card or another component.
- **Application incompatibilities:** You can try some workarounds to get an older application to work with a new operating system, but sometimes the best course of action is to upgrade or replace the application with a compatible version.
- **Data loss:** Data loss can be tragic, and it is the most preventable of all possible problems. User data should be stored on a different partition (if you have only one hard disk), on a different physical hard disk, on a different server, or in the cloud; data should be backed up regularly.

Compatibility Concerns

Computers are considered compatible within a family if software that runs on one model can run on all other models, even if performance, reliability, or other features vary. Hardware compatibility means that some components, such as a RAM chip, can be used on various models.

One consideration is related to 32-bit versus 64-bit systems. Most new systems today include processors that are based on a 64-bit architecture. These systems are compatible with 32-bit operating systems and 32-bit applications, but the converse is not true: 32-bit hardware cannot support 64-bit operating systems and applications.

Software **compatibility** can refer to whether a particular application must be used with a specific CPU architecture, such as Intel. It can also refer to the ability of software to run on one or more operating systems or one or more versions of an operating system.

When purchasing software, it is important to consider compatibility. Sometimes even upgrading software you are already running can cause incompatibility issues. Software released for a newer version of an operating system may not work or may not work as expected on an older version of the same operating system.

Forward compatibility, also known as **upward compatibility**, is designed by the software manufacturer. It means that a system should be able to accept input intended for a later version and is meant to allow older devices to recognize when data has been generated for new devices. An application that has been designed with forward compatibility usually also has **backward compatibility**, which means the new system can still process data from the older software.

Software with both forward and backward compatibility is not the same as software that is extensible. A forward-compatible system only means that older software is able to process some of the data from a new version of itself, but an extensible system, or **extensible software**, can be upgraded easily.

Because of the nature of operating systems, software is never completely compatible between different operating systems. For example, the Microsoft Word application written for macOS cannot run on Windows, and the Microsoft Word application written for Windows cannot run on macOS. Each operating system requires a unique version of Microsoft Word. However, the documents created in the OS-specific versions of Microsoft Word are usually compatible across operating systems.

A computer can have more than one OS installed. By dividing a hard drive into multiple sections called partitions, it is possible to use a dual-boot system. For example, when an Apple hard drive is partitioned, Windows can run on one partition and macOS on the other. With this type of setup, you would have to buy Windows-compatible software for the Windows partition and Apple-compatible software for the macOS partition.

One thing that must be considered when using a dual-boot system is what happens with the data. Luckily, most **file types** are compatible with both macOS and Windows. However, sharing folders may result in some issues because macOS and Windows deal with folders differently.

Corporate Operating System Needs

In a business environment, users have different needs than they would have at home. Also, corporate computers may have different operating systems than home computers. This is because an operating system in a corporate environment requires networking, configuration, and management features that are typically not needed in a home environment. Let's take a look at some of these differences.

Business computers tend to be organized in either a domain or a workgroup. In Windows, the concept of a domain is different from that of a workgroup:

- **Domain:** Domains are used to create networks in medium to large companies. **Active Directory (AD)**, which is part of the Microsoft Windows Server operating system, provides centralized authentication, authorization, and configuration for the network devices and people using the domain. Within AD, an organizational structure can be created to separate devices and people by location, department, or function. Single users or user groups can be authorized to use specific computers or groups of computers. Settings can be automatically applied to computers when they boot up or to user accounts when people log in to any authorized computer. Software can be automatically installed on each computer that needs it. AD enables IT staff to implement security policies and provide support and changes easily and efficiently.
- **Workgroup:** In Windows, a workgroup is an alternative to a domain. In a workgroup, settings are manually configured on each computer, and user accounts are manually created on each computer. Each computer has a separate user account for each unique person who needs to use that computer. If a user wants to use multiple computers, a separate user account must be created on each computer. A user's account settings must be configured manually on each device. In addition, software is manually installed on each computer that is part of a workgroup.

Windows workgroups are difficult to manage when there are more than a few users or computers, so they are more suitable for small businesses or home office networks. Active Directory, on the other hand, offers single sign-on, disaster recover functionality, and many security features that are lacking with workgroups. This makes Active Directory a better choice for larger businesses and organizations.

Domain Access

Computers in a business environment that has more than 10 computers commonly are registered with one or more domain controllers. A *domain controller* is a network server that has a network operating system installed. It has a centralized database that contains all the registered users and network devices. When a user logs into a company computer, the domain controller verifies the username and password to ensure that the user is allowed on the company network. A medium to large company is organized into one or more domains created on the domain controller. An authorized user who successfully logs into the domain is granted **domain access**.

Remote Desktop Protocol (RDP)

Remote Desktop Protocol (RDP) enables a user to access and use a computer remotely over a network instead of using the local keyboard, mouse, and monitor. With this feature, a technician can work on a computer, a laptop, or a server without leaving their home or office. This capability is very useful in companies that have hundreds of desktops or servers, especially if they are spread over a large geographic area. RDP is available in all Windows 10 and Windows 11 editions except the Home editions.

BitLocker

BitLocker Drive Encryption is a Windows data protection feature that scrambles the data on internal drives. If a drive is removed from a computer, a password is required to access its data. This is of particular interest to companies because laptops are often lost, computers are frequently stolen, and drives are easily removed. BitLocker helps reduce the threat of unauthorized access by enhancing file and system protections. When computers are decommissioned or recycled,

BitLocker protection helps render data inaccessible. **BitLocker To Go** provides the same data protection on removable drives such as USB flash drives, SD cards, and external hard disks. Both BitLocker and BitLocker To Go can optionally use a Trusted Platform Module (TPM), which is a chip on the motherboard that stores security information such as encryption keys.

There are two additional tools that can be used to manage BitLocker: BitLocker Recovery Password Viewer and BitLocker Drive Encryption. A best practice is for technicians to back up BitLocker recovery passwords. The BitLocker Recovery Password Viewer allows a technician to see those passwords. BitLocker Drive Encryption, which is used from the command line, is used when scripts involving drive deployment or refreshes are created and deployed. Chapter 15 covers PowerShell cmdlets and scripting in more detail.

Encrypting File System (EFS)

Some corporate environments require that specific files and folders be encrypted, especially on a laptop that might be stolen or on a computer that contains sensitive data. Corporate versions of Windows include a feature called Encrypting File System (**EFS**), which allows you to encrypt a file or folder as easily as making a file or folder read-only. Whereas BitLocker encrypts an entire drive, EFS allows you to control the encryption on a file or folder basis.

To enable EFS, right-click on any file or folder and select *Properties* > click the *Advanced* button > enable the *Encrypt Contents to Secure Data* checkbox > click *OK*. When you are encrypting a folder, you may be asked if you want the encryption for just this folder or for all subfolders and files as well. Click *OK* again if necessary. When you are prompted to back up the file encryption certificate and key for security purposes, save the certificate to a separate drive. This file is very important for decrypting files and folders.

When a file or folder is encrypted, you see what looks like a little lock over the file icon. To store and retrieve an encrypted file or folder, the user must request a key from a program that is built into Windows.

Basic Windows Usage Overview

If you have been using a Windows-based computer your entire life, you might find this first look at the Windows environment a little dry. It's the basics. However, little technical tricks and tips are among these basics, and even veteran technicians are likely to at some points say, "I didn't know that." So, look for those.

Windows Desktop/Start Screen

On a Windows computer, the user is initially presented with a logon screen. To gain access to the computer, the user must enter a user ID and password/PIN. On standalone and workgroup computers, the user ID and password/PIN can be created during the Windows Out-of-Box Experience (OOBE), which is the setup process that the user completes when the computer is first turned on. If the computer is connected to the internet, the user can also log in with their existing Microsoft account, or they can create a new Microsoft account. After the computer has been set up, additional authorized users can be created in Settings. In a domain network environment, user accounts are created and maintained in a directory database, which resides on a domain controller server. Windows computers can also be configured to allow access via facial recognition or fingerprint.

After the user logs in to the Windows environment, the desktop appears (see Figure 14.4). The **desktop** is the area on the screen of a GUI environment in which all work is performed. It is the interface between the computer user and the files, applications, operating system settings, and hardware that make up the computer. The desktop contains **icons**, which are pictures that provide

access to various devices, files, applications/apps, or other resources, such as a printer. The desktop can be customized so that the most commonly used applications or files are easily accessible.

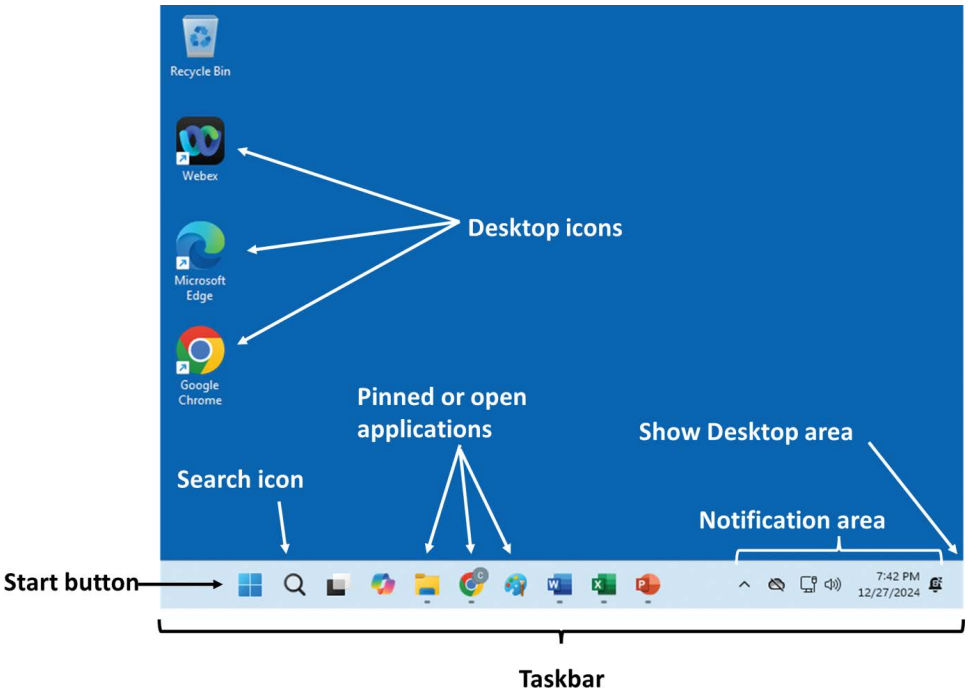


FIGURE 14.4 Windows 11 desktop

Windows 11 Desktop Components

The Windows 11 desktop has specific components. Figure 14.4 show a Windows 11 desktop with the primary components labeled.

Taskbar

The **taskbar** is the bar that commonly runs across the bottom of the desktop, which holds icons that allow quick launching of applications and icons that represent applications or files currently loaded into the computer's random access memory (RAM). The taskbar also holds icons that allow access to system utilities, such as a clock for the date and time and a speaker symbol for volume control. (Refer to Figure 14.4 to ensure that you know the location of the taskbar.) The basic Windows 11 taskbar consists of the five areas shown at the bottom of Figure 14.4: the Start button, the Search box or icon, the open or pinned applications area, the notification area, and the Show Desktop area.

Start Button

The **Start button** is used to launch applications and utilities, search for files and other computers, obtain help, and add and remove hardware and software. As shown in Figure 14.4, the Windows 11 Start button is at the left of a group of icons that are centered on the taskbar. In previous versions of Windows, the Start button was in the lower-left corner. To return the Windows 11 Start button to the lower-left corner, right-click the *taskbar* > *Taskbar settings* > *Taskbar behaviors* > *Taskbar alignment* > *Left.*

The Start menu, shown in Figure 14.5, appears when the user clicks the Start button. The Windows 11 Start menu consists of four sections: Pinned (apps), All (apps), Recommended (apps

and files), and More (apps and files). The pinned apps are a subset of all the applications available on the computer. To view all the apps on the computer, click the *All* button. You can configure the contents of the Pinned section via *All* > right-click an app > click *Pin to Start* or *Unpin from Start*.

Microsoft and/or the computer manufacturer configures the apps that appear in Recommended. Additional apps, files, and tools will appear in Recommended as you use the computer. Click the *More* button to see all the recommended resources.

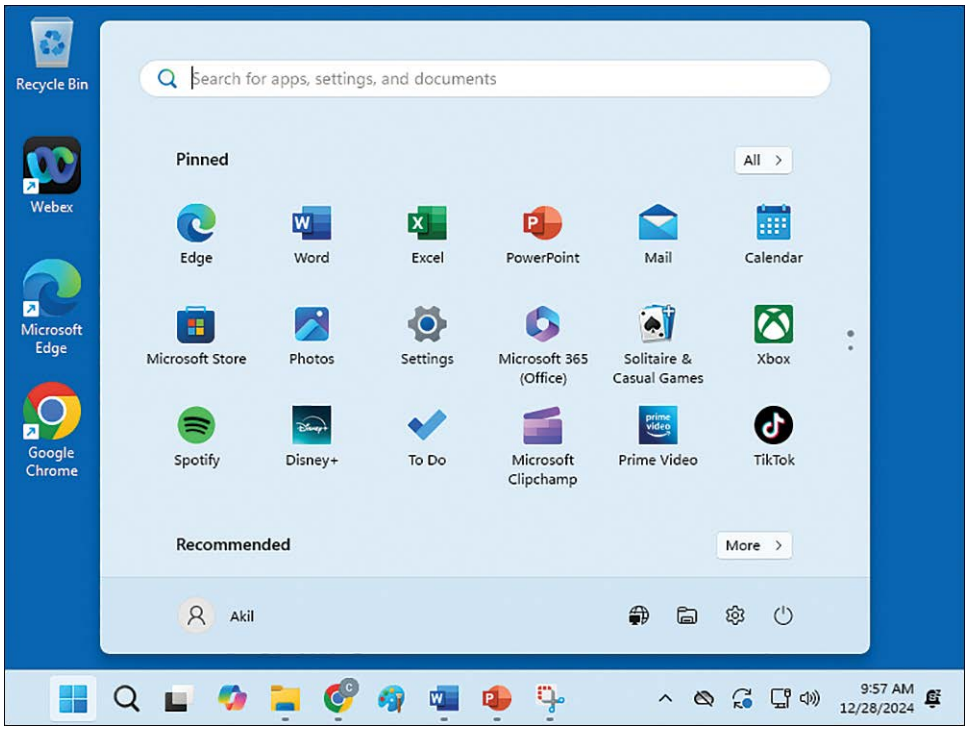


FIGURE 14.5 Windows 11 Start menu

TECH TIP

Start button missing?

The Start button (along with all other items on the taskbar) may not be visible if you enable *Automatically hide the taskbar*. You can press the ⊞ key to show the Start menu.

Shutdown Options

Shutdown options are located in the lower-right corner of the Start menu (see Figure 14.6). Click *Start* > ⏻, and the options *Shut down* and *Restart* appear. The options *Lock* and *Sleep* also appear if your computer can be configured for those modes. Some Windows updates need to be applied while the computer is booting up. If such updates are available, the options *Update and shut down* and *Update and restart* appear.

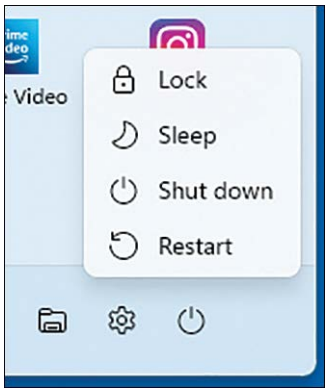


FIGURE 14.6 Windows 11 shutdown options

Task View

Windows 11 offers **Task View**, which enables you to view thumbnails of open apps and easily select which one to access (see Figure 14.7). You may be familiar with using the Alt+Tab key combination to select an open window; Task View does the same thing but more efficiently. You can also create more than one desktop by selecting the *New desktop* option in Task View. Figure 14.7 shows two desktops created. The windows open in Desktop 1 (selected at the bottom) are shown as thumbnails at the top of the figure.

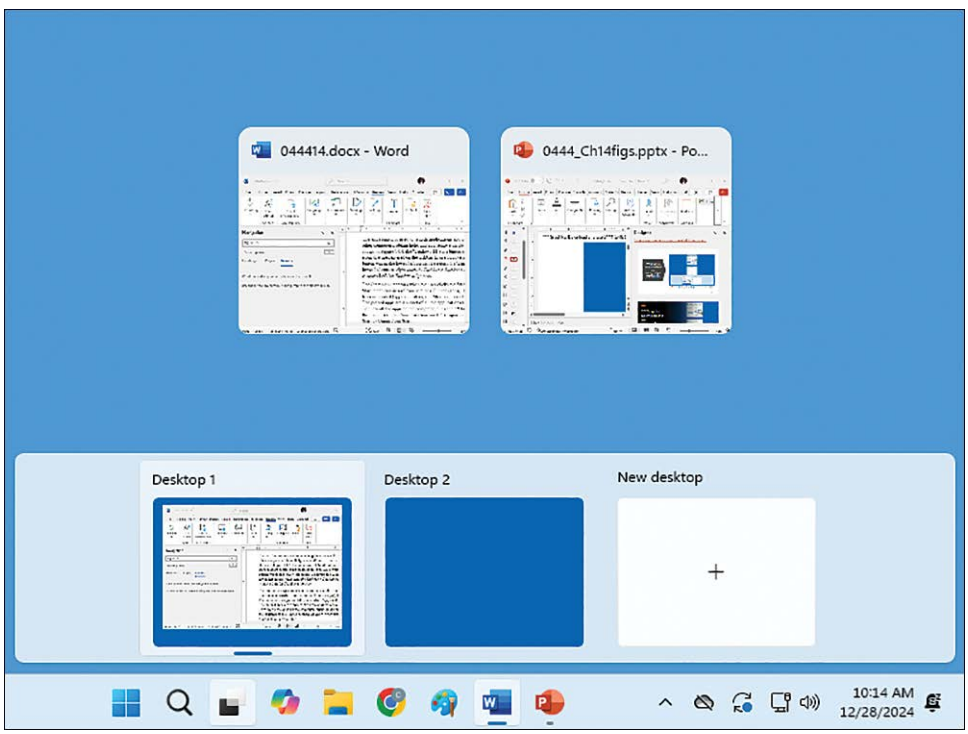


FIGURE 14.7 Windows 11 Task View window

Search Function

The search function is built into the taskbar and can appear as a search icon (magnifying glass) or as the *Search* textbox.

Running, Open, and Pinned Applications

When a user starts an application (such as from the Start menu), the application's icon appears on the taskbar. In Figure 14.4, the small gray bar under the taskbar icons indicates that the following applications are running in the computer but their windows are minimized: File Explorer, Google Chrome, Word, Excel and PowerPoint. If the user opens an application window, a longer blue bar will appear under the icon. The Windows Copilot and Paint applications are not running, so their icons do not have bars under them. However, these icons appear on the taskbar because the applications are pinned to the taskbar. Pinning an application to the taskbar provides quick access to the application.

TECH TIP

How to modify the buttons shown on the taskbar

To pin an application to the taskbar, launch the application, locate the application icon on the taskbar, right-click the icon, and select *Pin to taskbar*.

Notification Area

On the far right of the taskbar is the **notification area**, where you can find information about an application or a tool. In Figure 14.4, for example, the following icons are shown, from left to right: Show hidden icons (up arrow), OneDrive, Network, Notifications.

Show Desktop Area

The space on the far right of the taskbar is the Show Desktop area. A short vertical line appears in Windows 11 when the cursor is in the Show Desktop area. Clicking this area instantly minimizes all open windows and shows the desktop. Clicking the area again reopens the windows.

TECH TIP

Keeping the desktop organized

The Windows desktop may become cluttered with icons the user puts on it. To organize the desktop nicely, right-click an empty desktop space, point to *View* > select *Auto Arrange Icons*.

Shortcuts

Each icon on the desktop is a shortcut. A **shortcut** represents a **path** (a location on a drive) to a file, folder, or program. It is a link (pointer) to where the file or application resides on a disk. On the desktop, a shortcut has a small arrow in the lower-left corner. When a shortcut icon is double-clicked, Windows uses the associated path to find the specific item that the icon represents. Users and technicians frequently place shortcuts on the desktop, and it is important to know how to create, remove, modify, and troubleshoot them.

By default, the Windows 11 desktop displays the Recycle Bin icon only. However, some people like to have other Windows icons displayed. Common desktop icons and tiles are listed in Table 14.3.

TABLE 14.3 Common Windows desktop icons or tiles

Icon	Purpose
Documents	Maps to a folder location that is the default storage location for files
This PC	Allows access to hardware, software, and files
Network	Allows access to network resources, such as computers, printers, scanners, fax machines, and files
Recycle Bin	Holds files and folders that have been deleted
Edge	Starts the Microsoft browser that is used to access the internet

To discover the path to the original file used to create a shortcut, right-click the shortcut icon and select *Properties*. Click the *Shortcut* tab and look in the *Target* textbox for the path to the original file. The *Open File Location* button can be used to locate the actual file.

Recycle Bin

The Recycle Bin holds files and folders that the user deletes. When a file or folder is deleted, it is not actually gone. Instead, it goes into the Recycle Bin, which is just a folder on the hard drive. The deleted file or folder can be removed from the Recycle Bin just as a piece of trash can be removed from a real trash can. Keep in mind that deleted files and folders in the Recycle Bin consume hard drive space. To change how much space is reserved for the Recycle Bin or the drive on which the deleted files in the Recycle Bin are stored, right-click the *Recycle Bin* and select *Properties*. To permanently delete a file that is in the Recycle Bin, right-click the file and select the *Delete* icon (which looks like a trash can). To delete all the files from the Recycle Bin, right-click the *Recycle Bin* and select *Empty Recycle Bin*.

TECH TIP

Need hard drive space? Empty the Recycle Bin

A technician must remember that some users do not empty the Recycle Bin. Emptying the Recycle Bin frees up space on the hard drive.

TECH TIP

How to delete a file permanently

If you hold down the ⇧Shift key when deleting a file, the file is permanently deleted rather than going into the Recycle Bin.

TECH TIP

Removable media files are permanently deleted

When deleting a file or folder from an optical disc, a memory card, a digital camera, a remote computer, or a flash drive, the file or folder is permanently deleted. It does not go into the Recycle Bin, as is the case when a file is deleted from a local hard drive.

Interactions Within a Window

Whenever anything is double-clicked in Windows, a window appears. A **window** is a square or rectangular section on the screen. A dialog box is one type of window. Technicians frequently interact with the Windows operating system through dialog boxes. Dialog boxes allow a technician to configure application and operating system preferences. The most common features in dialog boxes are checkboxes, textboxes, tabs, drop-down menus, a Close button, an OK button, a Cancel button, and an Apply button. Figure 14.8 shows a sample dialog box.

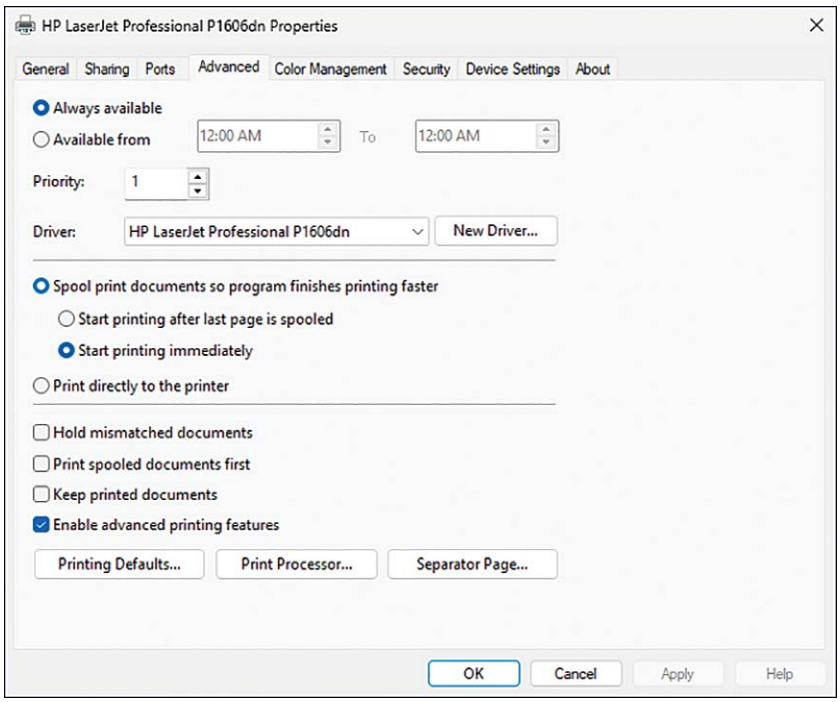


FIGURE 14.8 HP Printing Preferences dialog box

A textbox is an area where you can type a specific parameter. When the inside of a textbox is clicked, a vertical line or an entire default word appears. Any typed text is placed to the left of the insertion point. If you highlight any of the text in a textbox and then type, the original text is replaced with the text that you type. Up and down arrows are very common on textboxes for numeric values (see the *Priority* field in Figure 14.8).

Tabs frequently appear across the top of a dialog box. Each tab holds a group of related options. Click a tab once to bring that particular major section to the window's forefront. The tabs in Figure 14.8 are General, Sharing, Ports, Advanced, Color Management, Security, Device Settings, and About.

The **Apply button** saves changes immediately. The dialog box remains open after you click the Apply button. When you click the *OK* button, all options that are selected or changed are saved, and the dialog box is closed. The *Close* button, which is an *X* in the upper-right corner of the dialog box, closes the dialog box. You can click the *Close* button to discard updates made to the dialog box since the last time the *Apply* button was clicked; the same is true for the *Cancel* button.

TECH TIP

Click *OK* or *Apply* to make it work

To apply a change, inexperienced technicians often make the mistake of clicking the *Close* button (the red *X* button in the top right of a dialog box) instead of the *OK* or *Apply* button. When the *Close* button is used, changes in the dialog box made after the last Apply are neither saved nor applied.

Clicking inside a checkbox option places a check mark inside the checkbox, such as the one for *Enable advanced printing features* in Figure 14.8. When a checkbox option is checked, it is enabled or turned on. If you click inside the checkbox again, the check is removed, and the option is not enabled.

Another dialog box option is a radio button. A radio button is a circle that has a solid dot inside it when its value is enabled. The circle is empty if its value is not selected. This type of control inside a dialog box is used to select one of multiple options available for a specific setting. For example, in Figure 14.8, the *Always available* radio button is enabled for the printer's availability setting, and the *Available from* option is disabled.

When a drop-down menu is clicked, all the options that are available for the setting appear in the drop-down menu. Figure 14.8 shows one drop-down menu: the *Driver* option, in which *HP LaserJet Professional P1606dn* is selected.

Within a dialog box, help is commonly provided as *context-sensitive help*. To access context-sensitive help, simply hold the pointer over a particular item, and one or more words appear to assist with that setting.

Another popular type of interaction is with a **context menu**, which appears when you right-click an item on the desktop, in the **Start screen**, or in File Explorer. The context menu that appears is different in every situation but usually includes options that are available from the main menu or from Windows Settings. Technicians often use context menus to save time when managing settings and applications.

Managing Windows Files and Folders

Technicians often use File Explorer to create, delete, and move files and folders. You need to do these tasks quickly and without error. It is important to think about what file and folder you want to work with, where the items are initially located, and where you ultimately want them to be stored.

Each drive in a Windows computer is represented by a drive letter followed by a colon. For example, the first hard drive partition is represented by `C:`. The optical drives, flash drives, and any external drives are each represented by their own drive letters followed by a colon. Figure 14.9 shows drive letters within File Explorer on a Windows 11 computer.

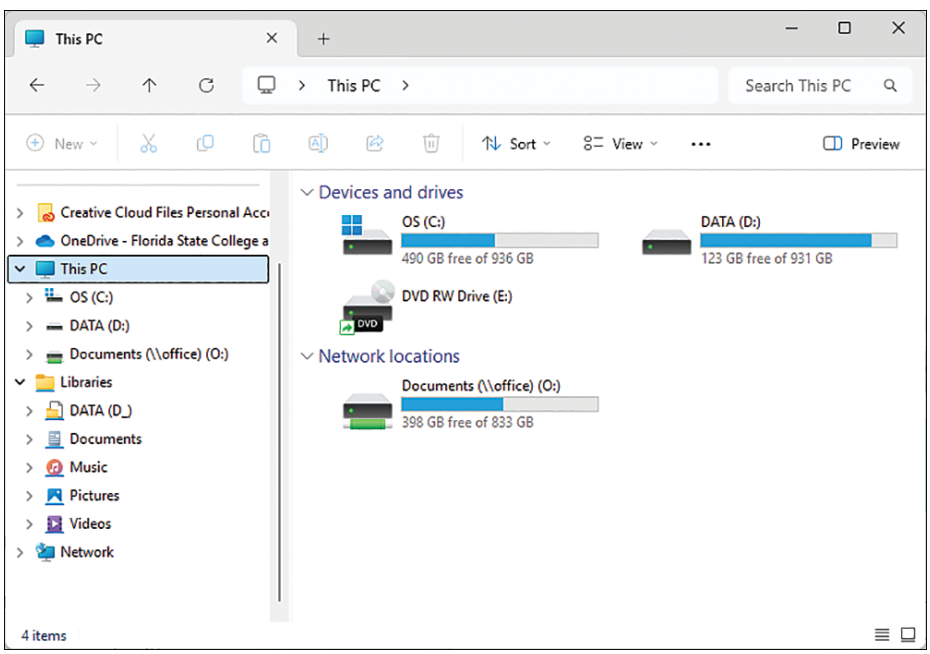


FIGURE 14.9 Windows 11 File Explorer drive letters

Folders, Filenames, and Extensions

Discs and drives hold files and folders. Files are usually organized in folders. In older operating systems, a folder was called a *directory*, and you still see this term today, especially when using the command-line interface. A folder within a folder is called a **subfolder** or **subdirectory**. A **library** is an automatic grouping for saving files. Some common Windows 11 libraries are Desktop, Downloads, Documents, Music, Pictures, and Videos. Applications save files in these libraries by default, based on various criteria, such as the type of file. You can create additional libraries, as needed.

Each file is given a name that includes two parts separated by a dot: the **filename** and the **extension**. For example, in the name `WIN8CHAP.DOCX`, the filename is `WIN8CHAP`, and the extension is `DOCX`. In Windows, filenames are not case-sensitive, so the filename `WIN8CHAP.DOCX` is the same as `Win8Chap.docx`. Therefore, the case does not matter when searching for a file or typing the name of a file to open. Each item in a folder must have a unique filename, so the file `WIN8CHAP.DOCX` cannot be saved in a folder that already contains the file `Win8Chap.docx`. Note that some operating systems, like Linux, are case-sensitive with respect to filenames.

TECH TIP

Characters you cannot use in filenames and folder names

Folder names and filenames can include all keyboard characters, numbers, letters, and spaces *except* the following: / (forward slash), " (quotation mark), \ (backslash), | (vertical bar), ? (question mark), : (colon), and * (asterisk).

When Windows recognizes an extension, the operating system associates the extension with a particular application. An extension can tell you a lot about a file, such as what application created the file or what its purpose is. Table 14.4 lists some common file extensions and their purpose or the application that creates the extension.

TABLE 14.4 Common file extensions

Extension	Purpose or application	Extension	Purpose or application
AAX	Audible enhanced audio file	JPG or JPEG	Joint Photographic Experts Group graphics file
AI	Adobe Illustrator or Corel Trace file	MPG or MPEG	Movie clip file
BAT	Batch file, for executing commands from one file	ONE	Microsoft OneNote file
BMP	Bitmap file	PCX	Microsoft Paintbrush file
CAB	Cabinet file, a compressed file that holds operating system or application files	PDF	Adobe Acrobat portable document format file
COM	Command file, an executable file that opens an application or a tool	PNG	Microsoft Paint or Snipping Tool graphics file
DLL	Dynamic link library file, which contains executable code that can be used by more than one application and is called upon from other code that is already running	PPT or PPTX	Microsoft PowerPoint file
DOC or DOCX	Microsoft Word file	RTF	Rich text format file

Extension	Purpose or application	Extension	Purpose or application
DRV	Device driver, a piece of software that enables an operating system to recognize a hardware device	TIF or TIFF	Tag image file
EPS	Encapsulated PostScript file	TXT	Text file
EXE	Executable file, a file that opens an application	VXD	Virtual device driver
GIF	Graphics interchange file	WPS	Microsoft Works text file
HLP	Windows-based help file	WRI	Microsoft WordPad file
INF	Information or setup file	XLS or XLSX	Microsoft Excel file
INI	Initialization file, used in older Windows environments	ZIP	Compressed file

In most views, Windows does not automatically show the extensions. To view file extensions in Windows 11, open *File Explorer* and click *View* > *Show* > *File name extensions* (see Figure 14.10).

When you save a file in a Windows application, the application automatically saves the file to a specific folder or library, known as the *default folder* or *default library*, unless the user specifies a different folder. With many applications, the default folder is the *Documents* folder or a folder for Microsoft OneDrive or another cloud-based storage solution.

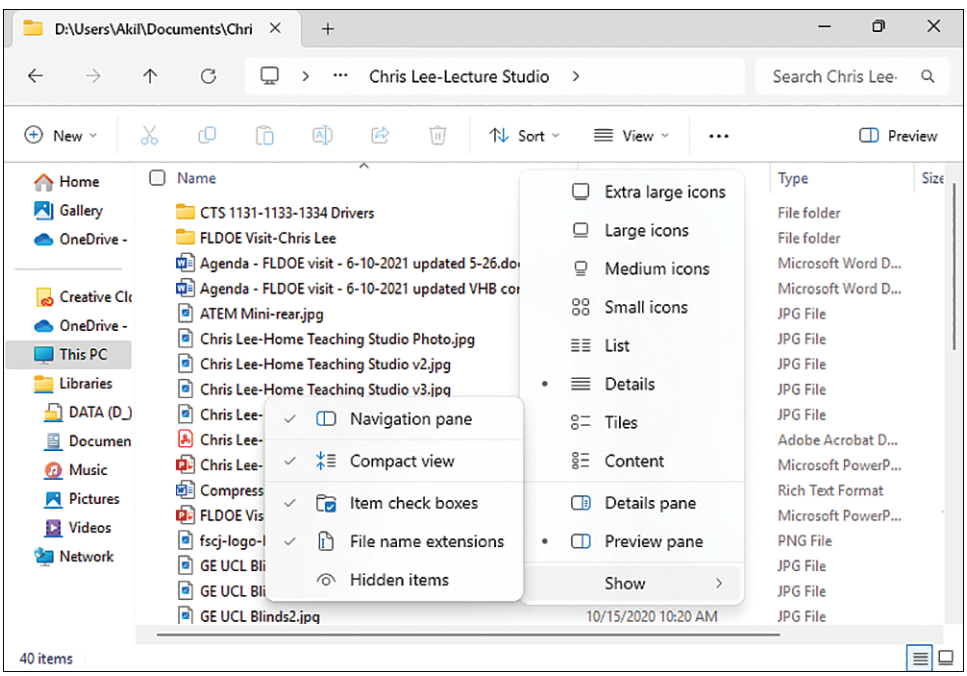


FIGURE 14.10 Selecting to view file extensions in Windows 11

File Explorer Path

A file's full path is like a road map to the file. It is often used in documentation, installation instructions, and other situations where the exact location of a file on a computer is very important. The full path consists of the drive letter plus all folders and subfolders that must be followed to get to that file's filename and extension. For example, let's say that the `webgl_sharing` file is

in the `Krazy Karts` folder, which is in the user Akil's Documents folder on the `D:` hard drive partition. In this case, the full path is as follows:

```
D:\Users\Akil\Documents\Krazy Karts\webgl_sharing
```

The first part of the file path is the drive letter where the file is stored—in this case, `D:`, which represents the hard drive partition. The name of the file is always at the end of the path. In our example, `webgl_sharing` is the name of the file. Everything between the drive letter and the filename is the name of one or more folders to get to where the `webgl_sharing` file is located. The drives, top-level folder, subfolders, and filename are separated by backslashes (the \ keyboard key, which is above the ↵ Enter key). The top-level folder in this example is `Users`. The `Akil` subfolder is in the `Users` folder. Another subfolder called `Documents` is in the `Akil` subfolder, and `Documents` contains another subfolder, `Krazy Karts`. Finally, the file `webgl_sharing` is stored in `Krazy Karts`. Figure 14.11 shows how this looks in Windows File Explorer.

Notice that the folder path appears in the address bar at the top of the File Explorer window, and the filename appears within the `Krazy Karts` folder. Note that this was done intentionally to show you the full path. However, when you open File Explorer and click the `Documents` library in the left navigation pain, the `Users` and `Akil` folders are not shown in the address bar. The path simply appears as `This PC > Documents`. That's because the `Documents` library has been associated with the full path `D:\Users\Akil\Documents`.

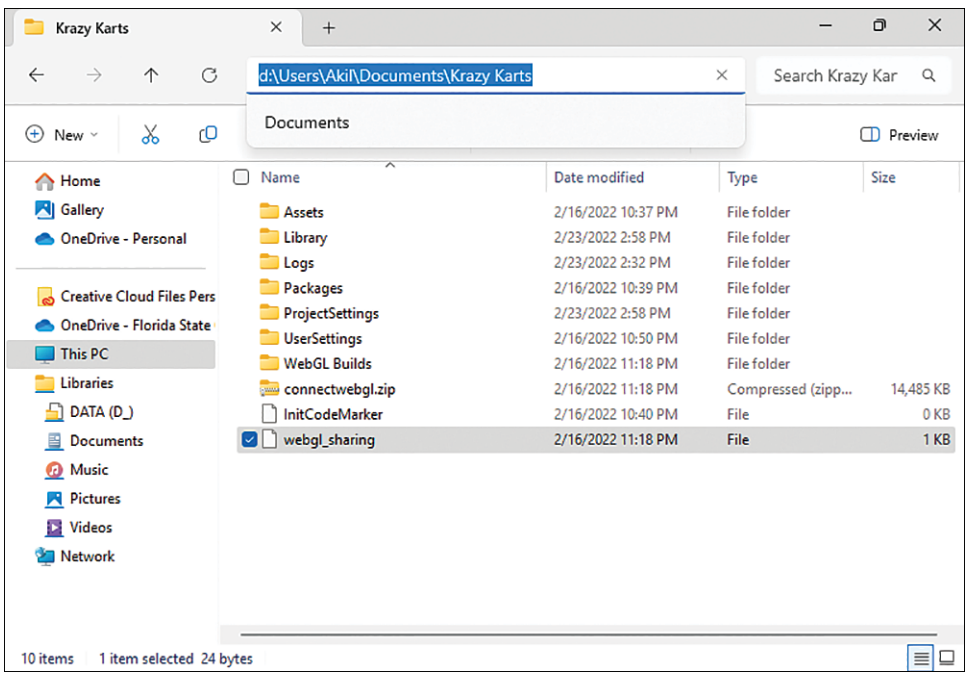


FIGURE 14.11 Windows File Explorer full path

As you navigate in File Explorer, the greater-than symbol (>) separates the drive, the folders, and the subfolders in the address bar. If you click to the right of the words in the address bar, the full path appears. Note that if you are viewing a library, only the name of the library appears when you click to the right of the library's name. When writing a complete path to a folder in a dialog box or in a command-line interface, a backslash is always used to separate the items in the path.

By default, only the name of the last folder in the path appears in the File Explorer title bar (the name area at the top of the File Explorer tab). To display the full path in the title bar, open File Explorer > click the three dots beside the *View* menu > select *Options* > select the *View* menu option > enable the *Display the full path in the title bar* option (see Figure 14.12). Only the first few characters appear in the title bar. Hover over the title bar to see the full path.

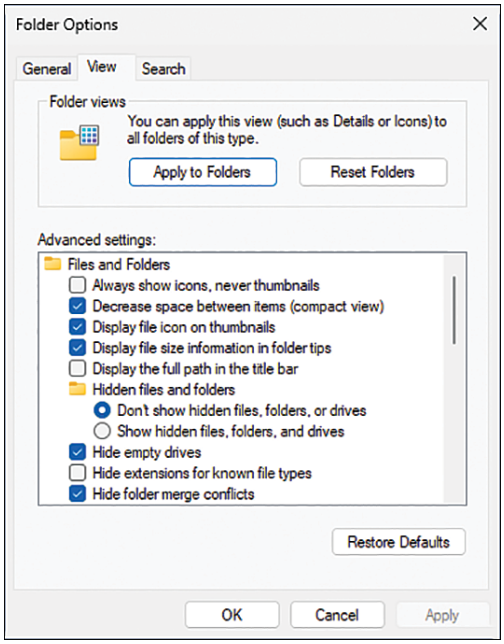


FIGURE 14.12 Windows 11 Display the full path in the title bar option

File Explorer View Options

It is important for a technician to be able to control how files and folders are displayed in File Explorer. Table 14.5 describes the basic View options that are available in File Explorer.

TABLE 14.5 File Explorer View options

File Explorer View option	Description
List	The icon and filename are displayed for each item. The items are sorted in vertical columns.
Details	The items are sorted in a table with configurable columns: name (and icon), modification date, file type, file size, and other optional columns.
Small Icons, Medium Icons, Large Icons, Extra Large Icons	Varying size file/folder icons appear with the file or folder name shown beside or under each icon. The items are sorted in horizontal rows.
Content	A single column of reduced-size icons appears, with file/folder name, file type, modification date, and file size.
Tiles	Multiple rows of file/folder icons appear with name, file type, and size shown.

Figure 14.12 shows more options that can be used to change how files, folders, images, and so on display in File Explorer. These options and many other settings are also available in File Explorer Options, which contains all the folder and search options. To access File Explorer Options in Windows 11, open *File Explorer* > click the *three dots beside the View* menu > select *Options* (see Figure 14.13).

Figure 14.14 shows the options that are available in the *General* tab, which has three main sections: Browse folders, Click items as follows, and Privacy. Each section has either radio buttons or checkboxes to enable various items.

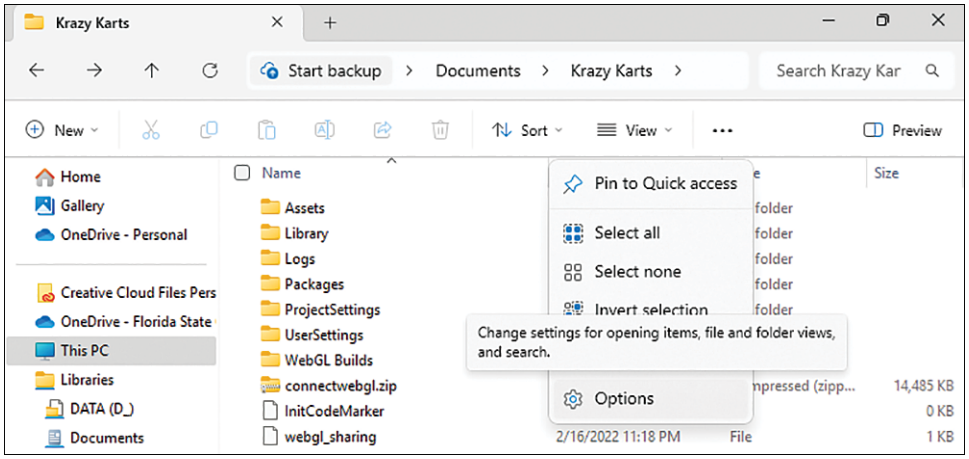


FIGURE 14.13 Windows 11 File Explorer Options button

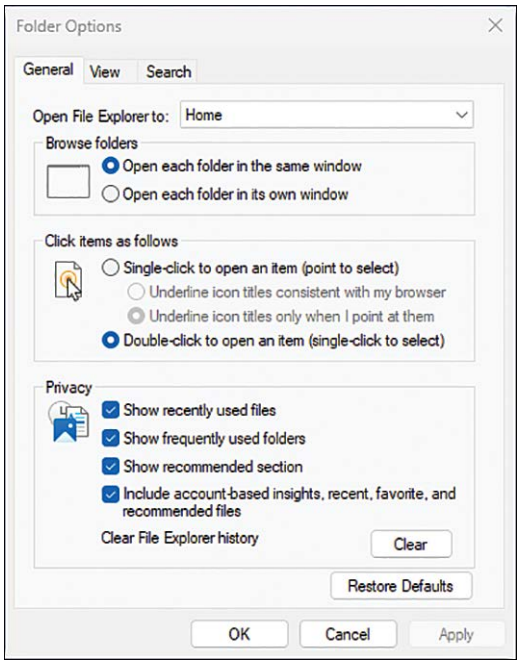


FIGURE 14.14 Windows 11 File Explorer Options > General tab

Figure 14.12 shows some of the options available in the View tab. A technician should be able to set the following important options through this window:

- View hidden files by using the *Hidden files and folders* settings
- Hide file extensions by using the *Hide extensions for known file types* checkbox
- Use other options on the *View* tab, including those for resetting the settings or applying them to subfolders and displaying full paths

Searches and Indexing

You can perform a search from within File Explorer by typing a filename or phrase in the *Search* textbox on the taskbar (refer to Figure 14.5). When you type a word or phrase in the *Search* textbox, Windows 11 looks for the word or phrase in several places:

- Filenames of the files on the computer
- Data within the files on the computer

> Names and descriptions of available computer settings
> Links in your web browser history
> The World Wide Web

The *Search* tab in the *Folder Options* window controls the Windows index feature, which affects searches within the operating system. Figure 14.15 shows the contents of this tab. **Indexing** is the process used in Windows to quickly search common locations for files and folders, including all libraries, the Start button menu, and Edge browsing history. (See the next sections to learn how to select which locations to index.) In Windows 11, the index is used for all searches by default, but the *How to search* section of the *Search* tab allows you to ignore the Windows index when searching. Enabling this option means that all the files and folders in the drive, folder, or subfolder will be searched, so searches might take longer. Files and folders to search outside the indexed locations can be specified in the *When searching non-indexed locations* section.

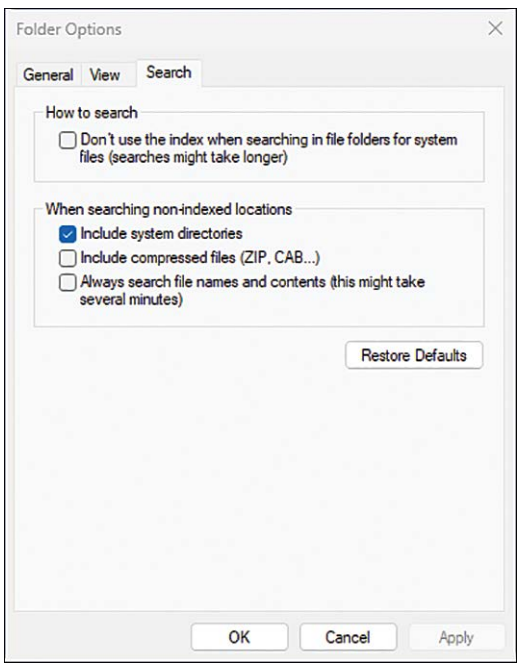


FIGURE 14.15 Windows 11 Folder Options > Search tab

Modifying Index Locations

To modify what locations are indexed, use File Explorer to search for `indexing` > select *Indexing Options* from the resulting list. Use the *Modify* button or *Advanced* button to change the settings. For example, if you want to exclude a particular folder and its contents from the index, click *Modify* > navigate to the folder > uncheck the folder. Note that you cannot exclude individual filenames from being indexed. Figure 14.16 shows the Indexing Options window as well as the window that appears if you click the *Advanced* button.

If you don't want a file's contents to be indexed and easily found, in File Explorer you can right-click the filename, select *Properties* > *Advanced* button > disable (uncheck) the *Allow this file to have contents indexed in addition to file properties* option.

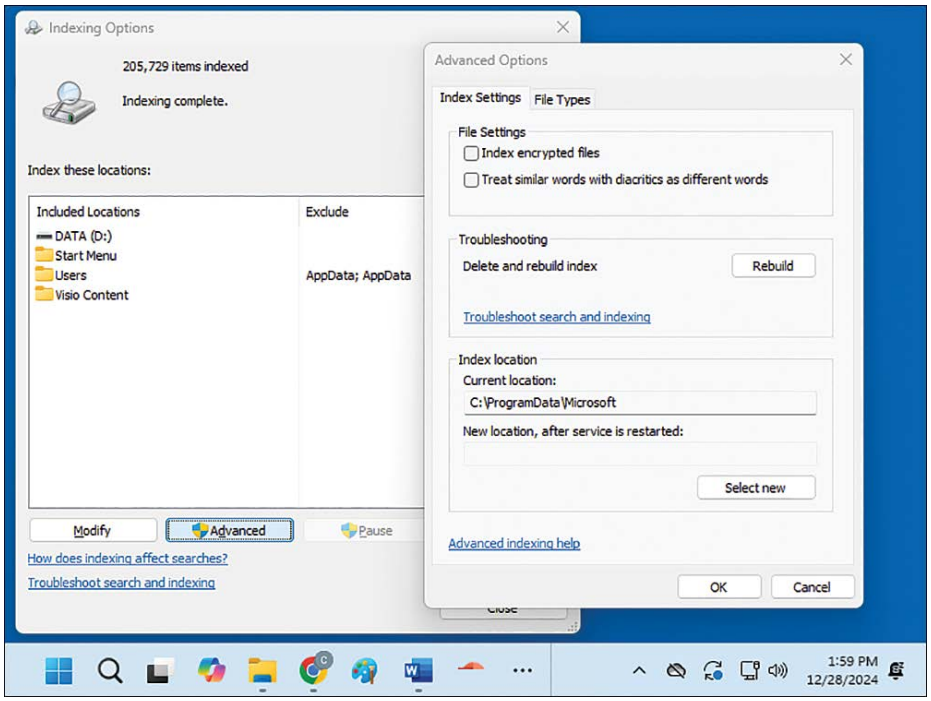


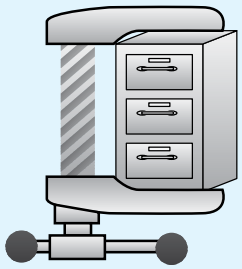
FIGURE 14.16 Windows 11 Indexing Options > Advanced button

Attributes, Compression, and Encryption

File Explorer can be used for setting attributes, which are specific qualities for a file or folder. The basic file and folder **attributes** are read-only, hidden, archive, and system, as shown in Figure 14.17. Files and folders can also be compressed and encrypted (see Figure 14.18).

	The read-only attribute marks a file or folder so that it cannot be changed.
	The hidden attribute marks a file or folder so that it is not visible through File Explorer unless you change the default view.
	Some applications use the archive attribute to control which files or folders are backed up.
	The system attribute is placed on certain files used to boot Windows.

FIGURE 14.17 Windows file/folder attributes



Compression involves compacting a file or folder to take less disk space. Right-click on a file/folder to be compressed > *Properties* > *General* tab > *Advanced* > *Compress contents to save disk space* or *Compress* checkbox > *OK*.

Encryption secures data from unauthorized users using an encryption feature called **EFS** (encrypting file system). Right-click on a file/folder to be encrypted > *Properties* > *General* tab > *Advanced* > *Encrypt contents to secure data* checkbox > *OK*.

FIGURE 14.18 Windows compression and encryption

TECH TIP

How to change a file's or folder's attributes

To change a file's or folder's attributes, right-click the filename or folder name > *Properties*. The Read-only and Hidden attributes appear at the bottom of the dialog box (see Figure 14.19). Click *Advanced* to see the archive, indexing, compression, and encryption attributes (see Figure 14.20). Click the appropriate attribute checkboxes to enable or disable them. Click *Apply*. (If a file is a system file, the system attribute is also available.)

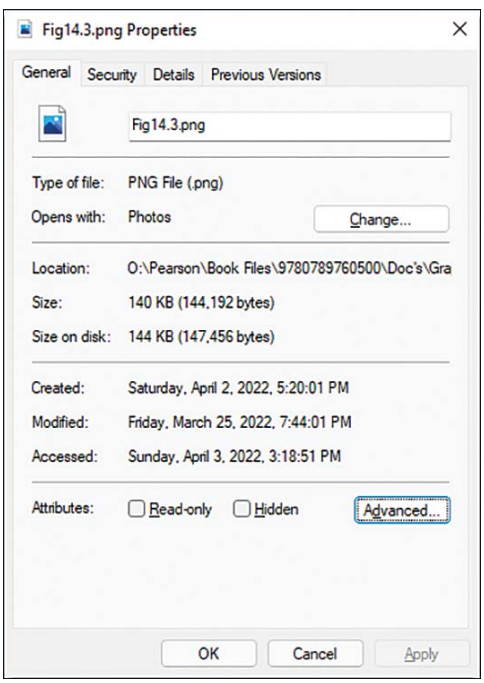


FIGURE 14.19 File Properties View tab

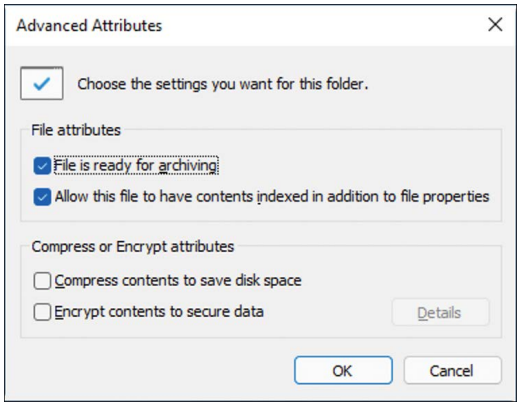


FIGURE 14.20 Advanced Attributes dialog

The archive attribute is enabled by default on Windows files and folders. This is sometimes referred to as having the archive bit set. A backup program can be configured to copy a file to the backup location only if its archive bit is set. After the file is backed up, the archive bit is reset. The bit will be set again when the file's contents change or when a user manually sets it in the Properties dialog box.

Compressed files occupy less disk space than files that are not compressed. All Windows-based applications can read from and write to compressed files. When an application needs to open a compressed file, the operating system decompresses the file, the file is available to the application, and the operating system recompresses the file when it is saved.

TECH TIP

Compression causes your computer to slow down

When **compression** is enabled, the computer's performance can degrade because when a compressed file is opened, the file must be uncompressed, and then it must be recompressed to be saved or closed. Degradation can also occur if a compressed file is transferred across a network because the file must be uncompressed before it is transferred.

TECH TIP

What happens when a compressed file is moved or copied?

Moving or copying a compressed file or folder can alter the compression. When you move a compressed file or folder, the file or folder remains compressed. When you copy a compressed file or folder, it is compressed only if the destination folder (where you are moving it to) is already compressed.

When a file or folder is encrypted with EFS (Encrypting File System), only authorized users can view or change the file. Administrators designated as recovery agents have the ability to recover encrypted files when necessary.

Windows Home does not support file encryption, but the Pro, Enterprise, and Education editions do. The `cipher` command can be used at the command prompt to decrypt, modify, and copy an encrypted file obtained from another computer or server that does support it. Compressed files, system files, and read-only files cannot be encrypted.

Figure 14.18 provides more information on archiving, compression, and encryption.

TECH TIP

Copying and moving

To copy a file or folder, use the *Copy* and *Paste* functions in File Explorer. To move a file or folder, use the *Cut* and *Paste* functions.

Introduction to Windows Settings

The Settings app is the main application for configuring Windows settings to meet an individual user's needs or to satisfy broader network requirements. You can access Settings from the Pinned section of the Start menu (the gear icon), or you can right-click the Start button and select Settings. Settings is organized into categories to assist in navigation to specific options. Figure 14.21 shows the System page in the Settings app in Windows 11.

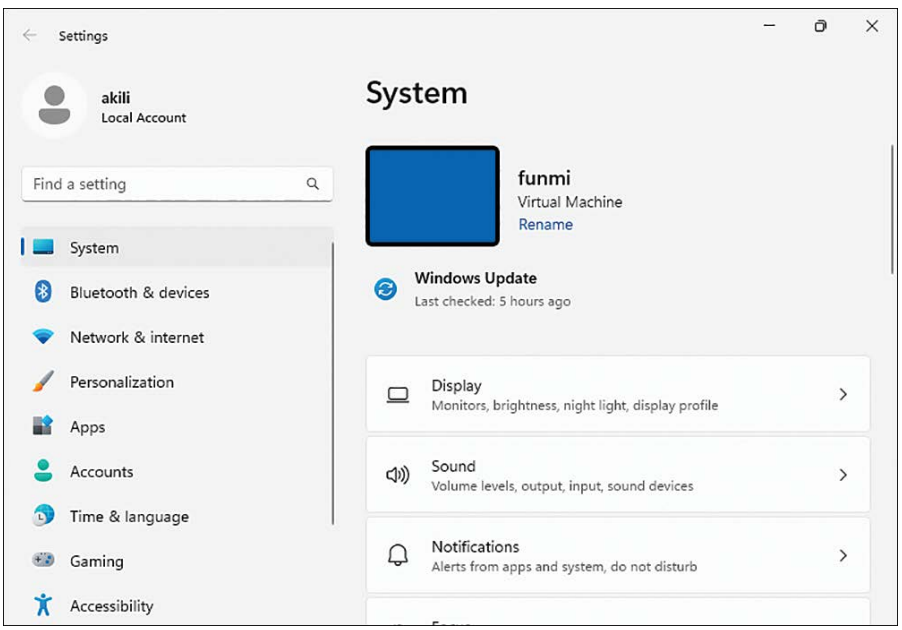


FIGURE 14.21 Windows 11 Settings app System page

Table 14.6 shows all the Windows 11 Settings categories and subcategories. Settings utilities are similar between Windows 10 and Windows 11.

TABLE 14.6 Common Windows 10/11 Settings categories

Settings category	Subcategory	
Home (not available on devices managed by organizations)	> Recommended Settings > Bluetooth devices > Personalize your device	> Cloud storage > Microsoft 365
System	> Display > Sound > Notifications > Focus > Power > Storage > Nearby sharing > Multitasking > For developers	> Activation > Troubleshoot > Recovery > Projecting to this PC > Remote Desktop > Clipboard > System components > Optional features > About

Settings category	Subcategory	
Bluetooth and devices	> Recent device list > View more devices > Bluetooth > Printers & scanners	> Cameras > Mouse > Pen & Windows Ink > AutoPlay > USB
Network & internet	> Wi-Fi > VPN > Mobile hotspot > Airplane mode	> Proxy > Dial-up > Advanced network settings
Personalization	> Background > Colors > Themes > Dynamic Lighting > Lock screen	> Text input > Start > Taskbar > Fonts > Device usage
Apps	> Installed apps > Advanced app settings > Default apps > Offline maps	> Apps for websites > Video playback > Startup
Accounts	> Microsoft storage > Microsoft 365 > PC Game Pass > Your info > Sign-in options > Linked devices > Email & accounts	> Family > Windows backup > Other users > Access work or school > Passkeys > Related settings
Time & language	> Date & time > Language & region	> Typing > Speech
Gaming	> Game Bar > Captures > Game Mode	
Accessibility	> Text size > Visual effects > Mouse pointer and touch > Text cursor > Magnifier > Color filters > Contrast themes	> Narrator > Audio > Captions > Speech > Keyboard > Mouse > Eye control
Privacy & security	> Windows Security > Windows permissions > App permissions	
Windows Updates	> Check for updates > More options > Related support links	

The **Control Panel** is the predecessor to Settings. Since Windows 10, Microsoft has been incrementally moving Control Panel utilities to the Settings app. For example, clicking *System* in Control Panel now takes you to *Settings* > *System* > *About*. The Settings app is designed to be more intuitive and easier to use than Control Panel, especially for new users. Microsoft encourages users to use Settings as their primary tool for configuring Windows, although some advanced options are still only available in Control Panel utilities. To open a Control Panel, search for "control" in the Search box and then select the Control Panel search result. Figure 14.22 shows the Windows 11 Control Panel.

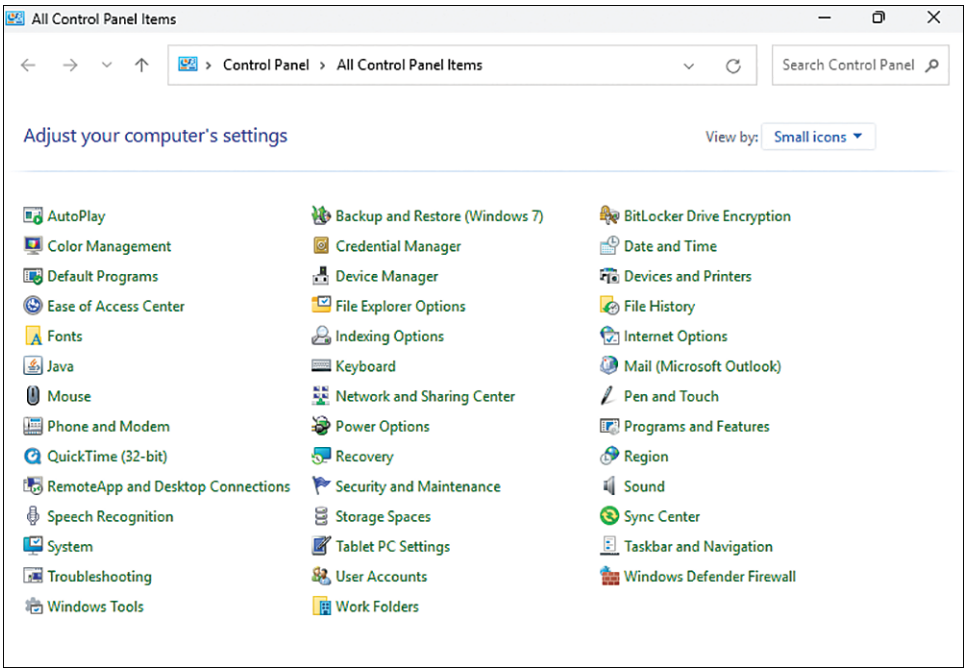


FIGURE 14.22 Windows 11 Control Panel utilities (small icons view)

Determining the Windows Version

The *Settings* > *System* > *About* option allows you to determine the amount of RAM, the processor, and the Windows version installed on the computer. The version of an operating system is important when troubleshooting because it is one more piece of information that can be placed within a search parameter. You can also access the *About* option by using *File Explorer* > right-click or tap and briefly hold *This PC* > *Properties*. Figure 14.23 shows the *About* option in Windows 11.

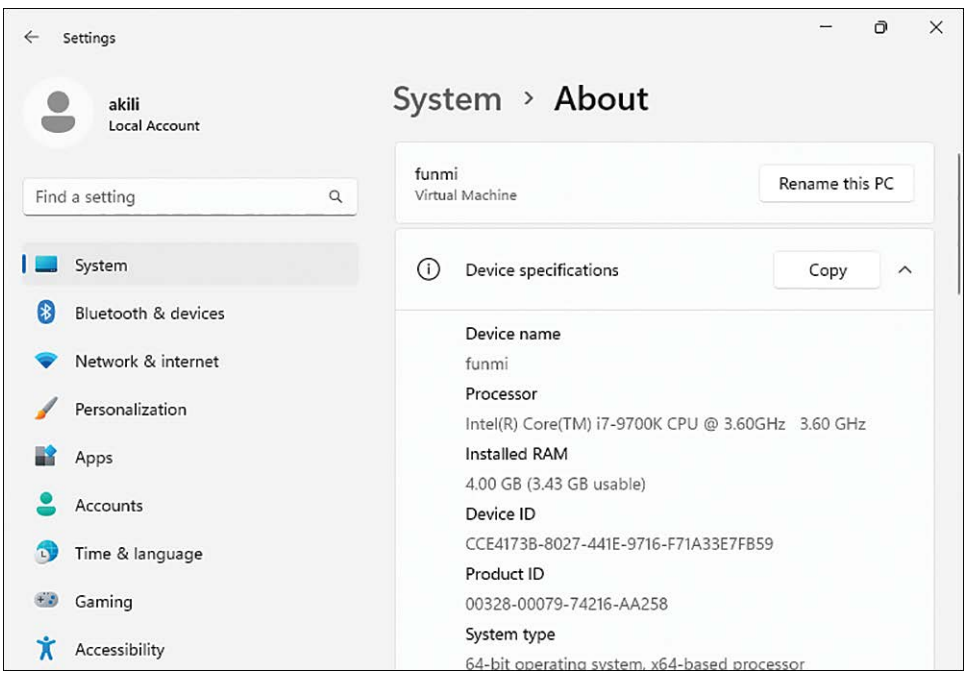


FIGURE 14.23 Windows 11 Settings > System > About option

Windows Registry

Every software or hardware configuration is stored in a database called the **registry**. The registry contains such things as folder and file property settings, port configuration, application preferences, and user profiles. A **user profile** contains specific configuration settings such as which applications the user can access, desktop settings, and each user's network configuration. The profile is different for each person who has an account on the computer. The registry loads into RAM (memory) during the boot process. When in memory, the registry is updated continuously based on changes made to software, hardware, and user preferences.

The registry is divided into five subtrees, sometimes called *branches* or *hives*: `Hkey_Local_Machine`, `Hkey_Users`, `Hkey_Current_User`, `Hkey_Current_Config`, and `Hkey_Classes_Root`. Each of these subtrees has keys and subkeys that contain values related to hardware and software settings. Table 14.7 lists and describes the five subtrees. The registry can contain other subtrees that are user defined or system defined, depending on what hardware or software is installed on the computer.

TABLE 14.7 Windows registry subtrees

Registry subtree	Description
`Hkey_Local_Machine`	Holds global hardware configuration. Includes a list of hardware components installed in the computer, the software drivers that handle each component, and the settings for each device. This information is not user specific.
`Hkey_Users`	Keeps track of individual users and their preferences.
`Hkey_Current_User`	Holds a specific user's configuration, such as software settings, how the desktop appears, and what folders the user has created.
`Hkey_Current_Config`	Holds information about the hardware profile that is used when the computer first boots.
`Hkey_Classes_Root`	Holds file associations and file links. The information held here is what allows the correct application to start when you double-click a filename in File Explorer or This PC (provided that the file extension is registered).

Editing the Windows Registry

Most changes to Windows are made through the various options in Settings, but sometimes the only way to make a change is to edit the registry directly. Depending on the Windows operating system used, one or two registry editors are available from a command prompt: `regedit.exe` (64-bit version) and `regedt32.exe` (32-bit version). Figure 14.24 shows the Windows 11 `regedit.exe` utility.

Notice in Figure 14.24 that subtrees such as `Hkey_Classes_Root` and `Hkey_Current_User` appear in the left window. If you click the chevron (looks like a "greater than" sign) beside a subtree, keys appear under it. After several layers, when you click a folder in the left window (a key), values appear in the right window. These values are the ones you must sometimes change in order to fix a problem.

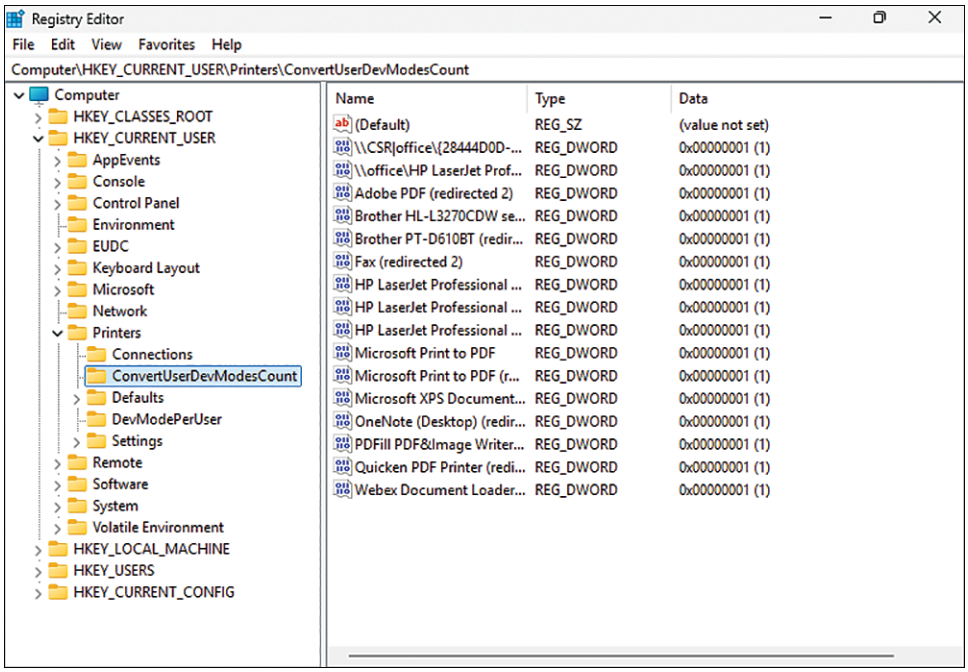


FIGURE 14.24 `regedit.exe` in Windows 11

TECH TIP

Make a backup of the registry before you change it

Before making any change to the registry, you should make a backup of it. This way, if the change does not work properly, it can be easily reversed.

For 64-bit versions of Windows, the registry is divided into 32- and 64-bit keys. The 32-bit keys are kept in a subfolder called `WOW6432Node`, located within the `Hkey_Local_Machine\Software` subfolder. On some machines, the vendor may have a subfolder under `Software`; it is this vendor subfolder that contains the `WOW6432Node` folder. Just do a search for `WOW6432Node` to find it. 64-bit software keys are kept directly in the `Hkey_Local_Machine\Software` subfolder.

Backing Up Data

Having a data **backup**, or a copy of that data, is important. A data backup can be restored if the original data is overwritten, lost, stolen, or damaged. Windows 10 and Windows 11 come with a backup solution called Windows Backup, which allows a user to back up their files, preferences, and installed apps to their OneDrive account. The data backup can be accessed on another computer after the user signs in to their OneDrive account. After the initial backup, future changes to the system can be continuously synced with OneDrive. Windows Backup is available at *Settings* > *Accounts* > *Windows backup*. Several other cloud storage solutions are available to back up data in a remote location, including Google Drive, iCloud, Dropbox, SugarSync, and iDrive.

The *Backup and Restore (Windows 7)* Control Panel applet allows a user to back up specific folders or entire disks to an internal hard drive, an external hard drive, or a network drive. The tool can also create a **system image**, which is a copy of the drive required for Windows to run, as well as all the files and applications on the drive.

The *File History* Control Panel applet also uses local media (such as an internal hard drive, a USB hard drive, or a network storage location) to save versions of files that are contained in libraries, contacts, desktop files, and favorites. To include files on a disk or on a folder that is not in one of these locations, you can right-click the disk or folder in File Explorer and then select *Include in library.* From there, you can choose an existing library, or you can create a new one.

WinRE

Windows Recovery Environment (**WinRE**) can be used when Windows 11 does not boot and when other tools and startup options do not solve a problem. WinRE has a list of recovery options, including a command prompt–only environment. WinRE provides access to tools to troubleshoot the operating system when the tools within the operating system cannot be accessed or don't work properly. You can access WinRE via *Settings* > *System* > *Recovery* > *Advanced startup* section > *Restart now*. WinRE is also available via the original Windows installation disc (select *Repair Your Computer* and use the *System Recovery Options*). Some of the recovery methods in the next section require WinRE. Chapter 16, "Advanced Windows," discusses WinRE in detail, including other methods to access the environment.

Recovering the Windows OS

When a computer starts performing poorly and the operating system tools do not seem to help, you may need to repair, replace (**reload OS**), or uninstall/reinstall the operating system. A virus could also cause extensive damage, resulting in the need for an operating system recovery. How you do this depends on what measures have been taken (or have not been taken, in some cases) and the type of environment in which the computer is located (home or work). The list below describes some of the common methods used to recover an operating system:

- Before you start using your computer, create a Windows **recovery drive**. The recovery drive contains the operating system, but it does not contain any user files, applications, or settings. In Windows 11, search for `recovery` and select *Create a Recovery Drive*. The system recovery drive can boot the system when you don't have an original Windows disc or flash drive, and then you can restore the computer from a previously saved system image.

  Some computer manufacturers provide a recovery disc to restore the computer to the original "as sold" condition. This recovery disc contains the vendor's customizations, including any software that was preinstalled on the computer. Keep in mind that with this option, the applications that the user installed and the user's data will not be restored.

- System imaging software creates a complete copy of a hard drive, including the operating system, configuration settings, installed applications, and user files. Such software can be purchased directly from a wide variety of vendors, and it is often included with external hard drives. The imaging software Backup and Restore (Windows 7) is included in Windows 11. When you boot the system from the Windows 11 original disc or flash drive, you can select the *System Image Recovery* option and then select the storage device that contains the system image created with Backup and Restore (Windows 7).

  Users should periodically create a system image, especially after installing new programs. Then, if the computer starts performing poorly, all or part of the image can be recovered. The image can be saved to one of several locations:

  - Optical discs
  - Flash drive
  - Hard drive (Do not store on the same hard drive as the operating system.)

  - Network location (Keep in mind that you must get to the network location to restore the image. This might be difficult if the computer is not working.)
- A restore point is a snapshot of the operating system settings but not the operating system itself. Furthermore, it does not contain applications or user files. If the operating system starts misbehaving, the settings can be restored to the previous values from *System Properties* > *System Protection* > *System Restore* or from *Windows Recovery Environment* > *Troubleshoot* > *Advanced Options* > *System Restore*. Chapter 16 discusses *System Restore* in detail, including how to enable the tool and how to create a restore point.
- A recovery partition (sometimes called the HPA, or host protected area) is a section of the hard drive created by the computer manufacturer and commonly accessed through *Windows Recovery Environment* > *Troubleshoot* > *Advanced Options* > *Reset this PC* in Windows 11. The *Reset this PC* tool reinstalls the operating system and removes all apps and settings. It gives the option of keeping the user's personal files.
- You can use network-based imaging services such as Windows Deployment Services. Companies frequently use a standard image stored on a server to install the initial operating system on a new computer or replace the operating system on a failing computer. The image can contain settings, files, folders, and applications that are pre-selected by the company. User-specific files and settings can be recovered via other means.
- Note that using an old operating system disc or image (such as the original one) is risky because it does not contain the latest service packs. You should download **service packs** and copy them to an optical disc, hard drive, flash drive, or network drive *before* reinstalling the operating system. Research the service pack requirements prior to installation. After the operating system is reinstalled, apply the service packs before accessing any other data on a network.

As you can see, most of these methods recover only the operating system. Table 14.8, which summarizes the items that can be restored via the various methods, can be used to develop a combined strategy that protects the user's applications, preferences, and files as well.

TABLE 14.8 Windows backup/recovery methods and items they restore

	Items Recovered					
Backup/recovery method	**Entire disk**	**OS**	**Pre-installed applications**	**User's preferences**	**User's files**	**User's applications**
Network-based imaging services	No	Yes	Yes	No	No	No
Recovery drive	No	Yes	No	No	No	No
System imaging software	Yes	Yes	Yes	Yes	Yes	Yes
System restore point	No	No	No	Yes	No	No
Windows backup	No	No	No	Yes	Yes	Yes

SOFT SKILLS: STAYING CURRENT

Technicians must stay current in the rapidly changing field of computers. Benefits of staying current include understanding and being able to troubleshoot the latest technologies, being able to recommend upgrades or solutions to customers, saving time (and therefore money) on troubleshooting, and being considered for promotion. Technicians use a variety of methods to stay current, including the following:

- Subscribe to a magazine or an online magazine.
- Subscribe to a news list that gives you email updates.
- Join or attend association meetings.
- Register for and attend a seminar.
- Attend an online webinar.
- Take a class.
- Read books.
- Talk to your department peers and supervisor.

Staying current on technology in the past few years has been challenging for all, but the rapidly changing environment is what draws many to the field.

Chapter Summary

- An operating system performs all the basic tasks to communicate between hardware and software, to communicate between hardware and users, and to facilitate communication between software and users.
- A user communicates with an operating system through a command prompt or a GUI interface.
- The most popular desktop/laptop operating systems are Microsoft's Windows, Apple's macOS, Chrome OS, and Linux. The most popular mobile operating systems are Android, iOS, and iPadOS.
- Operating systems use either 32-bit or 64-bit architecture. A 64-bit system has more processing power than a 32-bit system.
- When replacing or upgrading an operating system, end-of-life (EOL) concerns must be addressed, including security threats, software incompatibility, compliance issues, performance, reliability, and cost.
- Computers are considered compatible if software that runs on one model can run on all other models in that family, even if this results in performance issues. Forward and backward compatibility as well as extensibility are considerations.
- While specifics may differ, all Windows 10 and 11 editions offer the user a desktop or Start screen that consists of icons, the taskbar, shortcuts, and the Recycle Bin.
- Right-click a shortcut or tile and select *Properties* to see the path to the original file.
- File Explorer is commonly used to manipulate files and folders. Windows libraries (Documents, Music, Pictures, and Videos) are commonly part of the path to stored documents and subfolders.
- Deleted files are stored on a hard drive in a folder called Recycle Bin. The Recycle Bin must be emptied to release hard drive space. This is relevant only to files stored on hard drives.
- Windows supports encryption and compression. When a file or folder is encrypted with EFS, only authorized users can view or change the file. Encrypted files that are moved or

copied on NTFS volumes remain encrypted. Compressed files, system files, and read-only files cannot be encrypted. When a file or folder is encrypted with EFS, only authorized users can view or change the file.

> Technicians commonly use the Control Panel to modify how the hardware, software, and operating system environment functions and appears. The *System* section of the Control Panel can be used to determine the Windows version and to modify the registry. Other uses for the important Control Panel utilities are covered in Chapter 16.

> The Windows registry is a database of everything within the Windows environment. Configuring Control Panel settings modifies the registry. Use `regedit.exe` or `regedt32.exe` to manually modify the registry.

> You can recover the operating system in various ways: using a Windows or manufacturer-provided recovery disc, a recovery partition, a previously created image, a reload of the operating system and service packs, and the System Restore tool.

> Technicians must stay current in the IT field to move up or maintain their current job status. Methods used to stay current include joining associations, reading relevant magazines, taking classes, reading current books, and interacting with peers.

A+ CERTIFICATION EXAM TIPS

- ✓ Know the differences between 32-bit and 64-bit architecture.
- ✓ Know the types and uses of operating systems, including Microsoft Windows, Apples macOS, and Linux. Know the different types of licenses for operating systems: open, personal, corporate, and enterprise.
- ✓ Know the types and uses of cell phone/tablet operating systems, including Android, iOS, and Chrome OS.
- ✓ Describe the differences and similarities among Windows 10 and 11 editions, including Home, Pro, Pro for Workstations, Pro Education, and N versions. Pay special attention to the availability of security, networking, and remote access features.
- ✓ Describe how the following are addressed in a corporate environment and on a personal computer: workgroup vs. domain access, Remote Desktop Connection, BitLocker, BitLocker To Go, and EFS.
- ✓ Be able to set various folder options, including hiding file extensions, and viewing hidden files, view options, and the options available through the *Folder Options* Control Panel > *View* tab.

Key Terms

32-bit architecture, 64-bit architecture, Active Directory (AD), Android OS, Apple Macintosh OS, Apply button, attribute, backup, backward compatibility, BitLocker, BitLocker To Go, boot process, Chrome OS, command-line interface, compatibility, compression, context menu, Control Panel, desktop, Documents, domain access, Edge, EFS, end-of-life (EOL), extensible software, extension, file, file type, filename, folder, forward compatibility, GUI, icon, indexing, iOS, iPadOS, library, Linux, macOS, Microsoft Windows, Network, notification area, open source, operating system, path, proprietary system, RAM limitation, recovery drive, Recycle Bin, `regedit.exe`, `regedt32.exe`, registry, reload OS, security threat, service pack, settings, shortcut, software incompatibility, Start button, Start screen, subdirectory, subfolder, system image, Task View, taskbar, This PC, Tiles, upward compatibility, user profile, window, Windows 10, Windows 11, WinRE

Review Questions

1. The key piece of software that provides an interface between the user and installed hardware is a(n) _____.

   [application | time machine | operating system | registry]

2. What is the core of a computer's operating system?

   [CPU | kernel | RAM | commands]

3. [T | F] Programs and drivers written for 64-bit systems can always run on 32-bit systems.

4. Two methods of interacting with the operating system are through a(n) ____ or a(n) _____. (Choose two.)

   [tunnel | GUI | OS cache | command line | core | workstation]

5. Name two features specifically needed on a mobile device's operating system.

   _____

   _____

6. Name three possible consequences associated with using software that has reached its end-of-life (EOL).

   _____

   _____

7. Name two potential problems associated with updating an operating system.

   _____

   _____

8. [T | F] Backward compatibility means that a new application can still process data from older software.

9. [T | F] A folder and a directory are the same thing.

10. A file's name consists of a filename and a(n) _____.

    [path | size | folder | extension]

11. Describe how to show a file's extension if it is not displayed in File Explorer. Choose one version of Windows (10 or 11).

    _____

    _____

    _____

    _____

12. In the following path, which identify the subfolder(s).

    `C:\Users\Cheryl\NewFiles\review.docx`

    _____

13. [T | F] Deleted files stored on a hard drive can be recovered from the Recycle Bin.

14. What Windows option can access various icons or links that can configure the computer?

    [Control Panel | Time Machine | registry | Quick Launch]

15. What is the maximum memory that can be recognized by a Windows 32-bit operating system?

    [1 GB | 2 GB | 4 GB | 16 GB | 64 GB]

16. In the filename `Opsys_Quiz 4.docx`, what is the extension?

    [`Opsys_Quiz 4.docx` | `Opsys` | `4` | `docx`]

17. A user is working in Microsoft Word. She saves the document called `Ltr1.docx` to a folder called `Homedocs`. The `Homedocs` folder is a subfolder of the `Work` folder located on the `D:` hard drive volume. Write the complete path for the `Ltr1.docx` file.

_____

18. [T | F] File and folder compression can degrade computer performance.
19. List three methods that can be used to recover an operating system.

_____

_____

20. What is the name of a registry editor?

    [`registry` | `regedit.exe` | `edit` | `nano`]
21. Describe two methods commonly used to recover an operating system.

_____

_____

_____

22. List two methods that you think you will use to stay current in the IT field.

_____

_____

Exercises

Exercise 14.1 Windows Settings Categories

Objective: To recognize common Windows Settings categories

Procedure: Match the task to the appropriate Windows Settings category. Note that a category can be used more than once.

Control Panel category:

a. System	**e.** Accounts
b Network and internet	**f.** Personalization
c. Bluetooth & devices	**g.** Time & language
d. Apps	**h.** Accessibility

Task:

_____ **1.** Enable screen reading for any text shown on the screen.

_____ **2.** Determine whether a computer is on a domain or in a workgroup.

_____ **3.** Access Device Manager.

_____ **4.** Customize the Start button menu.

_____ **5.** Configure whether hidden files are shown.

_____ **6.** Configure power saving options.

_____ **7.** Back up the system.

_____ **8.** Configure the home page for the default Microsoft browser.

_____ **9.** Set the proper time zone.

_____ **10.** Change the Windows password for a home computer.

_____ **11.** Verify that a camera appears as being attached.

_____ **12.** Configure the Ethernet NIC for DHCP.

Exercise 14.2 Common Operating Systems

Objective: To differentiate between operating systems used today

Procedure: Match each OS to a description. Note that an operating system can be used more than once.

Operating system:

a. Windows

b. Linux

c. macOS

d. iOS

e. iPadOS

f. Android

Description:

_____ **1.** Microsoft's operating system

_____ **2.** The operating system most commonly used for office computers

_____ **3.** An open-source operating system

_____ **4.** A mobile operating system

_____ **5.** Apple's operating system for iPhones

_____ **6.** A proprietary operating system

_____ **7.** Torvalds worked on the kernel

_____ **8.** Runs on Apple desktop computers

_____ **9.** Has the Control Panel

_____ **10.** Has worldwide volunteer development efforts

_____ **11.** Operating system developed by Google

_____ **12.** iPad's operating system

Exercise 14.3 CLI vs GUI

Objective: To differentiate between when a command-line environment is used and when a graphical user interface is used

Procedure: Determine whether each action is using a (a) GUI environment or (b) command-line interface. Note that an option can be used more than once. You may have to do some research on your own to determine the answers.

Action:

_____ **1.** Working with File Explorer

_____ **2.** Typing `dir` to see a list of files

_____ **3.** Making a batch file

_____ **4.** Working with File Explorer

_____ **5.** Setting a configuration using the System Control Panel utility

_____ **6.** Using `regedit.exe`

_____ **7.** Creating a script

_____ **8.** Trying to fix a system on which the Windows operating system does not load

Activities

Internet Discovery

Objective: Access the internet to obtain specific information regarding a computer or its associated parts

Parts: A computer with internet access

Procedure: Complete the following procedure and answer the accompanying questions.

1. Locate an internet site that has a tutorial for Windows 11 troubleshooting or usage. Document the site and one thing you learned from the tutorial.

   _____

   _____

2. Find an online article on the differences between Windows 11 Pro and Windows 11 Enterprise editions. List the name of the article, three important differences, and the URL.

   _____

   _____

3. Locate a website that demonstrates how to edit the Windows registry for any edition of the Windows 11 operating system. Describe the registry hack using at least one complete sentence. State whether you would deploy such a hack and explain why or why not.

   _____

   _____

4. Locate a website that describes three things to do if Windows 11 (any edition) will not boot. Briefly describe the three things and document the URL.

   _____

   _____

   _____

   _____

   _____

   _____

Soft Skills

Objective: To enhance and fine-tune a technician's ability to listen, communicate in both written and oral form, and support people who use computers in a professional manner

Activities:

1. Access a monitor's *Setup* menu. Make a list of some of the settings that would be helpful to a computer user. Include in your list a description of each function. Document this in such a way that it could be given to users as a how-to guide.
2. On an index card, write a paragraph describing a problem and how a technician might look at the problem differently than a user would. Exchange cards with one classmate and discuss your paragraphs. Comment on anything you find unclear in your classmate's paragraph, listen to suggestions from your classmate, and rewrite your paragraph, if necessary.

Critical Thinking Skills

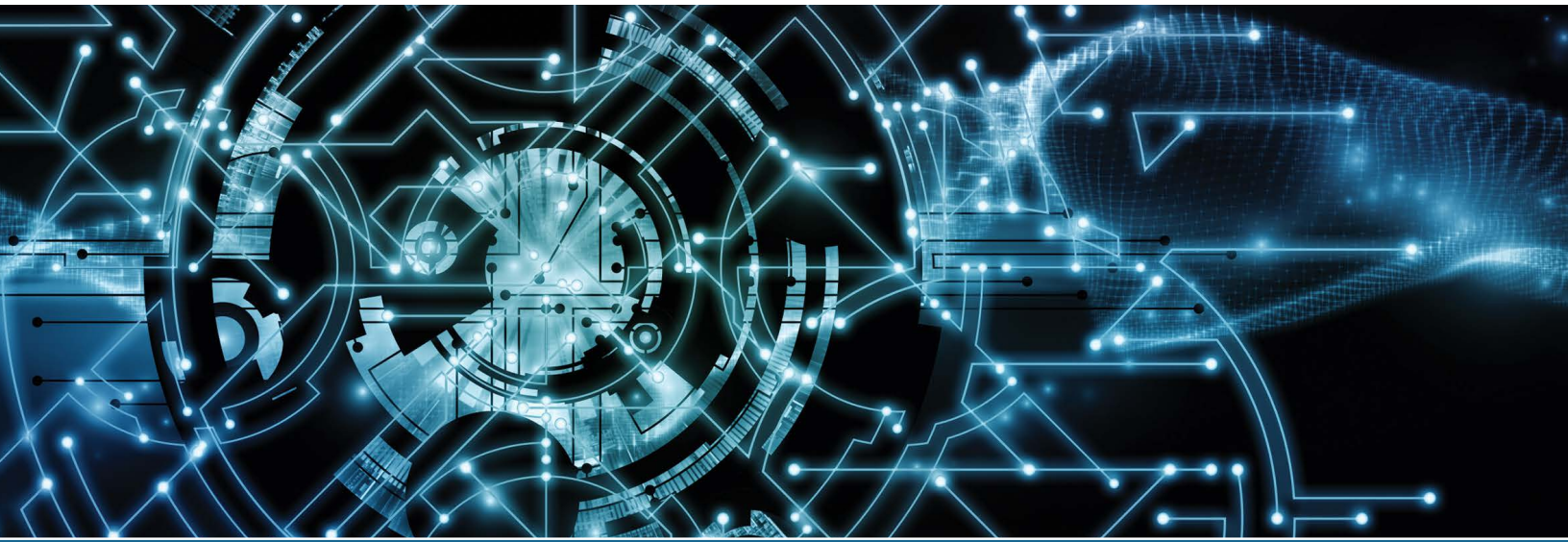
Objective: To enhance and fine-tune a technician's ability to listen, communicate in both written and oral form, and support people who use computers in a professional manner

Activities:

1. In a group environment, on a piece of paper or an index card, list two topics you would like to hear about if you were to attend a local association such as a PC users' group meeting. Share your ideas with your group. Consolidate ideas and present five of the best ideas to the class.
2. In a group environment, select one of the five ideas presented in Activity 1 to research. Every group member should present something about a new technology to the rest of the class. The class will vote on the best-presented topic and the most interesting topic.
3. On an index card, document a question that several students have asked the teacher about how to do a particular task. Exchange cards with a classmate. Correct each other's grammar, punctuation, and capitalization. When you have your original card back, exchange cards with a different classmate and perform the same task. Rewrite your index card based on the recommendations of your classmates. Keep in mind that all their suggestions are just that—suggestions. You do not have to accept any of them. A complaint in the industry is that technicians do not write well. Practice helps with this issue.

This page intentionally left blank

15 Introduction to Scripting



In this chapter you will learn:

- How to work from a command prompt
- How to use specific commands
- The basics of shell scripting and scripting in Python, JavaScript, VBScript, batch files, and PowerShell
- The most common use cases for scripting
- How to avoid unintended consequences with scripting
- How to define environment variables and distinguish between system and user environment variables
- How to view and modify environment variables
- The building blocks of scripting: variables and data types
- The three programming constructs used to build all scripts: sequence, selection, and repetition
- How to use relational and logical operators in a script
- The pros and cons of each of six scripting languages
- Changing your perspective when troubleshooting

CompTIA Exam Objectives

- ✓ 1202-1.4 Given a scenario, use Microsoft Windows operating system features and tools.
- ✓ 1202-1.5 Given a scenario, use the appropriate Microsoft command-line tools.
- ✓ 1202-4.8 Explain the basics of scripting.

Scripting Overview

While the Windows operating system offers technicians many dialog boxes that provide assistance in fixing problems and accessing various settings, sometimes technicians need to do things that cannot be done through a dialog box. In such cases, the command prompt environment can be used. From a command prompt, a technician can type commands that are specific to the operating system and to the required task. However, to do this, you must know the commands that a computer understands as well as the appropriate syntax to get commands to work. *Syntax* refers to the rules that specify the correct sequence of symbols or words. For example, in English, the phrase "table on This is book the" is meaningless, but the same words in a different order make perfect sense: "This book is on the table." In English, the correct syntax must be followed for the words to be understandable. Similarly, typing `/p dir w/` at a command prompt will give you an error, but typing `dir /p /w` will display the list of files and folders in a directory one page at a time in wide format. The same characters and symbols must be used in correct order—with correct syntax—for a command at the command prompt to work.

Network technicians can use scripts to automate tasks, to save time when completing complex procedures, to ensure consistency in tasks that must be executed over multiple servers in different locations, and to reduce human error. A **script** is a program that is designed to do a specific task. You can often find scripts written by others that you can use, and you can also create your own. Scripts are created in a text editor and are run from the command-line prompt. In this chapter you will learn the basics of scripting in some of the many scripting languages, including PowerShell, VBScript, Python, JavaScript, as well as shell scripts for Unix and batch files for Windows.

Command Prompt Overview

Even with the advent of newer and more powerful operating systems, a technician still must enter basic commands into computers while troubleshooting, when deploying computers, and when updating computers in a corporate environment. Functioning from a command prompt is a skill that a technician still must use sometimes.

To access a command prompt with **standard privileges** (user privileges) while logged into Windows, access the *Search* function > type `command` or `cmd` > press [Enter].

An elevated command prompt allows you to run commands that require a user account with **administrative privileges**. To access an elevated command prompt, access the *Search* function > type `command` or `cmd` > right-click the *Command Prompt* option > select *Run as administrator*. Figure 15.1 shows an elevated command prompt. If a message within the command prompt window indicates that the requested operation requires elevation, close the standard command prompt and open an elevated command prompt.

You can close the command prompt window in several ways:

- Use the *Close* button in the upper-right corner.
- In Windows 10, click or tap the little black box in the upper-left corner > select a *Close* option.
- In Windows 11, right-click the little black box in the upper-left corner > select a *Close* option.
- Type the `exit` command.

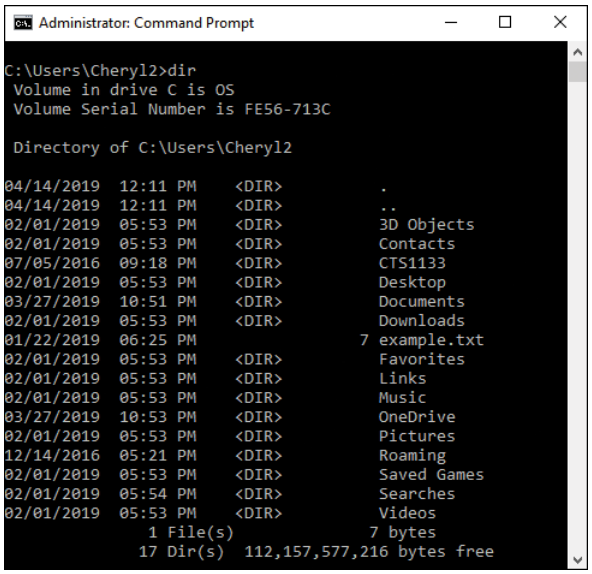


FIGURE 15.1 Windows command prompt

Command Prompt Basics

Drive letters are assigned to storage drives when a computer boots. For example, the first hard drive partition gets the drive letter `C:`. The colon is part of the device drive letter. The devices detected by the operating system can use and be assigned drive letters `A:` through `Z:`.

Commands can be typed using a keyboard or entered through a touch screen. All communication using typed commands begins at the **command prompt**, also called simply a *prompt*. A command prompt might look like `F:\>` or `C:\>` or `C:\Windows>`. Notice the backslash (\) that follows the colon and the greater-than sign (>) at the end of the prompt. Capitalization of commands does not matter when using a Windows command prompt (this is not true for all operating systems), but commands *must* be typed in a specific format and in a specific order. Practicing using commands from a command prompt is the best way to become proficient with this skill.

Computer files can be grouped like chapters in a book. On a computer, a file grouping is called a folder (in a GUI environment) or a **directory** (in a command prompt environment). The starting point for all directories is the **root directory**. Other directories can be created or accessed from the root directory. The root directory can hold only a limited number of files, and the quantity depends on the file system used. The root directory of a drive is shown as a backslash after the driver letter: `C:\` or `E:\`. In the command prompt environment, when you are at the root directory, a greater-than sign (>) follows the letter and the backslash: `C:\>` and `E:\>`.

Each filename or directory name within a directory must be unique, but multiple directories can contain the same object name. For example, assume that the `Cheryl.txt` file exists in the `Documents` directory. A different `Cheryl.txt` file can exist in the `Lotus` or `Utility` directory. In fact, the file called `Cheryl.txt` that contains the same information could also exist in all three folders. However, a second `Cheryl.txt` file cannot exist in the same folder (directory).

Files are kept in the root directory or within directories (folders) that reside within the root directory. A **subdirectory** can be created beneath another directory. For example, if a directory (folder) has the name `Book`, the subdirectories titled `Chap1`, `Chap2`, `Chap3`, and so on can be created below the `Book` directory. Since the word *root* identifies the start of the directory structure, many people describe the directory structure as a tree. Figure 15.2 illustrates this concept.

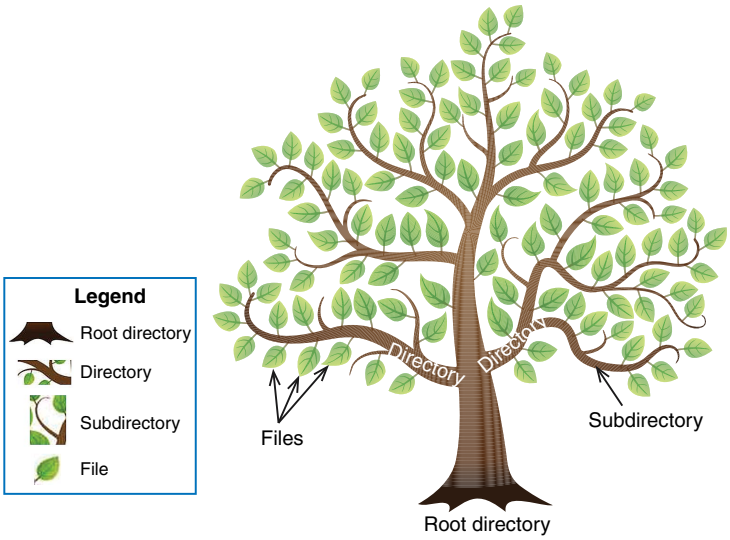


FIGURE 15.2 Tree structure concepts

Sometimes it's easier to see the file structure concepts from File Explorer than from the command prompt. Figure 15.3 shows the `Documents` directory of the `C:` drive for the user `Cheryl`. Notice that the path is listed at the top of the File Explorer window because that option has been enabled through the *Folder Options* window. Also notice the address bar, which shows part of the path (`<< Users > Cheryl > Documents`). The File Explorer window shows several types of items:

- **Folders:** `2015BookWin8Laptop`, `Custom Office Templates`, `Outlook Files`, and `SugarSync Shared Folders`
- **Files (unhidden):** `Chap1.docx`, `kara's books.docx`, `My class books.docx`, and `Spectre.docx`
- **Shortcuts to the other folders:** `My Music`, `My Pictures`, and `My Videos`
- **Hidden file:** `desktop.ini` (Settings in the *Folder Options* section of the Control Panel allow you to determine whether the filename extensions and hidden files are seen.)

Now let's view this same structure from the command prompt by using the `tree` command (see Figure 15.4).

Notice that Figure 15.4 actually shows two commands. The first one, `tree`, asks the computer to display a "tree," or the structure starting from `C:\Users\Cheryl\Documents`. The second `tree` command uses `/f` at the end, causing files to be shown.

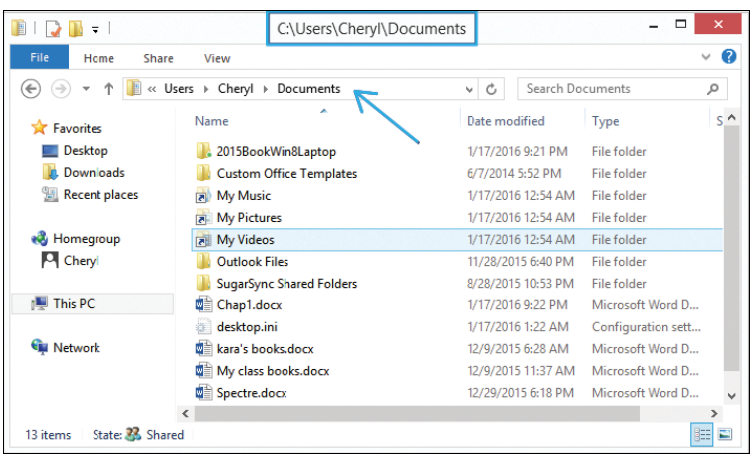


FIGURE 15.3 Sample file structure in File Explorer

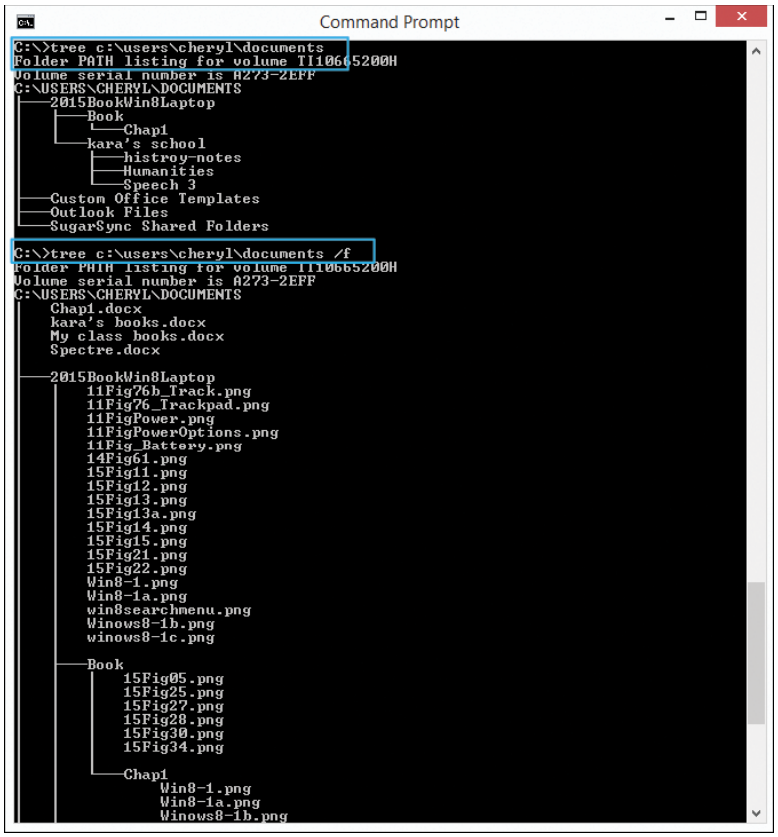


FIGURE 15.4 Tree structure from a command prompt

Every folder along the path is shown, starting with the root directory, `C:\`. The subfolders are separated by backslashes (\). The path tells you exactly how to reach the file. When something goes wrong in a particular application and Microsoft or another vendor posts a solution online, the solution commonly shows the complete path. It is the only way to clearly tell you where to find, put, delete, or replace a file.

Moving Around from a Command Prompt

One of the most important skills when working in the command-line environment is to be able to move around within that environment. The `cd`, `md`, `rd`, and `dir` commands are the four most popular commands used in the Windows environment to move around the directory structure. Let's take a look at each one.

The `cd` Command

The most frequently used command for moving around in the tree structure is `cd` (for *change directory*). The `cd` command enables you to "change" to a different directory so that the prompt changes to where you are within the directory (tree) structure. For example, say you have a flash drive with a `Test1` directory that has subdirectories called `Sub1`, `Sub2`, and `Sub3`, as shown in Figure 15.5.

Assume that the prompt is at `F:\>`. To get to this prompt, you simply type the drive letter of your flash drive and press [Enter]. To move to the *Sub2* subdirectory (subfolder), type the command `cd Test1\Sub2`. The prompt changes to `F:\Test1\Sub2>`. Another command that does the same thing is `cd F:\Test1\Sub2`. The difference is that with the second command, the full path is given. The `F:\` is not required because the prompt is already at the root directory of `F:` (`F:\>`).

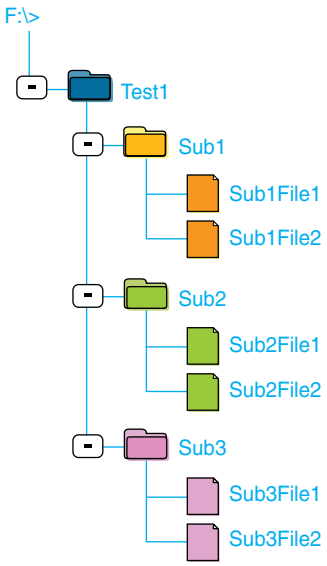


FIGURE 15.5 Sample tree structure

Two subdirectories are said to be at the same level if they reside immediately within the same directory. To move to a subdirectory that is on the same level as the `Sub2` directory (such as `Sub1` or `Sub3`), several commands are possible. For example, you can type `cd..` (you must type the two periods after `cd`) to move back one level and then type `cd Sub1`. Notice that there is no backslash (`\`) between `cd` and `Sub1`. You omit the backslash only when moving one level down the tree structure, as shown in Figure 15.5.

To get to the `Sub1` subfolder from the `F:\Test1>` prompt, you can type `cd Sub1`, `cd \Test1\Sub1`, or `cd F:\Test1\Sub1`. However, if the prompt shows that you are at the root directory (`F:\>`), you must use either `cd F:\Test1\Sub1` or `cd Test1\Sub1`. The command `cd Sub1` does not operate properly because of the current location within the tree structure (as shown by the prompt `F:\>`). Practice is the best way to get good at moving around from a prompt.

The `dir` Command

The `dir` command lists all the files and directories from wherever you are at the prompt. Figure 15.6 shows the `dir` command issued from the root directory of a flash drive (`G:\>`).

Notice in Figure 15.6 that directories are shown with `<DIR>`. There is nothing listed in that column to identify a file. Directories in the root directory of `G:` are `Chip`, `Dale`, `cotlong`, `Photos`, and `classes`. Files in the root directory of the same flash drive are `Dinfo.txt` and `Ninfo.txt`.

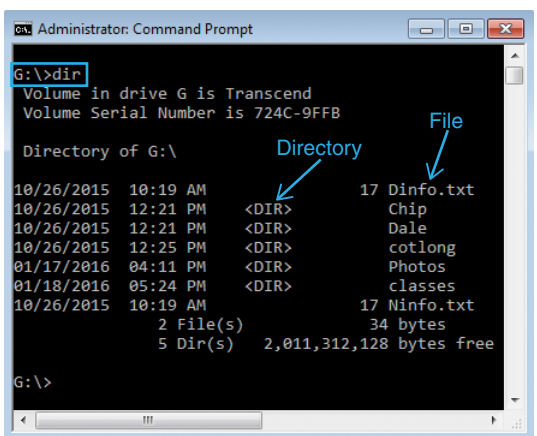


FIGURE 15.6 `dir` command from a prompt

When you use the `dir` command on a hard drive, you might notice directories for `.` and `..` (see Figure 15.7). The `.` and `..` are used with commands like `cd` to move around the directory structure. A single period (`.`) represents the current directory. Two periods (`..`) represents the parent directory (the directory that contains the current directory). That is why the command `cd..` moves you back one directory structure. In Figure 15.7, if someone were to type the command `cd..` from the `C:\Users\Cheryl2>` prompt, the prompt would change to `C:\Users>`. If the `cd \` command were issued from the `C:\Users\Cheryl2>` prompt, the prompt would change to `C:\`.

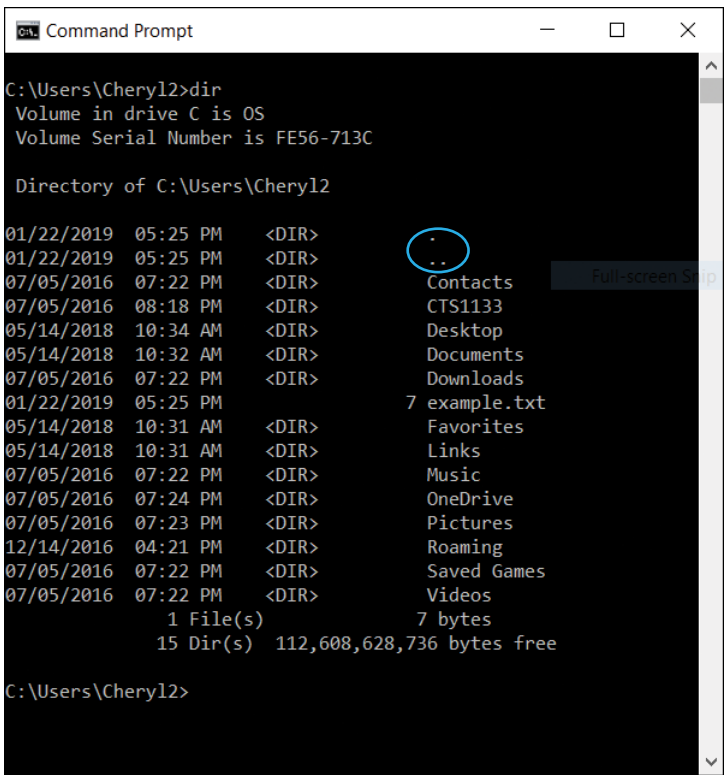


FIGURE 15.7 `dir` command showing the `.` and `..` directories

Each command commonly has one or more optional **command switches** that change how the command operates. To determine what switches are available with any command, enter the following:

command_name /?

where *command_name* is any one command. For example, the command `dir /?` shows all the possible options that can be used with the `dir` command (see Figure 15.8). Notice how `dir` is the *command_name* and how `/?` is used to get help for the `dir` command. In the third and fourth lines from the top of Figure 15.8, you can see that there is an order to the listing of the switches. Normally, they are shown in alphabetical order.

Notice in the output shown in Figure 15.8 that there are optional parameters such as `drive:` and `path`. Each optional parameter and switch has brackets (`[ ]`) around it. A switch is preceded by a `/` (forward slash). There is no space between the `/` and the optional switch. For example, with the `dir` command, you could simply type `dir` and press [Enter]. You could also type `dir /p` to display the output one page at a time or `dir /w` to display the output in a wide format. You can use multiple switches together, such as `dir /p /w`. While it is not necessary to put a space after each switch, you must put a space between a command and a switch. The command `dir /p/w` works exactly the same way as `dir /p /w`.

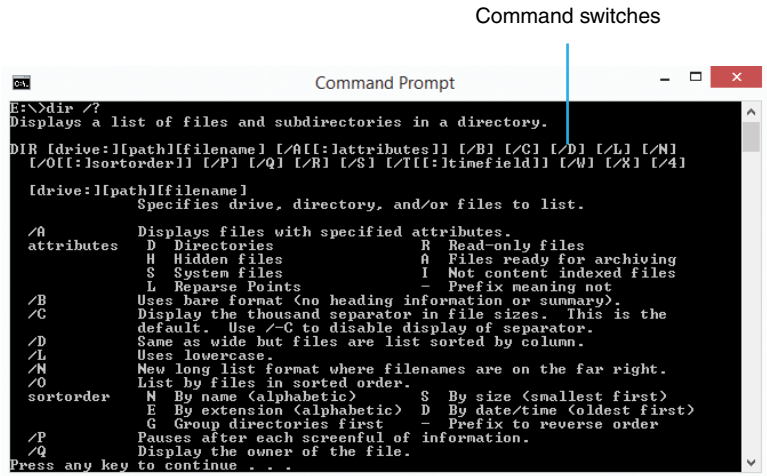


FIGURE 15.8 `dir` command switches

Figure 15.8 shows that each command switch is described below the options. Also notice in this figure that when some commands list more than one page of output, you get a `Press any key to continue...` message at the bottom of the screen.

TECH TIP

Make a command output one page at a time

If a command outputs more than one page at a time, you can use the `| more` option after the command and make it show only one page at a time. Note that the | (pipe) symbol is created by holding down the ⇧Shift key and pressing the | key located directly above the ↵Enter key.

TECH TIP

Limited commands in WinRE

Not all command parameters or switches shown may be available when using the Windows Recovery Environment (WinRE), which is discussed in Chapter 14, "Introduction to Operating Systems" and Chapter 16, "Advanced Windows." WinRE has a limited number of commands. Type the `help` command to see a list of available commands.

The `md` and `rd` Commands

Sometimes as an IT staff person, you might be required to create or remove a directory from a command prompt to install software or as part of a repair. The `md` and `rd` commands are used to perform these tasks.

The `md` or `mkdir` Command

The `md` or `mkdir` (for *make directory*) command makes a directory from wherever you are in the directory structure (as shown from the prompt on the screen). Consider the following command: `F:\>md CTS1133`. The `CTS1133` directory would be made in the root directory of the `F:` drive. Now consider the following set of commands:

```
F:\>
F:\>cd Classes
```

```
F:\Classes>md CTS1133
F:\Classes>
```

What is different about this set of commands is that the `cd Classes` command was issued before the `md CTS1133` command was issued. The `cd Classes` command changed the prompt to `F:\Classes>` (the `Classes` folder on the `F:` drive). Then the `md CTS1133` command was issued, thus creating a subdirectory called `CTS1133` under the `Classes` folder. An alternative way of doing the same thing is to issue the full path with the command, as shown here:

```
F:\>md \Classes\CTS1133
```

or:

```
F:\>md F:\Classes\CTS1133
```

Note that the second command would work from any prompt, including the `C:\>` prompt, because it includes the full path as part of the command.

TECH TIP

The full path works from everywhere

If you begin learning the command prompt by typing the full path no matter where you are in the directory structure, you will be better prepared for working in this environment.

The `rd` or `rmdir` Command

The `rd` or `rmdir` command removes a directory or subdirectory. If the directory you try to remove has files in it, this message will appear: `The directory is not empty`. You can only use these commands on empty directories. The examples here show how to remove a directory from the different prompts:

```
F:\>rd F:\Classes\cts1133
F:\>rd \Classes\cts1133
F:\Classes>rd cts1133
```

Note that the first example here works from any prompt, even if it is another drive letter.

Two Useful Commands: `del` and `type`

When problems occur while a technician is working at a command prompt, two tasks that might need to be accomplished are to delete a particular file or to read the contents of a text file, such as a log file. The `del` and `type` commands can be used to do this, so let's look at them next.

The `del` Command

Sometimes a file has to be deleted as part of the repair process. The `del` (for *delete*) command removes a file. It cannot be used to remove a directory. That is an important point to remember. To issue the command, simply type the `del` command followed by the name of the file you want to delete. You must be in the correct directory (as shown by the prompt) to use this method, and you must include the file extension as part of the filename. In the commands shown below, the user is in the root directory of the `F:` drive and wants to delete a file named `homework1.docx` that is

in the `cts1133` subdirectory of the `Classes` directory. Before issuing the `del` command, the user must change directories to be in the `cts1133` subdirectory:

```
F:\>
F:\>cd F:\Classes\cts1133
F:\Classes\CTS1133>del homework1.docx
F:\Classes\CTS1133>
```

An alternative method can work from any prompt. You can type the full path of the file to be deleted, as shown here:

```
F:\>del F:\Classes\cts1133\homework1.docx
```

The `type` Command

Another useful command is the `type` command, which displays text (`.txt`) or batch (`.bat`) files on the screen. `Readme.txt` files are often included with software applications and utilities. The `type` command allows you to view these files from the command-line interface; however, most of the time, these files occupy more than one screen. So, using the `| more` parameter after the `type` command permits viewing the file one screen at a time. After viewing each screen, press the Spacebar key to see the next screenful of content. For example, `type readme.txt | more` allows you to view the text file called `readme.txt` one page at a time.

Copying Files

The commands `copy`, `xcopy`, and `robocopy` can copy files. The `copy` command is used to make a duplicate of a file. The `xcopy` command is used to copy and back up files and directories. The `robocopy` command enables you to copy a directory, its contents, all its subdirectories (and their subdirectories), and each attribute.

We focus on the `copy` command because it is the command you can use in any environment. The `copy` command is an internal command, meaning it cannot be found as an executable file on the hard drive or Windows disc. The operating system can always find an internal command no matter where the command is located in the directory structure. The `copy` command enables you to copy a file to a different disk, copy a file from one directory to another, copy a group of files using wildcards, or rename a file as it is being copied. A **wildcard** replaces one or more characters. `?` and `*` are examples of wildcards; `?` represents a single character, and `*` represents any number of characters.

The `copy` command has three parts, separated by spaces:

- The command itself (`copy` or `xcopy`)
- The source (the file being copied)
- The destination (where the file is being copied to)

In technical documentation, this would be shown using the syntax `copy` *`source destination`*. In this syntax, *`destination`* is optional if the file is being copied into the current directory. For example, if you are working from the `E:\>` command prompt and you're copying a file called `Document.txt` from the hard drive's root directory, the command could be `copy C:\Document.txt`. The destination is omitted because the file automatically copies to the current drive and directory (which is `E:\`). The same function can be accomplished by typing `copy C:\Document.txt E:\`, which has all three parts: the `copy` command, the *`source`* (a file called `Document.txt` located on the hard drive or `C:\Document.txt`), and the *`destination`* (the root directory of `E:`, or `E:\`).

The command requires all three parts if the destination is *not* the current drive and directory. For example, consider the situation of being at the `C:\>` command prompt. To copy the `format.com` file from the hard drive (the `System32` subfolder of the `Windows` folder) to a disk shown as `E:`, enter the following command:

```
C:\> copy C:\Windows\System32\format.com E:\
```

Note that the `copy` command is first. Then you specify the drive, location, and name of the file being copied: `C:\Windows\System32\format.com`. Finally, you include the destination, `E:\`, or the root directory of the flash drive where the file is to be placed. If the current directory is the `C:\Windows\System32` hard drive directory, then the source path does not have to be typed. Instead, the command would look like the following:

```
C:\Windows\System32>copy format.com E:\
```

The backslash (`\`) after the `E:` is not necessary if the flash drive does not have directories (folders). The `copy` command does not need the entire path in front of the command because `copy` is an internal command.

TECH TIP

Getting the command straight in your head

Before using any command, consider the following questions:

- What command do you want to issue?
- Where in the directory structure are you currently working? Look at the prompt to determine where you are.
- If you are copying a file or moving a file, what is the name of the file, and what is the full path to it? This is the source file.
- If you are copying a file or moving a file, in what directory does the file need to be placed? This is the destination file.

The `attrib` Command

The `attrib` command sets, removes, or shows the attribute(s) of a file or a directory. Attributes change how a file or directory is displayed on the screen or what can be done with the file or directory. Possible attributes are read-only, archive, system, and hidden:

- The read-only attribute protects files so that they cannot be accidentally changed.
- The archive attribute marks files that have changed since they were last backed up by a backup program.
- The system attribute designates a file as a system file; by default, files with this attribute do not appear in directory listings.
- The hidden attribute allows you to hide files and directories.

Set each attribute using the `attrib` command with the `+x` switch, where *x* is `r` for read-only, `a` for archive, `h` for hidden, or `s` for system. Remove each attribute by using the `-r`, `-s`, `-h`, or `-a` switch with the `attrib` command. One `attrib` command can set more than one attribute on a file or directory. For example, to make the `Cheryl.txt` file hidden and read-only, type `attrib +r +h Cheryl.txt`.

Why Learn Commands?

With many Windows problems, some solutions involve working from a command prompt until a Windows update fixes the problem. Other problems simply involve using a command from a prompt. Commands can also be used in a script. A *script* is a group of commands in a file that together automate a particular task. For example, say that you want to write a script to stop a computer print spooler and delete all spooled files that are in the queue to be printed. The following commands could be written in Notepad and saved to a file called `DeletePrint.cmd`:

```
net stop spooler
del %systemroot%\system32\spool\printers\*.shd
del %systemroot%\system32\spool\printers\*.spl
net start spooler
```

After the file is saved, you could copy it to a hard drive, type `DeletePrint`, and press [Enter] to execute the four commands.

TECH TIP

Start your favorite tools by using a command

For example, at a command prompt or in the *Search* textbox, type `mmc devmgmt.msc` to start Device Manager. Note that you can access the Microsoft Management Console and still get to Device Manager by simply typing `mmc`.

PowerShell

In today's computing environment, a technician frequently has to do things to hundreds, or even thousands, of computers. Scripts and Windows PowerShell can help. Windows PowerShell is a tool that helps technicians and network administrators automate support functions through the use of scripts and snippets. PowerShell is included in both Windows 10 and Windows 11. Every command that you can type from a command window (and a lot more) can be executed from within PowerShell.

TECH TIP

How do you open PowerShell?

There are several ways to access PowerShell in Windows 10 and Windows 11.

- Type `powershell` in the search window, right-click on the resulting Windows PowerShell app, and selecting *Run as Administrator*.
- In File Explorer, type `powershell` in the address bar and press [Enter].
- In Task Manager, select *File* menu > *Run new task* and then type `powershell` and click *OK*.
- If you're already in the command prompt, type `powershell` and press [Enter]. The letters `PS` will be added to the front of the prompt to indicate that you're in PowerShell instead of the command prompt.

Other Commands You Should Look Over

Some commonly used commands are discussed in other chapters of this book or are beyond the basics of learning how to function from a command prompt. When you understand how to work from a prompt, you can execute any command fairly easily. In the "Command Format" section that follows, commands shown as key terms (boldfaced and purple) are in objectives for the certification exam.

The following are the most common and, perhaps, most important commands that you should be familiar with as a technician:

> [*command name*] /?
> Current directory and parent directory (. and ..)
> Drive navigation inputs (C: or D: or x:)
> bootrec
> cd
> chkdsk
> command
> copy
> defrag
> del
> dir
> diskpart
> dism
> dxdiag
> exit
> expand
> explorer
> format
> gpresult
> gpupdate
> help
> hostname
> ipconfig
> md/mkdir
> mmc
> msconfig
> msinfo32
> mstsc
> nbtstat
> net
> net use
> net user
> netdom
> netstat
> notepad
> nslookup
> pathping
> ping
> rd/rmdir

```
> regedit
> regsvr32
> robocopy
> services.msc
> sfc
> shutdown
> taskkill
> tasklist
> tracert
> xcopy
> whoami
> winver
```

Command Format

When Windows does not boot, a technician must work from a command prompt. Some of the most frequently used commands are outlined in detail on the following pages. Items enclosed by brackets (`[ ]`) are optional. Items in italics are command-specific values that you must enter. When the items are separated by a | (called a pipe, or bar), one of the items must be typed.

The following pages provide a command reference. Some of these commands are used elsewhere in this chapter or in others. This list is by no means comprehensive. You can expect to see the key terms (boldfaced and purple) on the CompTIA A+ Core 2 Exam (V15) certification exam. Visit the microsoft.com website for a complete list of Windows commands; the Microsoft Learn website (https://learn.microsoft.com) is a good asset.

TECH TIP

How to get help when working from a prompt

To get help while working from a prompt, type `help` *`command_name`* or type *`command_name`* `/?`. For example, to get help for the `attrib` command, type `help attrib` or `attrib /?`.

[*command name*] /?

The **[*command name*] /?** command displays help information about a specific command.

Syntax: [*command_name*] /?

Explanation: [*command_name*] is the name of the command for which you want help.

Example: `dir /?`

Notes: If you do not specify the *command_name* parameter when using this command, no commands are listed, and an error appears, saying that `/?` is not recognized as an internal or external command, operable program, or batch file.

Current Directory and Parent Directory (. and ..)

The special folder . refers to the current folder in which a file or folder is located. The special folder .. refers to the parent of the current folder. These special folders can be used when specifying filepaths.

Example: `C:\Windows>cd..`

This command changes the prompt to `C:\` because `C:\` is the parent of the `Windows` folder.

Drive Navigation Inputs (`C:` or `D:` or `x:`)

To change the active drive, type the new drive letter and a colon and then press Enter.

Example: `C:\Windows>D:`

This command changes the active drive to D:. The new prompt will be `D:\`.

`attrib`

The `attrib` command controls the attributes for a file or folder.

Syntax: `attrib [+|-h] [+|-r] [+|-a]`
`[+|-s] [drive:] [path] filename [/S] [/D]`

Explanation: `+` adds an attribute.

`-` takes away an attribute.

`h` is the hidden attribute.

`r` is the read-only attribute.

`a` is the archive file attribute.

`s` is the system attribute.

`[drive:]` is the drive where the file is located.

`[path]` is the directory/subdirectory where the file is located.

`filename` is the name of the file.

`[/S]` includes subfolders.

`[/D]` includes folders.

Example: `attrib +h c:\cheryl.bat`

This command sets the hidden attribute for a file called `Cheryl.bat` located on the hard drive.

Notes: The `dir` command (typed without any switches) is used to see what attributes are currently set. You may set more than one attribute at a time.

`bcdedit`

The `bcdedit` command is used at the command prompt or in the System Recovery environment to modify and control settings contained in the BCD (boot configuration data) store, which controls how the operating system boots.

Syntax: `bcdedit [/createstore] [/copy] [/create] [/delete] [/deletevalue] [/set] [/enum] [/bootsequence] [/default] [/displayorder] [/timeout]`

Explanation: `[/createstore]` creates a new empty BCD store that is not a system store.

`[/copy]` makes a copy of a specific boot entry contained in the BCD store.

`[/create]` creates a new entry in the BCD store.

`[/delete]` deletes an element from a specific entry in the BCD store.

`[/deletevalue]` deletes a specific element from a boot entry.

`[/set]` sets a specific entry's option value.

`[/enum]` lists entries in a store.

`[/bootsequence]` specifies a display order that is used one time only. The next time the computer boots, the original display order is shown.

`[/default]` selects the entry used by the boot manager when the timeout expires.

`[/displayorder]` specifies a display order that is used each time the computer boots.

`[/timeout]` specifies, in seconds, the amount of time before the boot manager boots using the default entry.

Example: `bcdedit / set Default debug on`

This command troubleshoots a new operating system installation. It is the default option that appears in the Boot Manager menu.

Notes: Use the `bcdedit /? types` command to see a list of data types. Use the `bcd /? formats` command to see a list of valid data formats. To get detailed information on any of the options, type `bcdedit /?` followed by the option. For example, to see information on how to export the BCD, type `bcd /? export`.

bootrec

The `bootrec` command is used in the System Recovery environment to repair and recover from hard drive problems.

Syntax: `bootrec [/FixMbr] [/FixBoot] [/ScanOs] [/RebuildBcd]`

Explanation: `[/FixMbr]` repairs the hard drive MBR (master boot record) by copying a new MBR to the system partition. The existing partition table is not altered.

`[/FixBoot]` repairs the hard drive boot sector if it has been corrupted and replaces it with a higher boot sector or if an earlier version of Windows has been installed after Windows 10 or Windows 11.

`[/ScanOs]` looks for compatible operating system installations that do not currently appear on the Boot Manager list.

`[/RebuildBcd]` scans all disks for operating systems compatible with Windows Vista or higher and optionally rebuilds the BCD store. The BCD store provides structured storage for boot settings, which is especially helpful in multiple-operating-system environments. Discovered operating systems can be added to the BCD store.

Example: `bootrec /fixmbr`

This command could be used if a virus has destroyed the MBR.

Notes: If you receive an `Element not Found` error when using the `bootrec` command, the hard drive partition might not be active. Use the Windows Recovery Environment command prompt and the `diskpart` command to select the drive disk number. (If you only have one and it has one partition, it will be the command `select disk 0`, as an example.) Then type the

command `active`. Exit the `diskpart` utility and reboot the computer. Re-access the System Recovery environment and rerun the `bootrec` command.

If the system needs a new BCD and rebuilding it does not help, you can export the existing BCD and then delete the current BCD. To export the BCD, type `bcdedit /export x:\folder` (where `x:\folder` is the location where you want the BCD store exported). Then run of these commands, one at a time `c:`, `cd boot`, `attrib bcd -s -h -r`, `ren c:\boot\bcd bcd.old`, and `bootrec /RebuildBcd` to create a backup copy of the BCD store, make it so it is not hidden and can be deleted, and then rebuild it.

NOTE Use of the terms *master* and *slave* is ONLY in association with the official terminology used in industry specifications and standards and in no way diminishes Pearson's commitment to promoting diversity, equity, and inclusion and challenging, countering, and/or combating bias and stereotyping in the global population of the learners we serve.

cd

The **cd** command is used to navigate through the directory structure.

Syntax: `cd [drive:] [path] [..]`

Explanation: `[drive:]` specifies the drive (if it is different from the current drive) to which you want to change.

`[path]` is the directory/subdirectory to reach the folder.

`[..]` changes to the parent directory (moves you back one directory in the tree structure).

Examples: `C:\Windows>cd..`

`C:\>`

This command moves you from the `Windows` directory (folder) to the parent directory, which is the root directory (`C:\`).

`C:\>cd \Windows`

This command moves you from the root directory to the `Windows` directory on the `C:` drive.

chkdsk

The **chkdsk** command checks a disk for physical problems, lost clusters, cross-linked files, and directory errors. If necessary, the `chkdsk` command repairs the disk, marks bad sectors, recovers information, and displays the status of the disk.

Syntax: `chkdsk [drive:] [/r] [/f] [/i] [/b]`

Explanation: `[drive:]` specifies the drive to check.

`[/r]` locates bad sectors and attempts recovery of a sector's information.

`[/f]` fixes drive errors.

`[/i]` checks only index entries on NTFS volumes.

`[/b]` re-evaluates bad clusters.

Example: `chkdsk d:`

This command checks the disk structure on the `D:` drive.

Notes: This command can be used without switches. For the `chkdsk` command to work, the file `Autochk.exe` must be loaded in the `System32` folder or used with the correct path and run from the Windows drive. If one or more files are open on the drive being checked, `chkdsk` prompts you to schedule the disk to be checked the next time the computer is restarted.

chkntfs

The `chkntfs` command can display whether a particular disk volume is scheduled for automatic disk checking the next time the computer is started. It can also be used to modify automatic disk checking.

Syntax: `chkntfs volume: [/D] [/X] [/C]`

Explanation: `volume:` specifies the drive volume to display or modify.

`[/D]` places the computer back to default behavior. (All drives are checked at boot time, and `chkdsk` is run on those that are dirty.)

`[/X]` excludes a particular volume from the default boot-time check.

`[/C]` schedules a drive to be checked at boot time. The `chkdsk` command will be run if the drive is dirty.

Example: `chkntfs c:`

This command displays whether the drive is dirty or scheduled to be checked on the next computer reboot.

cipher

The `cipher` command displays or alters file or folder encryption.

Syntax: `cipher [/e] [/d] [/f] [/q] [/k] [/u] [/n] [path]`

Explanation: `[/e]` encrypts the specified folder, including files that are added to the folder in the future.

`[/d]` decrypts the specified folder.

`[/f]` forces encryption or decryption because, by default, files that have already been encrypted or decrypted are skipped.

`[/q]` reports essential information about the encryption or decryption.

`[/k]` creates a new file encryption key.

`[/u]` updates the encryption key to the current one for all encrypted files if the keys have been changed. `/u` works only with the `/n` option.

`[/n]` finds all encrypted files. It prevents keys from being updated. It is used only with `/u`.

`[path]` is a pattern, file, or folder.

Examples: `cipher /e Book\Chap1`

This command encrypts a subfolder called `Chap1` that is located in a folder called `Book`.

`cipher /e /s:Book`

This command encrypts all subfolders in the folder called `Book`.

`cipher Book`

This command displays whether the `Book` folder is encrypted.

`cipher Book\Chap 1\*`

This command displays whether any files in the `Chap1` subfolder of the `Book` folder are encrypted.

Notes: Multiple parameters are separated with spaces. Read-only files and folders cannot be encrypted.

cls

The `cls` command clears the screen of any previously typed commands.

Example: `C:\Windows>cls`

command

The `command` command is executed from the *Search* textbox by simply typing `command` and pressing [Enter]. A command prompt window appears. Type `exit` to close the window.

Syntax: `command`

Explanation: When `command` is entered, a command prompt window opens.

copy

The `copy` command is used to copy one or more files to the specified destination.

Syntax: `copy [/a] [/y] [/-y] source [destination]`

Explanation: `[/a]` indicates an ASCII text file.

`[/y]` suppresses the prompt to overwrite an existing file.

`[/-y]` prompts to overwrite an existing file.

`source` is the file that you want to copy, and it includes the drive letter and the path if it is different from your current location.

`[`*`destination`*`]` is the location in which you want to put the file and includes the drive letter and path if it is different from your current location.

Example: `copy c:\cheryl.bat f:\`

This command copies a file called `cheryl.bat` that is located in the root directory of the hard drive to a flash drive.

Notes: You do not have to include a target if the file is going to the current location specified by the command prompt. If a file already exists, you will be asked whether to overwrite the file. Compressed files that are copied from the Windows media are automatically uncompressed to the hard drive as they are copied.

defrag

The `defrag` command is used to locate and reorder files so that they are contiguous (not fragmented) to improve system performance.

Syntax: `defrag [drive:] [/a] [/c] [/x]`

Explanation: `[drive:]` is the drive letter where the files are located.

`[/a]` analyzes the drive volume specified.

`[/c]` includes all volumes.

`[/x]` consolidates free space on the specified volume.

Example: `defrag c: d: /a`

This command defragments the `C:` and `D:` drives and analyzes them.

Notes: Multiple switches can be used, as long as spaces appear between them. Multiple drive letters (volumes) can be used with a single command.

del

The `del` command is used to delete a file.

Syntax: `del name [/p] [/f] [/s]`

Explanation: `name` is the file or directory (folder) that you want to delete, and it includes the drive letter and the path if it is different from your current location.

`[/p]` prompts for confirmation before deleting.

`[/f]` forces read-only files to be deleted.

`[/s]` deletes files from all subdirectories.

Example: `C:\Windows>del c:\cheryl.bat`

This command deletes a file called `cheryl.bat` that is located in the `Windows` directory on the hard drive.

dir

The **`dir`** command list files and folders and their attributes.

Syntax: `dir [drive:] [path] [filename] [/a:attribute] [/o] [/p] [/s] [/w]`

Explanation: `[drive:]` is the letter of the drive where the files are located.

`[path]` is the directory/subdirectory to reach the folder.

`[filename]` is the name of a specific file.

`[/a:attribute]` displays files that have specific attributes, where the attributes are `D`, `R`, `H`, `A`, and `S`. `D` is for directories; `R` is for read-only, `H` is for hidden, `A` is for archive, and `S` is for system files.

`[/o]` displays the listing in sorted order. Options you can use after the `o` are `E`, `D`, `G`, `N`, and `S`. `E` is by alphabetic file extension; `D` is by date and time, with the oldest listing shown first; `G` shows the directories listed first; `N` displays by alphabetic name; and `S` displays by size, from smallest to largest.

`[/p]` displays the information one page at a time.

`[/s]` includes subdirectories in the listing.

`[/w]` shows the listing in wide format.

Example: `dir c:\windows`

This command shows all the files and folders (and their associated attributes) for the `windows` folder that is located on the `C:` drive.

disable

The `disable` command disables a system service or hardware driver.

Syntax: `disable name`

Explanation: `name` is the name of the service or driver that you want to disable.

Notes: You can use the `listsvc` command to show all services and drivers that are available to be disabled. Make sure that you write down the previous *START_TYPE* before you disable the service in case you need to restart the service.

diskpart

The **`diskpart`** command is used to manage and manipulate the hard drive partitions.

Syntax: `diskpart [/add|/delete] [devicename] [drivename | partitionname] [size]`

Explanation: `[/add |/delete]` creates a new partition or deletes an existing partition.

`[devicename]` is the name given to the device when creating a new partition, such as `\Device\HardDisk0`.

`[drivename]` is the drive letter used when deleting an existing partition, such as `E:`.

`[partitionname]` is the name used when deleting an existing partition and can be used instead of the `drivename` option. An example of a `partitionname` is `Device\HardDisk0\Partition2`.

`[size]` is used when creating a new partition and is the size of the partition, in megabytes.

Notes: You can just type the `diskpart` command without any options, and a user interface appears that helps when managing hard drive partitions.

dism

The `dism` command is a Windows utility, Deployment Image Servicing and Management, which can be used to repair and prepare Windows images.

Syntax: `dism /Online /Cleanup-Image /[/CheckHealth] [/ScanHealth] [/RestoreHealth]`

Explanation: `[/CheckHealth]` checks whether the image has been flagged as corrupted and whether the corruption can be repaired.

`[/ScanHealth]` scans the image for component store corruption and records that corruption to the log file.

`[/RestoreHealth]` scans the image for component store corruption, performs repair operations automatically, and records that corruption to the log file.

dxdiag

The `dxdiag` command is used to perform DirectX diagnostics.

Syntax: `dxdiag [/dontskip] [whql:on|/whql:off] [/64bit target] [/x filename] [/t filename]`

Explanation: `[/dontskip]` causes all diagnostics to be performed, even if a previous crash in `dxdiag` has occurred.

`[/whql:on]` checks for WHQL (Windows Hardware Quality Labs, now known as Windows Hardware Certification) digital signatures.

`[/whql:off]` prevents checking for WHQL digital signatures.

`[/64bit target]` uses 64-bit DirectX diagnostics.

`[/x filename]` saves XML information to the specified filename and quits.

`[/t filename]` saves TXT information to the specified filename and quits.

Notes: When DirectX diagnostics checks for WHQL digital signatures, the internet may be used.

enable

The `enable` command is used to enable a system service or hardware driver.

Syntax: `enable name [start-type]`

Explanation: `name` is the name of the service or driver that you want to disable.

`[start-type]` is used when you want the service or driver scheduled to begin. Valid options are as follows:

`SERVICE_BOOT_START`

`SERVICE_SYSTEM_START`

`SERVICE_AUTO_START`

`SERVICE_DEMAND_START`

Example: `enable DHCP client service_auto_start`

Notes: You can use the `listsvc` command to show all services and drivers that are available to be enabled. Make sure that you write down the previous value before you enable the service in case you need to restart the old service or driver.

exit

The `exit` command closes the command prompt environment window.

Example: `C:\Windows>exit`

expand

The `expand` command uncompresses a file from a CAB (short for *cabinet*) file. A CAB file holds multiple files or drivers that are compressed into a single file. Technicians sometimes copy the CAB files onto the local hard drive so that when hardware and/or software is installed, removed, or reinstalled, the application disc does not have to be inserted.

Syntax: `expand [-i] source [destination]`

Explanation: `[-i]` renames files but ignores the directory structure.

`source` is the name of the file, including the path that you want to uncompress.

`[destination]` is the path where you want to place the uncompressed file.

Example: `expand d:\i386\access.cp_ c:\windows\system32\access.cpl`

This command expands (uncompresses) the compressed file `Access.cp_` and puts it into the `C:\Windows\System32` folder with the name `Access.cpl`.

Notes: You cannot use wildcard characters with the *`source`* parameter.

explorer

The `explorer` command is used to start File Explorer from a command prompt.

Syntax: `explorer`

format

The **`format`** command is used to format a disk or drive and can format it for a particular file system.

Syntax: `format [driveletter:] [/q] [/fs:filesystem] [/v:label] [/x]`

Explanation: `[driveletter:]` is the drive letter for the disk or hard drive volume that you want to format.

`[/q]` is the parameter used if you want to perform a quick format.

`[/fs:filesystem]` is the parameter used if you want to specify a file system. Valid values are FAT, FAT32, exFAT, and NTFS.

`[/v:label]` must have `/v:` as part of the command, followed by the name of the volume assigned.

`[/x]` dismounts the volume first, if necessary.

Example: `format c: /fs:ntfs`

Notes: If no `/fs:filesystem` parameter is specified, the NTFS file system is used. FAT is FAT16. FAT16 hard drive volumes cannot be more than 4 GB in size.

gpresult

The **`gpresult`** command is used to display Group Policy settings. Group Policy determines how a computer is configured for both system and user (or a group of users) settings.

Syntax: `gpresult [/s computer] [/u domain\user] [/p password] [/user target_user] [ /r] [/v] [/z]`

Explanation: `[/s computer]` is an optional parameter that specifies a remote computer using the computer name or IP address; otherwise, the local computer is selected by default.

`[/u domain\user]` specifies authentication for the remote computer.

`[/p password]` specifies a password for the remote computer user ID.

`[/user target_user]` specifies to display a user's Group Policy settings.

`[/v]` outputs data in verbose mode.

`[/z]` displays all available data about the Group Policy.

Examples: `gpresult /r`

`gpresult /s 10.3.207.15 /u pearson\cschmidt /p G#t0Ut0fH3R3`

gpupdate

The **gpupdate** command refreshes local- and Active Directory–based Group Policy settings.

Syntax: `gpupdate [/target:{computer | user}] [/force] [/wait:value] [/logoff] [/boot]`

Explanation: `[/target:{computer | user}]` is an optional parameter used to specify whether either the *computer* settings or the current *user* settings are used. When neither is specified, both *computer* and *user* settings are processed.

`[/force]` reapplies all settings.

`[/wait:value]` specifies the number of seconds policy processing waits to finish. The default is 600 seconds. A `0` wait value processes immediately. A `-1` value places the wait time at indefinitely.

`[/logoff]` forces a logoff after the refresh completes.

`[/boot]` forces the computer to restart after the refresh completes.

Example: `gpupdate /force /boot`

help

The `help` command displays information about specific commands.

Syntax: `help [command]`

Explanation: `[command]` is the name of the command for which you want help.

Example: `help expand`

Notes: If you do not specify the *command* parameter when using the `help` command, all commands are listed.

hostname

The **hostname** command displays the name of the current host.

Syntax: `hostname`

ipconfig

The **ipconfig** command is used to view and control information related to a network adapter.

Syntax: `ipconfig [/allcompartments] [/all|/renew [adapter] | /release [adapter]|/renew6 [adapter]|/release6 [adapter]| /flushdns|displaydns|/registerdns|/showclassid [adapter]| /setclassid adapter [classid]|/showclassid6 [adapter]| /setclassid6 adapter [classid]]`

Explanation: `[/allcompartments]` displays information regarding all compartments and, when used with the `/all` option, shows detailed information about all compartments.

`[/all]` displays all configuration information, including IP and MAC addresses.

`[/renew]` renews the IPv4 address for a specific adapter.

`[/release]` releases the IPv4 address for a specific adapter.

`[/renew6]` renews the IPv6 address for a specific adapter.

`[/release6]` releases the IPv6 address for a specific adapter.

`[/flushdns]` removes all entries from the DNS resolver cache.

`[/displaydns]` shows the contents of the DNS resolver cache.

`[/registerdns]` refreshes DHCP leases and re-registers recently used DNS names.

`[/show classid]` displays all configured IPv4 DHCP class IDs allowed for a specific adapter.

`[/setclassid adapter]` configures an adapter for a specific IPv4 DHCP class ID. A class ID is used to have two or more user classes that are configured as different DHCP scopes on a server. One class could be for laptops, and a different class could be for desktop computers in an organization.

`[/showclassid6 adapter]` displays all configured IPv6 DHCP class IDs allowed for a specific adapter.

`[/setclassid6 adapter]` configures an adapter for a specific IPv6 DHCP class ID.

Examples: `ipconfig /all`

This command verifies whether an IP address has been configured or received from a DHCP server.

`ipconfig /release`

This command releases a DHCP-sent IP address.

`ipconfig /renew`

This command starts the DHCP request process.

md

The **`md`** or **`mkdir`** (for *make directory*) command is used to create a directory (folder).

Syntax: `md [driveletter:] [dirname]`

Explanation: `[driveletter:]` is the drive letter for the disk or volume on which you want to create a directory (folder). It can also include the path.

`[dirname]` is the parameter used to name the directory (folder).

Example: `md c:\test`

Notes: You cannot use wildcard characters with this command.

mmc

The `mmc` command is used to open the Microsoft Management Console in Windows.

Syntax: `mmc [path\filename.msc] [/a] [/64] [/32]`

Explanation: `[path\filename.msc]` is an option to specify where to locate a saved console.

`[/a]` opens the console in author mode.

`[/64]` opens the 64-bit console.

`[/32]` opens the 32-bit console.

Notes: Use the `/32` parameter if you are in a 64-bit operating system and want to run 32-bit snap-ins.

more

The `more` command is used to display a text file.

Syntax: `more filename`

Explanation: `filename` is the path and name of the text file you want to display on the screen.

Example: `more c:\boot.ini`

Notes: The Spacebar enables you to view the next page of a text file. The Enter key enables you to scroll through the text file one line at a time. The Esc key enables you to quit viewing the text file.

msconfig

The `msconfig` command starts the System Configuration utility from a command prompt instead of from a Control Panel or from Settings. The System Configuration utility is commonly used to troubleshoot boot issues specifically related to software and services. The Startup tab lists software that is loaded when the computer boots, and a checkbox enables you to disable and enable the particular application. The same concept is used with the Services tab, which contains checkboxes next to services that are started when the computer boots.

Syntax: `msconfig`

msinfo32

The `msinfo32` command brings up the System Information window from a command prompt. The System Information window contains details about hardware and hardware configurations as well as software and software drivers.

Syntax: `msinfo32 [/computer computer_name]`

Explanation: `[/computer computer_name]` starts the System Information utility for a remote computer.

Examples: `msinfo`

`msinfo /computer Cheryl_Dell`

mstsc

The `mstsc` command starts the Remote Desktop Connection utility.

Syntax: `mstsc [/v:computer[:port]]`

Explanation: `[/v:computer[:port]]` specifies the specific remote computer—by name or IP address and port number—to which you want to connect.

Example: `mstsc /v:Cheryl-PC`

Notes: The default port number for Remote Desktop is 3389, but if a different port has been specified, then you can specify a port by using this command.

nbtstat

The `nbtstat` command is used to display statistics related to current TCP/IP connections on the local computer or a remote computer using NBT (NetBIOS over TCP/IP).

Syntax: `nbtstat [-a remotename] [-A IPaddress] [-c] [-S]`

Explanation: `[-a remotename]` shows the NetBIOS name table for a remote computer designated by `remotename`.

`[-A IPaddress]` shows the NetBIOS name table for a remote computer designated by `IPaddress`.

`[-c]` shows the NetBIOS name cache, names, and resolved IP addresses.

`[-S]` shows NetBIOS client and server sessions.

Examples: `nbtstat -S`

`nbtstat -A 10.5.8.133`

net

The `net` command has many options, and each of them has specific parameters. A few options are shown. Use the `net /?` command to see all options.

Syntax: `net [computer] [group] [localgroup] [print] [session] [share] [use] [user] [view]`

Explanation: `[computer]` adds or removes a computer from the network domain.

`[group]` adds, views, or modifies domain groups.

`[localgroup]` adds, views, or modifies local groups.

`[print]` displays or controls a specific network printer queue.

`[share]` manages share resources.

`[session]` manages sessions with remote devices.

`[use]` attaches to a remote network device.

`[user]` adds, modifies, or views a network user account.

`[view]` lists resources or computers shared by the computer this is used on.

net use

The **`net use`** command attaches to a remote network device.

Syntax: `net use [drive_letter] [\\server_name\share_name /user:domain_name\user_name [password]]`

Explanation: `drive_letter` is the letter (followed by a colon) that `net use` assigns to the network device connection.

`\\server_name` is the name of the network device to which to connect.

`share_name` is the name of the share.

`domain_name` is the domain used to validate the user.

`user_name` is the user to be validated.

`[password]` is an optional entry, so the system does not prompt for a password. If this option is not entered, a password prompt appears, and the system automatically assigns a drive letter once a connection is made.

Example: `net use \\ATC227-01\cisco /user:cisco\student`

net user

The **net user** command is used to add, delete, and make changes to a user on a Windows domain.

Syntax: net user [*username* [*password* | *]] [*options*]] [/domain]

Explanation: *username* is the domain username assigned to the person in the company.

password is used to change a password or assign one to a particular user.

* is used instead of the *password* option to force the password to be entered after the net user command is entered.

options include things like /add, /delete, /times, and /active.

/domain executes the command on the Microsoft domain controller instead of on the local computer.

Examples: net user cschmidt

This command allows you to see account information related to the cschmidt account.

net user cschmidt /active:no

This command allows you to disable the cschmidt account.

net user cschmidt /delete

This command allows you to delete the cschmidt account; note that common practice is to disable, not delete, an account.

netdom

The netdom command manages Active Directory domains and trust relationships. This command has many operations.

Syntax: netdom {add | computername | join | move | query | remove | renamecomputer | reset | resetpwd | verify} [<Computer>] [{/d: | /domain:} <*Domain*>] [<Options>]

Explanation: add adds a workstation to the domain.

[computername] manages the primary and alternate names for a domain controller.

[join] joins a computer to the domain.

[move] moves a computer to a new domain.

[query] presents information about the domain membership, trust, and so on.

[remove] deletes a computer from the domain.

[renamecomputer] renames a domain workstation.

[reset] resets the connection between a domain workstation and the domain controller.

[resetpwd] resets a computer account password for a domain controller.

[verify] verifies the connection between a domain workstation and the domain controller.

netstat

The **netstat** command displays protocol statistics and current TCP/IP network connections.

Syntax: `netstat [-a] [-e] [-n] [-o] [-p protocol] [-r] [-s]`

Explanation: `[-a]` shows all connections and listening port numbers.

`[-e]` shows Ethernet statistics and can be used with the `-s` option.

`[-n]` shows addresses and port numbers.

`[-o]` shows active TCP connections.

`[-p protocol]` shows specific connections that use a specific protocol. The *protocol* parameter can be one of the following: IP, IPv6, ICMP, ICMPv6, TCP, TCPv6, UDP, or UDPv6.

`[-r]` shows the routing table.

`[-s]` shows statistics for a particular protocol.

Examples:

```
netstat
netstat -a
netstat -p TCP
```

Notes: The parameters used with this command must be preceded by a dash rather than the / (forward slash) used by most commands.

notepad

The `notepad` command starts the Windows Notepad accessory.

Syntax: `notepad`

nslookup

The **nslookup** command is used to troubleshoot DNS issues.

Syntax: `nslookup [-option] [hostname] [server]`

Explanation: `[-option]` can be a variety of options, such as `exit`, `finger`, `help`, `ls`, `lserver`, `root`, `server`, and `set`. See Microsoft Learn for a complete list.

`[hostname]` is the name of a host, such as the computer name for a specific computer in an organization.

`[server]` is the URL of a specific server, such as www.pearsoned.com.

Examples:

```
nslookup www.pearsoned.com
nslookup -querytype=hinfo -timeout=10
```

The second example changes the default query type to a host and the timeout to 10 seconds.

Notes: You must have at least one DNS server IP address configured on a network adapter (which you can view with the `ipconfig /all` command) in order to use the `nslookup` command. There are two modes of operation: non-interactive and interactive. The non-interactive has more commands than those shown in the examples given. The interactive mode is started by simply typing `nslookup` and pressing [Enter].

pathping

The **pathping** command sends multiple ping requests (see the following section, on the `ping` command) to each router between the source computer and the target device over a period of time. Based on results from each device, the command provides information about network latency and network loss at the intermediate hops.

Syntax: `pathping [-g host-list] [-h maximum_hops] [-i address] [-n] [-p period] [-q num_queries] [-w timeout] [-4] [-6] target_name`

Explanation: `[-g host-list]` forces use of loose source routing along host-list. In other words, *`host-list`* is the set of routers that must be pinged along the path to *`target`*. *`host-list`* is a series of (a maximum of nine) IP addresses separated by commas.

`[-h maximum_hops]` specifies the maximum number of hops to search for the target.

`[-i address]` forces the use of the specified source address.

`[-n]` suppresses resolution of router IP addresses to hostnames, potentially speeding up the `pathping` process.

`[-p period]` defines the wait period, in milliseconds, between pings.

`[-q num_queries]` indicates the number of queries per hop.

`[-w timeout]` dictates the wait timeout, in milliseconds, for each reply.

`[-4]` forces the use of IPv4.

`[-6]` forces the use of IPv6.

`target` is the destination IP address.

Examples: `pathping -4 -n www.pearson.com`

This example generates network latency and loss statistics for the www.pearson.com website, using IPv4 and suppressing the resolution of intermediate router IP addresses to hostnames.

ping

The **ping** command tests connectivity to a remote network device.

Syntax: `ping [-t] [-a] [-n count] [-l size] [-i ttl] [-S source_addr] [-4] [-6] target`

Explanation: `[-t]` pings the destination until stopped with Ctrl+c keystrokes. To see the statistics and continue, press the Ctrl+Break keys.

`[-a]` resolves IP addresses to hostnames.

`[-n count]` defines how many pings (echo requests) are sent to the destination.

`[-l size]` defines the buffer size (the length of the packet).

`[-i ttl]` defines a Time to Live value from 0 through 255.

`[-S source_addr]` defines the source IP address to use.

`[-4]` forces the use of IPv4.

`[-6]` forces the use of IPv6.

`target` is the destination IP address.

Examples: `ping -t www.pearson.com`

This example pings the Pearson website indefinitely until the Ctrl+c key combination is used.

`ping -n 2 -l 1450 165.193.130.107`

This example sends two echo requests (pings) that are 1450 bytes to the Pearson website.

rd or rmdir

The `rd` command and the **`rmdir`** command perform the same function. They are used to remove a directory (folder).

Syntax: `rd [driveletter:][path] name`

Explanation: `[driveletter:]` is the drive letter for the disk or hard drive volume from which you want to remove a directory (folder).

`[path]` is the optional path and name of the directory (folder) you want to remove.

`name` is the name of the folder/directory to remove.

Example: `rd c:\Test\Junkdata`

This command removes a directory (folder) called `Junkdata` that is a subdirectory under a directory (folder) called `Test`. This directory is located on the hard drive (`C:`).

Notes: You do not have to use the `driveletter:` parameter if the default drive letter is the same as the one that contains the directory to be deleted.

regedit

The `regedit` command accesses the Windows registry editor.

Syntax: `regedit`

Explanation: All the Windows configuration information is stored in a hierarchical database. The registry editor can modify specific registry keys, back up the registry, or set specific values to the defaults.

Notes: The `regedt32` command brings up the same registry editor window as `regedit`.

regsvr32

The `regsvr32` command registers `.dll` files in the Windows registry.

Syntax: `regsvr32 [/u] name`

Explanation: `name` is the name of the `.dll` file that will be registered.

`[/u]` is an optional switch used to unregister a `.dll` file.

Example: `regsvr32 wuapi.dll`

This command registers a Windows update DLL file.

Notes: There is a 64-bit version of this file in the `SysWow64` folder.

ren

The `ren` command renames a file or directory (folder).

Syntax: `ren [driveletter:] [path] name1 name2`

Explanation: `[driveletter:]` is the drive letter for the disk or hard drive volume where you want to rename a file or a directory (folder).

`[path]` is an optional parameter that tells the operating system the path of the file or directory (folder) you want to rename.

`name1` is the old name of the file or directory (folder) that you want to rename.

`name2` is the new name of the file or directory (folder).

Example: `ren c:\cheryl.bat c:\newcheryl.bat`

Notes: The renamed file cannot be placed in a new location with this command. Move or copy the file after you rename it if that is what you want to do. The `*` and `?` wildcard characters are not supported.

robocopy

The **`robocopy`** command is used to copy files and has a lot more parameters than `copy` or `xcopy`.

Syntax: `robocopy [source] [destination] [file [file]...] [options]`

Explanation: `[source]` specifies the source directory in the `drive:|` path format or the `\\server\share` path format.

`[destination]` specifies the destination directory in the drive:| path format or the `\\server\share` path format.

`[file]` is the files to copy, including wildcards. The default is `*.*`.

`[options]` includes various options, such as `/s` to copy subdirectories (but not empty ones), `/e` to copy subdirectories (including empty ones), `/mov` to move files and delete the source, `/move` to move files and directories and delete the source, `/a` to copy files with the archive attribute set, and `/m` to copy files with the archive attribute set and to reset the archive bit.

Examples: `robocopy c:\users\cschmidt\My Documents\Book d:\ /e`

This command copies the contents of the `Book` subfolder to the `D:` drive and includes any empty directories.

`robocopy \\CSchmidt\Book \\RLD\SchmidtBook`

This command copies all files from the `CSchmidt` computer share called `Book` to the `RLD` computer network share called `SchmidtBook`.

services.msc

The `services.msc` command is used to open the Microsoft Management Console and display the Services window.

Syntax: `services.msc`

Notes: The Services window shows the applications that run as background applications. Some services are manually started by the user or a technician,

some start automatically, and some start automatically but delay starting to allow faster booting. This window is commonly used to start a service or to verify that a service such as the print service is still started.

set

The `set` command is used to display and view different variables.

Syntax: `set [variable = value]`

Explanation: `variable` is one of the following:

`AllowWildCards` is a variable used to enable wildcard support for the commands that normally do not support wildcards.

`AllowAllPaths` is a variable that allows access to all the computer's files and folders.

`AllowRemovableMedia` is a variable that allows files to be copied to removable media.

`NoCopyPrompt` is a variable that disables prompting when overwriting a file.

`value` is a setting associated with a specific variable.

Examples: `set allowallpaths = true`

This command allows access to all files and folders on all drives.

`set allowremovablemedia = true`

This command allows you to use a flash drive.

`set allowwildcards = true`

This command allows you to use wildcards at the command prompt.

Notes: To see all the current settings, type `set` without a variable, and the current settings display. The `set` command can be used only if it is enabled using the Group Policy snap-in.

sfc

The **`sfc`** command starts the System File Checker utility from a command prompt. The System File Checker verifies operating system files.

Syntax: `sfc [/scannow] [/verifyonly] [/scanfile=file_name] [/verifyfile=file_name] [/offwindir=windows_directory] [/offbootdir=boot_directory]`

Explanation: `[/scannow]` scans all protected system files and repairs those that are damaged, if possible.

`[/verifyonly]` scans all protected system files but does not repair any detected problems.

`[/scanfile=file_name]` scans the specified file and repairs it if necessary. `file_name` should contain the full path.

`[/verifyfile=file_name]` verifies the specified file but does not repair it. `file_name` should contain the full path.

`[/offwindir=windows_directory]` is used for offline repairs for the specified Windows directory.

`[/offbootdir=boot_directory]` is used for offline repairs for the specified boot directory.

Examples: `sfc /scannow`

`sfc /scannow /offwindir=c:\Windows`

shutdown

The `shutdown` command is used to restart or shut down a local or remote computer.

Syntax: `shutdown [-l] [-s] [-r] [-a] [-f] [-m [\\computer_name]] [-t xx] [-c "message"]`

Notes: If this command is used without any parameters, the command logs off the current user.

You can use the `-a` parameter only during the timeout period.

Explanation: `[/l]` logs off the current user.

`[-s]` shuts down the computer.

`[-r]` reboots the computer.

`[-a]` aborts the shutdown process.

`[-f]` forces active applications to close.

`[-m [\\computer_name]]` specifies a particular computer to shut down.

`[t xx]` specifies the number of seconds to wait before shutting down the computer.

`[-c "message"]` specifies a 127-maximum-character message to show in the System Shutdown window.

Examples: `shutdown -f -m \\Raina-PC -t 30 -c "Going down in 30 seconds, daughter"`

systeminfo

The `systeminfo` command displays detailed configuration information about a specific computer.

Syntax: `systeminfo [/s computer] [/u domain\user] [/p password] [/fo [table | list | csv]]`

Explanation: `[/s computer]` is an optional parameter that designates a specific remote computer using the computer name or IP address; otherwise, the local computer is selected by default.

`[/u domain\user]` specifies authentication for the remote computer.

`[/p password]` specifies a password for the remote computer user ID.

`[/fo [table | list | csv]]` defines whether the output displays in table format, list format, or CSV (comma-separated-values) format. The default is to display in table format.

Examples: `systeminfo`

`systeminfo /s CSchmidt /u pearson\cschmidt /p G#T0UT0FH3R#`

taskkill

The `taskkill` command is used to halt a process or task.

Syntax: `taskkill [/s computer] [/u domain\user] [/p password] [/pid process_id] [/im name] [/f] [/t]`

Explanation: `[/s computer]` is an optional parameter that designates a specific remote computer using the computer name or IP address; otherwise, the local computer is selected by default.

`[/u domain\user]` specifies authentication for the remote computer.

`[/p password]` specifies a password for the remote computer user ID.

`[/pid process_id]` specifies a specific process ID to halt.

`[/im name]` specifies a specific image or application name to halt.

`[/f]` forcefully terminates the process.

`[/t]` is a "tree kill" that kills all child processes associated with the process ID.

Examples:

```
taskkill /pid 1230 /pid 1231 /pid 1242
taskkill /im iexplore.exe
```

tasklist

The `tasklist` command is used to list process IDs (PIDs) for active applications and services.

Syntax: `tasklist [/s computer] [/u domain\user] [/p password] [/fo {table|list|csv}] [/v]`

Explanation: `[/s computer]` is an optional parameter that designates a specific remote computer using the computer name or IP address; if no computer is specified, the local computer is selected by default.

`[/u domain\user]` specifies authentication for the remote computer.

`[/p password]` specifies a password for the remote computer user ID.

`[/fo {table|list|csv]` specifies the output format (table, which is the default, list, or CSV).

`[/v]` displays output in a verbose format.

Example: `tasklist /fo csv`

Notes: This command should be used before the `taskkill` command.

telnet

The `telnet` command is used to access a remote network device.

Syntax: `telnet [destination]`

Explanation: `[destination]` is the name or IP address of the remote network device.

Notes: The Telnet client must be enabled through the *Programs and Features* section of the Control Panel > *Turn Windows Features On or Off*. SSH is a better and more secure tool to use.

tracert

The **tracert** command verifies the path taken by a packet from a source device to a destination.

Syntax: `tracert [-d] [destination]`

Explanation: `[-d]` speeds up the `tracert` process by not attempting to resolve intermediate router IP addresses to names.

`[destination]` is the targeted end device, listed by IP address or name.

Example: `tracert -d www.pearsoned.com`

type

The `type` command displays the contents of a text file.

Syntax: `type filename`

Explanation: `filename` is the path and name of the text file you want to display on the screen.

Example: `type c:\byteme.txt`

Notes: The Spacebar enables you to view the next page of a text file. The Enter key enables you to scroll through the text file one line at a time. The Esc key enables you to quit viewing the text file.

wbadmin

The `wbadmin` command is used to perform backups and restores.

Syntax: `wbadmin [start backup] [stop job] [get versions] [get items]`

Notes: Each parameter listed for `wbadmin` has options (settings) that follow. Use the `/?` after each parameter to see these options; for example, `wbadmin start backup /?`.

Explanation: `[start backup]` begins the backup process.

`[stop job]` halts the currently running backup.

`[get versions]` provides a list of available backups from the local computer or from a remote computer.

`[get items]` provides a list of items included in a particular backup.

Example: `wbadmin start backup`

If no parameters are specified after `wbadmin start backup`, the settings within the daily backup schedule are used.

Notes: You cannot recover backups that were made with `ntbackup` using the `wbadmin` command, but you can download the `ntbackup` command/application from Microsoft.

whoami

The **whoami** command can be used to get username and group information along with the security identifiers (SIDs), claims, privileges, and logon identifier (logon ID) for the current user on the local system. That is, it shows who is the currently logged on user. If no switch is specified, `whoami` displays the username in NTLM format (*domain\username*).

Syntax 1: `whoami [/upn | /fqdn | /logonid]`

Syntax 2: `whoami { [/user] [/groups] [/claims] [/priv] } [/fo format] [/nh]`

Syntax 3: `whoami /all [/fo format] [/nh]`

Explanation: `[/up]` displays the username in user principal name (UPN) format.

`[/fqdn]` displays the user name in fully qualified domain name (FQDN) format.

`[/user]` displays information on the current user along with the SIDs.

`[/groups]` displays the group membership for the current user, the type of account, security identifiers (SIDs), and attributes.

`[/claims]` displays claims for the current user, including the claim names, flags, types, and values.

`[/priv]` displays the security privileges of the current user.

`[/logonid]` displays the logon ID of the current user.

`[/all]` displays the current user's username, the groups they belong to and SIDs, claims, and privileges for the current user's access token.

`[/fo format]` specifies the output format to be displayed. Valid values are `TABLE`, `LIST`, and `CSV`. Column headings are not displayed with `CSV` format. The default format is `TABLE`.

`[/nh]` specifies that the column header should not be displayed in the output. This is valid only for `TABLE` and `CSV` formats.

Example: `whoami /groups`

winver

The **winver** command shows the Windows version that is currently running, along with the build number. The results are displayed in a graphical window, not at the command prompt.

Syntax: `winver`

Example: `winver`

wscript

`wscript` is the command that brings up a Windows-based script property sheet that sets script properties. The command-line version is `cscript.exe`.

xcopy

The `xcopy` command copies and backs up files and directories.

Syntax: `xcopy source [destination] [/e] [/h]`

Explanation: `source` is the full path from where the files are copied.

`[destination]` is the optional destination path. If the destination is not given, the current directory is used.

`[/e]` copies all directories and subdirectories, including empty ones.

`[/h]` copies hidden and system files.

Example: `xcopy c:\users\cheryl\Documents\Chap1\Chap1.docx e:\Book\Chap1`

This command copies a file called `Chap1.docx` (which is located in a folder called `Chap1` that is a subfolder of the `Documents` folder, which is a subfolder of the `cheryl` folder, which is a subfolder of the `users` folder) to the `E:` drive and places it in the `Chap1` subfolder that is contained in the `Book` folder.

Notes: The `xcopy` command normally resets read-only attributes when copying.

Introduction to Scripting

A *script* is a little program that is designed to do a specific task. There are many scripts available for networking professionals to use, and you can also create your own. While you don't need to become a coding expert to write useful scripts, you'll find that being able to create short scripts yourself will not only help your career but simplify many of your tasks.

This section will help you understand the basics of scripting. It introduces various script languages, including Python and JavaScript; shell scripts for Unix-based systems; and PowerShell, VBScript, and batch files for Windows-based systems.

What Is Scripting?

A script is a small program that carries out a task or a series of tasks based on specific conditions. Whereas programs written in programming languages you may have heard of (such as C++ or Java) are compiled, scripts are interpreted. The difference is in how the code is executed. An **interpreted program** is carried out one line at a time as the computer encounters each line of code. This makes it ideal for use by IT professionals. On the other hand, with a **compiled program**, the entire program must be converted into machine language before it can be run.

A script is a **text file**. This means it can be created in any text editor, such as Notepad in Windows. However, each scripting language has its own specific syntax (commands, rules, and symbols that are used to create instructions) that you need to learn before you can create your own scripts. Running a script is easy. From a command prompt or command line, you simply type the name of the script and press Enter.

For example, Figure 15.9 shows a batch script written in Notepad. The purpose of the script is to count by 5s from 5 to 50. At this point, you don't need to understand each line of the file. Just know that the file contains instructions that are written according to the syntax for batch files.

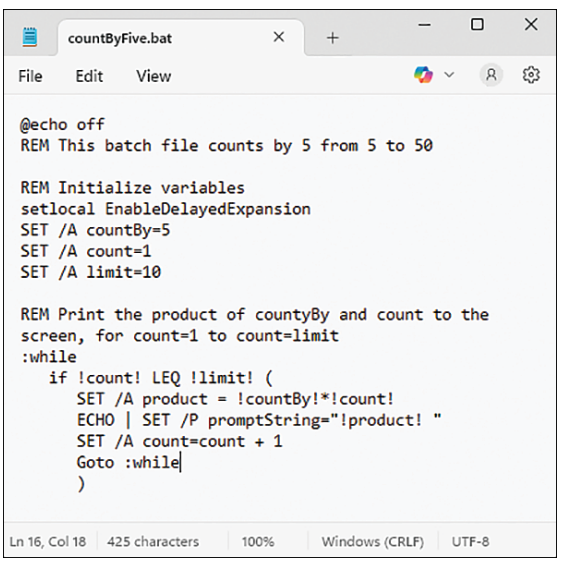


FIGURE 15.9 Batch script in Notepad

The `dir` command in Figure 15.10 shows that the script has been saved in plaintext to the file `countByFive.bat`. The next command (`countByFive.bat`) illustrates that the batch file can be run by typing its name and pressing [Enter].

```
Command Prompt

D:\Users\Akil\Documents\batchFiles>dir
 Volume in drive D is DATA
 Volume Serial Number is 76CD-D1CA

 Directory of D:\Users\Akil\Documents\batchFiles

03/30/2025  08:17 AM    <DIR>          .
03/30/2025  08:17 AM    <DIR>          ..
03/30/2025  08:13 AM               442 countByFive.bat
               1 File(s)            442 bytes
               2 Dir(s)  101,952,819,200 bytes free

D:\Users\Akil\Documents\batchFiles>countByFive.bat
5 10 15 20 25 30 35 40 45 50
D:\Users\Akil\Documents\batchFiles>
```

FIGURE 15.10 Running a batch script

Scripting allows you to automate some network administration tasks. For example, every time a user logs in to a network, that user must be assigned various network drives based on certain conditions. A script can automate this process. This type of script would run each time a user logs on. In other cases, a script may need to run only once, but it might be able to be written to be applied in different situations. For example, a script may be able to modify the registry under one specific condition. If many servers on a network need to do this task, the script can be distributed and can run that one task on all the servers.

A network administrator gains many advantages by being able to create and use scripts. The following are some of them:

- Scripts save time. They can be written to carry out complex tasks that would take you a lot of time if done by hand. While a script runs, you are free to concentrate on other things.
- Scripts ensure consistent operation. Once a script is written, each time it is run, you can be sure it will be completed exactly as before. Using scripts to complete a task is less likely to cause errors than if the task were done manually at various times.
- Scripts can be flexible. Since scripts use the basic logical constructs of all programming languages, they can be created to respond in different ways to different conditions.

Script File Types

There are many scripting languages that you can choose from, although some of them must be used with specific operating systems, and some are more suited to certain tasks than others. Table 15.1 shows the most common and easily learned scripting languages.

TABLE 15.1 Common scripting languages

Language	File extension	Description
Shell script	`.sh`	A shell script is a set of commands within a text file for a Unix- or Linux-based system. Shell scripts may not run correctly on a Windows system.
Batch file	`.bat`	A batch file is a script file that is strictly Windows based. It contains a series of commands to execute one after another. The instructions in a batch file can only be interpreted by the Windows operating system.

Language	File extension	Description
Python	`.py`	Python is a good language for writing scripts because it is relatively easy to learn, and Python scripts can run on most operating systems.
VBScript	`.vbs`	VBScript is a Microsoft scripting language that has some commands that are part of the Visual Basic programming language. It was designed specifically for use with Microsoft's Internet Explorer. Unless you are certain you will only use a script on a Windows machine, it is probably better to use a more versatile language.
JavaScript	`.js`	JavaScript is a programming language that has many uses. In some ways, it is valuable for creating script files because it can be run on any operating system. However, it may be more difficult to learn than Python, which also has the benefit of being platform independent. Creating and running command-line JavaScript requires that Node.js be installed.
PowerShell	`.ps1`	PowerShell is a Windows environment that was created to help in IT task automation and configuration management. It is an interface that allows you to use small programs called cmdlets that run consecutively from a single file that you can use repeatedly and share with others. PowerShell files with the `.ps1` extension can be opened, edited, and run in the PowerShell Script pane.

TECH TIP

Scripts are just text files

Scripts contain only text, with no special formatting. Each byte of a text file represents one character of ASCII code. Text files must be created in a text editor such as Notepad. Files that have been created with Microsoft Word or OpenOffice's Writer are stored as binary files, which do not have a one-to-one mapping between bytes and characters. If you attempt to copy and paste code from any source that is not a text file, you may cause issues, even if you see no visible difference between your file and the text that you copied. This is because formatting commands are automatically included in the copy process.

Use Cases for Scripting

As indicated earlier, scripting is available in many operating systems and application environments. Thus, scripts can be used for a wide variety of purposes, from automating a simple process to configuring an entire virtual network. The following are some of the most common use cases for scripting available in most operating systems:

- **Basic automation:** A task that needs to be completed at a particular time with specific requirements can be automated with scripting. In the Windows environment, Task Scheduler can execute a script according to the prescribed schedule. The `crontab` command is used to schedule automated jobs in Unix/Linux.
- **Restarting machines:** Sometimes computers need to be restarted for maintenance purposes at particular times during the day or after they have been running for a specified amount of time. A script can be used to calculate the uptime, perform the required maintenance, and then send a restart command to the operating system. Additional tasks can be completed after the system boots up again.

- **Remapping network drives:** As discussed in Chapter 18, "Computer and Network Security," folders can be shared across a network so data can be centrally stored and accessed. If one or more shared drives are always needed on a computer, a script can connect (or mount) the required folders when the computer boots up or when specific users log in. The shared folders can also be mapped to drive letters; for example, the `T:` drive can represent the shared `contracts` folder on the `ATCDOC1` server.
- **Installation of applications:** Applications must be installed with the correct options in order to work properly. Most installation processes prompt the technician for settings as the application is installed. To minimize installation mistakes, a script can be configured to automatically provide the required information for the program.
- **Automated backups:** The backup schedule for a computer depends on the device's role and the type of information stored on the device. In addition, backups might need to be spaced out due to restraints on backup resources. A script can be used to back up a computer to a designated storage device (local, network, or cloud) according to a prescribed schedule.
- **Initiating updates:** Timely updates for applications, devices, and operating systems are important for the health and security of computers. As with backups, scripts can download and install the required updates from a specified location and on a predetermined schedule.
- **Gathering of information/data:** The health, security, utilization and efficiency of network devices changes over time. Network technicians and engineers need to collect information from devices to make decisions regarding issues such as deployments, maintenance, updates, and replacements. Scripts can be used to automatically send various data points (disk utilization, failed logins, ping response times, and so on) to a central location for analysis. The collections can be scheduled or on demand.

Note that some of these tasks are used in conjunction with each other; for example, a restart script can be used to back up a computer, download updates, and then restart the computer.

Mitigating Consequences of Scripting

Scripts must be carefully designed and thoroughly tested before they are deployed. Scripts can configure multiple system settings on several devices on a network. Therefore, any mistakes can potentially affect thousands of computers, even more internal users, and millions of customers. One seemingly small mistake could have a significant impact on a company's operations, finances, or reputation.

Furthermore, while scripts are intended to increase operational efficiency, a poorly written script can have the opposite effect and mishandle system or network resources. For example, a script might mount the wrong network drives, allocate excessive or insufficient memory space for a particular application, establish the wrong user rights or permissions, or create an infinite loop. These and other mistakes can cause browser or system crashes, create network delays, or render resources inaccessible.

Finally, since scripts are usually intended to run unattended, any issues that they cause might go undetected for days or months. A threat actor could have unfettered access to a few machines or an entire network if a script accidentally introduces malware or creates some other security vulnerability.

The following practices can help you avoid these and other unintended consequences of scripting:

- **Team programming and peer review:** Whenever possible, at least two people should synchronously work on a script together, especially if the script is complicated. Team programming (also called pair programming) takes advantage of the fact that everyone brings their

own perspective to a problem. This blending of ideas helps in developing solutions more quickly because everyone compensates for another's deficiencies. For the same reason, a finished script should be reviewed by a qualified peer before it is deployed, especially if team programming is not feasible.

> **Establishing a test regimen:** All scripts should be thoroughly tested before they are deployed. In a corporate environment, any changes to a system (including script changes) should be tested in a development environment (DEV) and then a user acceptance test environment (UAT) before they are deployed to the full live production environment (PROD). Because end users or customers do not access the DEV systems, technicians and engineers should use the DEV devices to perform the initial troubleshooting and testing. They can then coordinate with a small group of end users in UAT to validate the new code. Any issues discovered in UAT should be resolved and then retested in DEV and UAT. Only after the new code successfully passes DEV and UAT testing should it be deployed to PROD.

> **Testing multiple scenarios:** If a script is targeted for multiple devices, the unique characteristics of the devices must be considered during the testing phases because these differences can affect the script's performance across the network. Test units should account for variances in parameters such as memory and hard drive space, CPU type and speed, location, operating system version, internal network equipment, broadband connection, and Active Directory domain.

Environment Variables

Like variables in traditional programming languages, variables in scripts allow the scripts to adapt to changing conditions. An **environment variable** is a variable that describes the environment in which a program runs. For example, environment variables can tell the computer where to find a specific program and can be used to answer questions such as, "Where are saved files stored?" or "Where are the temporary files stored for this particular application?" Environment variables can also describe parameters such as the number of processors, the processor model, or the processor architecture.

In Windows, an environment variable has a name and a value. For example, the variable that stores the location of the Windows operating system files is `windir` (short for *Windows directory*), and the value associated with this variable is normally `C:\Windows`. This means that the Windows program is located in the `C:\` drive in a folder called `Windows`. In this case, the value of the environment variable is the path to the program identified by the variable name.

Another important variable is `PATH`. The `PATH` **variable** tells a program where to find the files it may need. Programs that need specific files to run look for the `PATH` variable automatically. The value of the `PATH` variable is set by a program when it is installed.

Two types of environment variables are system and user. System environment variables are global and cannot be changed by any user. They refer to critical system resources, such as the location of Windows or where program files are stored on a computer. They are set by specific programs and drivers. System environment variable values are the same for all user accounts.

User environment variables, however, have values that differ from user to user. They store the location of such things as a user's profile, where that user stores temporary files, and so on. These variables can be set by the user, by Windows, or by various programs that work with user-specific locations.

To access environment variables in Windows, you can type `environment` into the search box and then click or select *Edit the system environment variables*. The System Properties window opens (see Figure 15.11), and you can click on *Environment Variables* to open the Environment Variables window (see Figure 15.12). There are some minor visual differences between various

versions of Windows, but the options and buttons are the same, regardless of which version of Windows you are using.

You can also open the Environment Variables window by accessing *Settings* > *About* > *Advanced system settings*. This takes you to the *System Properties* window, where you can click the *Environment Variables* button to open the *Environment Variables* window.

To edit an environment variable, to add a new environment variable, or to reorder the current environment variables, you can click the *Edit* button in the *Environment Variables* window.

You can also access the *System Properties* window by pressing ⊞+R to open the *Run* dialog box and then enter the command `systempropertiesadvanced.exe`, as shown in Figure 15.13.

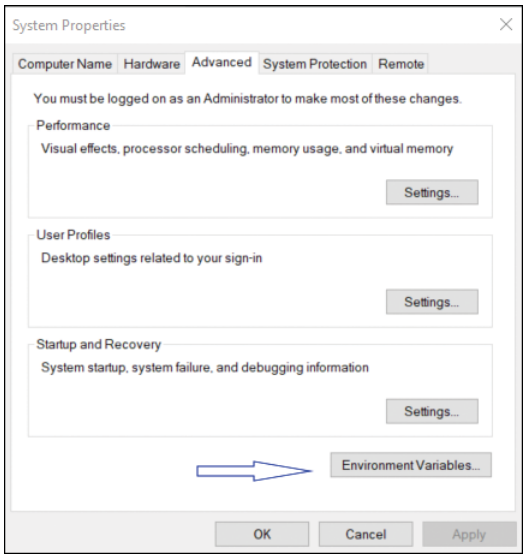


FIGURE 15.11 Accessing Windows environment variables

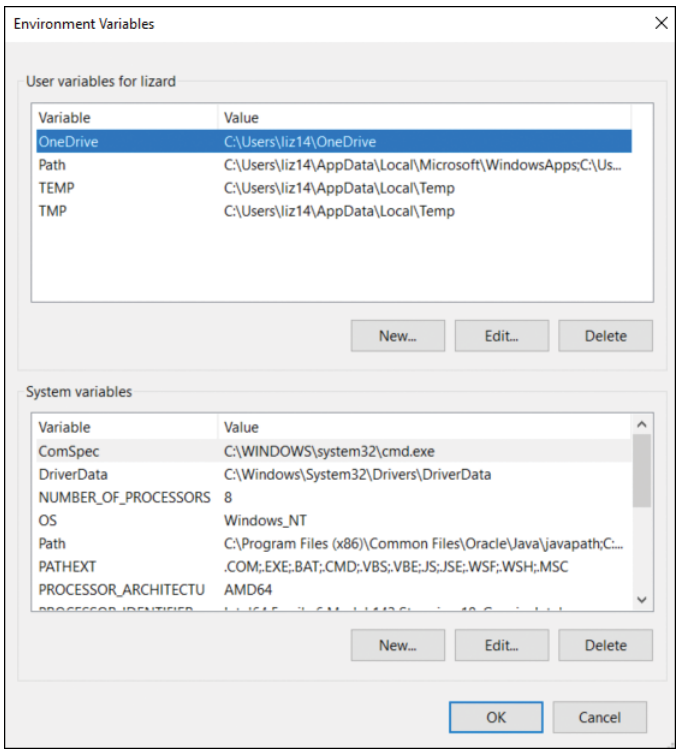


FIGURE 15.12 Environment Variables window

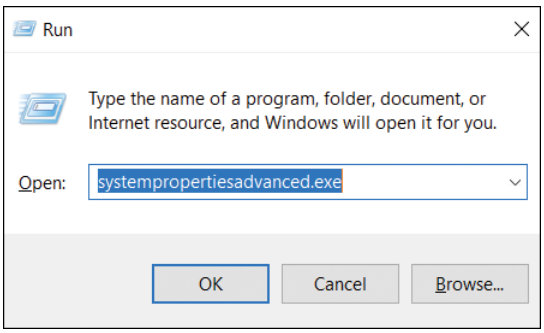


FIGURE 15.13 Accessing the System Properties window through the Run dialog box

At the command prompt, you can enter `set` to see all the environment variables, as shown in Figure 15.14.

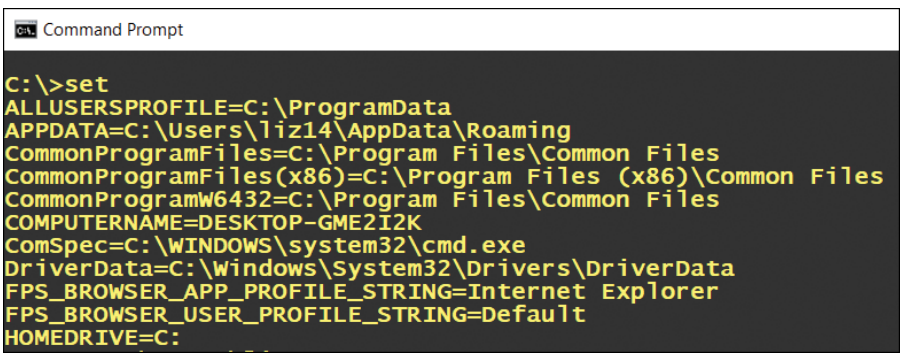


FIGURE 15.14 Viewing environment variables by using the `set` command

There may be times when you need to create an environment variable to tell a computer how to find the program needed to run a script. PowerShell (`.ps1` files) and VBScript (`.vbs` files) both run on the .NET framework, which is installed with Windows. Batch files (`.bat`) are run from the command line. Running Python, however, requires a little more work. The Python engine is not preinstalled on Windows, even though Windows installers have been included with every release. Still, you may need to create an environment variable to run Python. The same is true for JavaScript, for which you need to install Node.js. Node.js is a free, open source environment where you can run JavaScript code without a browser. Node.js is also very flexible in that it can run on most operating systems, including Windows, Linux, and macOS.

Script Syntax

Every programming language has its own syntax. The **syntax** of a language is the set of symbols and rules used to create instructions. Understanding and using correct syntax is the only way you can get a script to work because a computer cannot understand the context of an instruction otherwise. If an instruction is not composed in the exact syntax for that language, it will not be executed and, worse, may cause the whole script to crash.

Syntax refers to more than using the correct words in a command. It includes the correct symbols and punctuation. For example, if a language requires an instruction to terminate with a semicolon, leaving off the semicolon invalidates the entire instruction and usually causes serious errors. Each scripting language has its own specific syntax, which you must learn in order to write a script in that language. However, it isn't as hard as it sounds. Most languages have similar syntax. And all scripting and programming languages use the same logical constructs to write instructions. Once you understand the logic behind programming instructions and commands, learning a language's specific syntax is pretty easy.

For example, the syntax to display a sentence such as `Hello, my friend!` on the console uses the following syntax in these four scripting languages:

> **Python:** `print("Hello, my friend!")`
> **JavaScript:** `console.log("Hello, my friend!");`
> **Batch file:** `ECHO Hello, my friend!`
> **Shell script:** `echo "Hello, my friend!"`

Introduction to Script Programming

In the 1960s, scientists proved that all programming code can be done using three constructs: sequence, selection, and repetition. **Sequence** refers to how a computer executes code one line at a time from top to bottom. **Selection** refers to how specific lines of code are run if a specific condition is met. **Repetition** (sometimes called iteration) refers to how a computer can execute specific lines of code repeatedly. Everything you see and do with any computer or any device that uses a computer runs on programming code, and all of that code is based on the same simple logic described here. This is incredible.

A program is a list of instructions written by a programmer to perform a task or tasks. The instructions are executed one line at a time, in the order in which they are written. A script is simply a type of program. The difference between a scripting language and other types of programming languages lies in how the code executes, not in how the code is written.

Programming languages such as C++ and Java are compiled languages. A compiled language uses a compiler to translate the source code to machine code. Machine code is code that is specific to a given processor and operating system. Once a program has been translated to machine code, the computer directly runs the machine code, without any additional conversion. Before a program can be compiled, it must be completely error free.

In an interpreted implementation of a language, the computer does not execute the source code directly but uses an interpreter to translate each line of source code to machine code. If an error is found, the program stops and sends feedback to the programmer. This allows the programmer to see the error immediately and make necessary changes. Networking professionals commonly use interpreted languages, often called *scripting languages*, because they are relatively easy to learn and use, they are easy to debug, and they are portable across various hardware and network platforms.

All programs rely on input, processing, and output. A program performs a task based on some type of input. The **input** may come from a user typing information that the program requests, from values sent by other parts of the program, or from the computer itself. During **processing**, the program manipulates this information and returns some output (the **processing**). The **output** can be results shown on the screen or console or may be changes sent to other parts of the program or to the computer itself.

Together, the input–processing–output sequence and the three programming constructs form the basis for all programs. Before learning about those constructs, it is important to understand two basic concepts: variables and data types.

Variables

A program **variable** is a named memory location that stores data of a specific type (integer, floating-point number, or text). The *value* of that variable is the data contents at that memory location. It is called a variable because its value can change (vary) as the program runs. You can think of a location in the computer's memory as a mailbox. The variable is the name printed on that mailbox,

and the value of the variable is the contents of that box. For example, if you have a variable named `myNumber` and you set its value to `23` using an instruction in the syntax of the language you are using, the memory location named `myNumber` stores the number `23`:

myNumber
23

However, as soon as you write another instruction to change the value of `myNumber` to, for example, `584`, the value `23` is lost forever, and the new value takes its place:

myNumber
584

From now on, every time `myNumber` is referenced in a program, it means `584`—at least until that value is changed by a different instruction.

Previously you saw how to display some text on the screen using the syntax of several different scripting languages. The text that was displayed was hard-coded, which means the programmer wrote the exact words to be displayed. But if the programmer had, instead, used a variable to store the text, the text might be changed every time the program runs, depending on different conditions.

For example, the program could display `Good morning` if the current time is between 5:00 a.m. and 11:59 a.m., `Good afternoon` if the current time is between noon and 5:00 p.m., `Good evening` if the current time is between 5:01 p.m. and 9:00 p.m., and so on. The instructions in this code would include a check of the system for the current time and would assign the correct greeting to the variable, depending on the result of the time check. Then the display would greet the user with a message that is appropriate for the time of day.

For example, if a variable is named `myGreeting`, the command to display the correct greeting would then be:

> **Python:** `print(myGreeting)`
> **JavaScript:** `console.log(myGreeting);`
> **Batch file:** `ECHO myGreeting`
> **Shell script:** `echo $myGreeting`

You can see that, while the specific command to have output displayed on the screen differs for each language, the logic for this instruction is the same for all languages: Use the correct command for outputting something on the screen, followed by the variable name that represents the value to be displayed.

A programmer must follow certain rules in selecting variable names. While not every language has exactly the same rules for naming variables, there are some universal rules:

> A variable name cannot begin with a number but may contain numbers. For example, `1stNumber` is not acceptable, but `Number1` is fine.
> A variable name may not include any spaces and, except for the underscore and sometimes the hyphen (_ and -), should not include any punctuation. For example, `my Greeting` is not acceptable, nor is `my&Greeting`, but `my_Greeting` is fine.
> Variables are case sensitive. For example, `Username` is not the same variable as `username` or `userName`.
> A variable name cannot begin with a language's keyword. A **keyword** is a set of characters that is an instruction in that language. In the Python language, for example, `try` is a keyword. Therefore, `tryIt` is not an acceptable variable name in Python; however, `attemptIt` is fine.
> Variable names can be long, but each language has a restriction on how many characters are allowed.

> A variable name should indicate the nature of the content without being too long. Since you will probably have to type variable names many times in a script, you want to keep your variable names as short as possible while still indicating what the variables represent. For example, `gt` is an acceptable variable name but would be confusing to someone who had to work with your code at a later date. Also, `the_greeting_to_be_displayed_to_the_user` is an acceptable variable name, but do you really want to type it 20 times in a script? A better option would be `greeting`.

In order to create a variable, a programmer must declare the variable. This means the programmer writes a line of code to tell the computer that there will be a variable with a specific name and type. (The concept of data types is explained more fully in the next section of this chapter.) Each language has its own way to declare variables, but the concept of a variable **declaration** is consistent across languages: The computer must be told that a variable with a given name will exist, and the computer then assigns a memory location to hold the value of that variable.

If a variable is set to a beginning value when it is declared, this is known as **initialization**. If no value is given when the variable is declared, the computer may leave the memory location empty or may place a default value in that location. The syntax for declaring a variable named `myVarName` and setting its initial value to `0` is shown here for four scripting languages:

> **Python:** `myVarName = 0`
> **JavaScript:** `var myVarName = 0;`
> **Batch file:** `set myVarName=0`
> **Shell script:** `myVarName=0`

Notice that JavaScript and `.bat` files require a keyword before the variable name (`var` in JavaScript and `set` in a batch file), but Python and shell scripts don't. However, in Python and JavaScript, the spaces before and after the `=` symbol are optional, while in a `.bat` file or a `.sh` file, putting spaces before and after this symbol will not work. JavaScript requires a semicolon at the end of the variable declaration, while the other languages shown here do not. You can see why it is important to learn the syntax of each language.

Data Types

The value of a variable is stored in computer memory as a specific type of data. Some languages have a long list of possible data types, while others have only a few. However, all languages distinguish between numbers, types of numbers, and characters or strings of characters (including numbers that are dealt with as text). Strings of numbers are sometimes simply called **strings**.

The data type of a variable determines how much space is allotted in memory to store that value and also determines what operations can be performed with that data. For example, numeric data can be multiplied, but you cannot multiply two alphanumeric characters. **Alphanumeric characters** include all the letters of the alphabet, both uppercase and lowercase, as well as the digits 0 through 9, plus the punctuation marks and symbols available on a normal keyboard (for example, `@`, `#`). If you try to perform an unsupported operation on data stored as a particular data type, your program will either not work at all or will work incorrectly.

There are two basic types of numbers that a computer program normally deals with: integers and floating-point numbers. **Integers** are whole numbers, including zero, and the negatives of whole numbers. **Floating-point numbers** are numbers that can be written in the form $x \div y$, where x and y are integers. A floating-point number can be thought of as a number that includes a decimal value, even if that value is 0. For example, the number 6 is an integer, but the number 6.0 is a floating-point number. Floating-point numbers are handled very differently from integers but,

because they are rarely used in scripts, for the purposes of this book, we do not need to concern ourselves with them. When referring to numeric data, we will only consider integers.

In the previous examples, all the variables named `myVarName` would be stored as numeric data because they were initially given integer values (in this case, `0`). In some languages, you must specify what data type a variable will be. In others, such as Python and JavaScript, the data type of a variable is set by the computer based on the variable's initial value. Once set, a variable's data type cannot be changed while the variable is in use.

Examples of Using Variables

The following examples demonstrate how variables can be used in several scripting languages. In each of the first set of examples, two numeric variables, named `num1` and `num2`, are declared and initialized to integer values and then added together. The result is stored in a third variable, named `numResult`, and then output to the console. The output in all cases would be `7`.

> **Python:**

```
num1 = 3
num2 = 4
numResult = num1 + num2
print(numResult)
```

> **JavaScript:**

```
var num1 = 3;
var num2 = 4;
var numResult = num1 + num2;
console.log(numResult);
```

> **Batch files:**

```
set /A num1=3
set /A num2=4
set /A numResult=%num1%+%num2%
Echo %numResult%
```

> **Shell scripts:**

```
num1=3
num2=4
numResult=$num1+$num2
echo $numResult
```

The following script snippets demonstrate how to join two string variables (variables that hold alphanumeric data) to output a result. In each case, one string variable named `username` is joined with the value of a second string variable named `message`, and the resulting string is output to the console. In these examples, it may be assumed that the name of this computer's user, to be stored in `username`, is Joey Jones. The output in all cases would be `Welcome Joey Jones`.

> **Python:**

```
username = "Joey Jones"
message = "Welcome "
result = message + username
print(result)
```

> **JavaScript:**

```
var username = "Joey Jones";
var message = "Welcome ";
var result = message + username;
console.log(result);
```

> **Batch files:**

```
set username=Joey Jones
set message=Welcome
set result=message+" "+username
Echo %result%
```

> **Shell scripts:**

```
username="Joey Jones"
message="Welcome "
result=$message$username
echo $result
```

You have now seen how to join variables of the same data type—integer and integer, string and string. But it is also possible to join a string variable with an integer variable; however, each language handles this situation differently.

Comments Within Scripts

When a script runs, the computer processes each instruction and does what that instruction says to do. In the examples shown in the previous section, you can see that a script works as follows:

> The first line declares a variable and initializes it with a value.
> The second line declares a second variable and initializes it with a value.
> The third line declares a third variable on the left-hand side of the instruction. Then it joins the values of the first and second variables on the right-hand side of the instruction. Finally, it puts that value into the third variable.
> The last line outputs the value of the third variable to the screen or console.

The purpose of each of these short snippets is clear and easy to see. But you can also see that some of the syntax may be confusing, such as when variable names are enclosed in symbols like `%` (batch files) or have a required symbol like `$` before the variable name (shell scripts). As a script becomes longer, the purpose of some parts of it may not be immediately clear. As you continue to write scripts, you will also see that there may be more than one way to write code to do a specific task. And you may be asked to use or edit a script written by someone else who may no longer be working with you.

For these reasons, it is always a good idea to include **comments** when you write scripts. Comments are put into a script to explain what the script or part of the script is supposed to do. They are meant to be read by the person who is using the script, and they are ignored by the computer when the script runs. Each language has its own syntax for writing comments:

> **Python:** A comment can be on one line or can span multiple lines. A comment that is on one line starts with a hash character (#). A comment may be placed on a new line or following a space at the end of a coded instruction. A multi-line comment begins and ends with three double quotes (`"""`).Consider these examples of Python comments:

```
# This is a single line comment in Python.
Print(result)  # Here's another comment.
"""  This begins a multi-line comment. Everything
until the end of the comment is ignored by the
processor. The comment will end here. """
```

> **JavaScript:** A comment starts start with two slashes (`//`) and goes to the end of the line. A comment may be placed on separate lines or following a line of code. If you want to include several lines in a single comment, open the comment with `/*` and end the comment with `*/`. Consider these examples of JavaScript comments:

```
// This is a single line comment in JavaScript.
Console.log(result)   // Here is another comment.
```

```
/* This begins a multi-line comment. Everything
until the end of the comment is ignored by the
processor. The comment will end here. */
```

> **Batch files:** A comment in a batch file begins with the keyword `REM` of with two colons (`::`). There is a slight danger in using the `REM` command. If `ECHO` (the command to output to the screen) is on, then the comment itself will be displayed. Consider these examples of batch file comments:

```
REM This is a comment in a batch file.
:: This is also a comment in a batch file.
```

> **Shell scripts:** The hash symbol (#) is used to identify a comment in a `.sh` file. It can be placed on a separate line or after the first space following a line of code, as in these examples:

```
# This is a comment in a shell script file.
echo $result  # This is another comment.
```

Basic Script Constructs

As mentioned earlier, all scripts—in fact, all computer programs—are built around three basic **constructs**: sequence, decision (or selection), and repetition (or iteration). Instructions in a script file are executed by the computer in the order in which they are written. Executing instructions in the order in which they appear in the code is known as the *sequence structure*. However, the code may instruct the computer to follow one sequence of instructions under certain conditions and a different sequence of instructions under different conditions. Without this ability to make decisions, a script could do only a very limited number of tasks.

Take, for example, a script that displays a greeting to the user based on the time of day. The computer must be told to check the time and, depending on the result of that check, do only one thing and skip the remaining options. This is known as a selection structure, or a **decision structure**.

A script may also require that a task or part of a task be repeated 2 or 3 or even 1,000 times. Rewriting an instruction many times is tedious and unnecessary. For example, if you want to check a directory to see if it includes a specific file, you need to compare the filename you're searching for with each file in that directory. Instead of writing separate instructions to check the first file, the second file, the third file, and so on, you can write a single structure that says to check a file in that directory and, if it is not the filename you seek, do the same thing again with the next file, and the next, and so on until the list of files in that directory ends or until you have found the file you want. This is known as a **loop structure**, or **repetition structure**.

Decisions: The Selection Structure

A *decision structure*, also referred to as a *selection structure*, consists of a test condition and one or more groups (or blocks) of statements. The result of the test condition determines which block of statements will be executed. This means that some statements in a selection structure will never be executed. For example, if you wrote a script to display a greeting based on the time of day, and it is 10:00 a.m., you only want the block of statements that display `Good morning!` to be executed. The blocks that display `Good afternoon!` or `Good evening!` should be—and are—skipped.

Three main types of selection/decision structures are used in programming: single alternative, dual alternative, and multiple alternative. Before we discuss these three types of selection structures, we need to define the operators used in these structures.

Relational Operators

Operators that compare two expressions are known as **relational operators**. In most programming languages, the symbol >= means "greater than or equal to," the symbol <= means "less than or equal to," and the symbol != means "is not equal to." The > and < symbols mean "greater than" and "less than," but in batch files, the > symbol is a redirection operator and cannot be used to compare values. Batch files and shell scripts use other commands to compare two expressions. Table 15.2 shows the various relational operators and their meanings in most languages.

TABLE 15.2 Relational operators

Meaning	Most common operator	Batch file command	Shell operator
Equal to	`==`	`EQU`	`-eq`
Not equal to	`!=`	`NEQ`	`-ne`
Less than	`<`	`LSS`	`-lt`
Less than or equal to	`<=`	`LEQ`	`-le`
Greater than	`>`	`GTR`	`-gt`
Greater than or equal to	`>=`	`GEQ`	`-ge`

Three Types of Selection Structures

As stated earlier, there are three types of programming structures: sequence, decision (or selection), and repetition (or iteration). In addition, there are three different types of the decision/selection structures: single alternative, dual alternative, and multiple alternative. It is also possible to nest a selection structure inside another selection structure. Let's take a look at each one of these.

Single Alternative

With the single-alternative structure, a test is performed, and if the outcome of the test is true, a block of statements is executed, and then program control moves to the next instruction after the selection structure. If the outcome of the test is not true, nothing is executed, and program control proceeds to the next instruction. For example, imagine a script that is written to check whether the current user is named `Jonas`. If the current user is named `Jonas`, the program displays `User found!`, and if they are not, it does nothing. The current user's name is stored in a variable named `name`. The single-alternative logic for this script in Python would be:

```
if name == "Jonas":
    print("User found!")
continue...
```

If `name` is anything other than `"Jonas"`, the program continues, and nothing happens. This is known as an `if` structure.

Note: Notice the double equals sign (==) in the `if` statement shown in the preceding example. It is called the **comparison operator** or, sometimes, the **equals operator** or the **equality operator**. In most programming languages, a single equals sign (=) assigns the value on the right side of the expression to the variable name on the left side. But a double equals sign *compares* the two values. Basically, this statement says, "Is the value stored in the variable `name` *the same as* `"Jonas"`?" This distinction is very important; using a single equals sign when trying to compare values is an error that often causes a lot of trouble.

Dual Alternative

With the dual-alternative structure, a test is also performed, but one of two possible blocks of statements will always execute. If the outcome of the test is true, one block of statements is executed, and then program control moves to the next instruction after the selection structure. If the outcome of the test is not true, a different block of statements is performed, and the program control proceeds to the next instruction. In a dual-alternative structure, the example shown above might look like this in Python:

```
if name == "Jonas":
    print("User found!")
else:
    print("User not found!")
continue...
```

In this case, one of the two statements (`User found!` or `User not found!`) would always be displayed, and the other would be skipped. This type of structure is called an `if-else` structure.

Multiple Alternative

Sometimes you need more than two options in a selection structure. For example, a script might assign a student's letter grade based on the numeric result of an exam score. Every language has the ability to create a multiple-alternative structure, but each has its own syntax for doing so. In Python, such a structure is known as an `if-elif-else` structure. The code to assign a letter grade in Python is as follows:

```
1.  if score >= 90:
2.      print("Congratulations! You have a grade of A.")
3.  elif score >= 80:
4.      print("You have a grade of B.")
5.  elif score >= 70:
6.      print("You have a grade of C.")
7.  elif score >= 60:
8.      print("You have a grade of D.")
9.  else:
10.     print("You have a grade of F.")
11. continue...
```

NOTE The line numbers shown above and referenced in the information that follows are for clarity only. In a real program, there would be no line numbers.

The `if-elif-else` structure begins on line 1 and ends on line 10. It is assumed that a variable named `score` already holds a student's numeric score on the exam. In this code, the value of `score` is checked in a test condition. If it matches, the block of statements that follows that test condition is executed, and all the other code up to the end of the `if-elif-else` structure is skipped. If the first condition is not true, the second condition is tested. If that one is also not true, the third condition is tested, and so on. As soon as one condition is found to be true, that block of statements is executed, and any remaining conditions are skipped. In a multiple-alternative structure, only one block of statements is executed and all the others are skipped.

NOTE In Python, the indentation of various statements is important. Proper indentation tells the computer which statements are part of the various blocks of code. Other languages use other syntax to define blocks of statements in control structures.

You might wonder how this program works for a score of 96 or 78 or why it is not necessary to specify that a score of 84 must be less than 90 as well as greater than 80. Consider the logic of the program. Line 1 checks to see if `score` is greater than or equal to 90. This includes everything from 90 and above, including 96. If, however, `score` is less than 90, line 2 is skipped, and the value of `score` is tested on line 3. The only way the program can execute line 3 is if the test on line 1 fails. And that means `score` is less than 90, so there is no need to specify it in the code. If `score` is 62, the only way line 8 can be executed is if the tests on lines 1, 3, and 5 have failed, which means `score` is already known to be less than 70. If `score` is anything greater than or equal to 60, line 8 is executed. If it is not greater than or equal to 60, then `score` must be less than 60, so there is no need to specify that in the code. No matter what value `score` holds, only one block of statements will be executed and, regardless of what that block is, the program will continue on line 11.

Selection Structure Examples

Following are examples of how a multiple-alternative selection structure would be coded in several scripting languages. In each case, it is assumed that one variable (`num1`) holds the value of a number, and a second variable (`num2`) holds the value of another number. If the first number is greater than the second number, one message is displayed. If the first number is less than the second, a different message is displayed. If the two numbers are the same, a third message is displayed:

> **Python:**

```
if (num1 > num2):
    print(num1," is greater than ",num2)
elif (num1 < num2):
     print(num1," is less than ",num2)
else:
     print(num1," and ", num2 ," are the same")
```

> **JavaScript:**

```
if (num1 > num2) {
        console.log(num1 + " is greater than " + num2);
    }
    else if (num1 < num2)    {
        console.log(num1 + " is less than " + num2);
    }
       else
        console.log(num1 + " and " + num2 + " are equal");
```

> **Batch files:**

```
IF  %num1% GTR %num2% (
    ECHO %num1% is greater than %num2%
         ) ELSE IF %num1% LSS %num2% (
        ECHO %num1% is less than %num2%
        ) ELSE (
          ECHO %num1% and %num2% are the same
        )
```

> **Shell scripts:**

```
if [ $num1 -gt $num2 ]
 then
   set str="$num1 is greater than $num2"
   echo $str
 elif [ $num1 -lt $num2 ]
```

```
then
   set str="$num1 is less than $num2"
   echo $str
else
  set str="$num1 and $num2 are the same"
     echo $str
```

NOTE In a shell script comparison, every conditional expression must be placed inside square brackets with spaces around the expression.

Compound Conditions and Logical Operators

In all the examples of selection structures shown so far, a single condition has been tested. However, it would be restrictive if you could test only one condition at a time. For example, you might want to test whether a computer is registered to a specific user *and* whether that user has a specific version of the operating system. In such a test, both conditions must be true in order for any statements that follow to be executed. You could test first to see if the user is the one you are looking for and then nest a second selection structure to test for the operating system version. Or you could use one of the **logical operators** to test both conditions in one statement. When you join two test conditions in a single statement, this is known as a **compound condition**.

The three logical operators that are most commonly used are `AND`, `OR`, and `NOT`. When comparing two expressions, the result of the comparison is always either `true` or `false` (as with relational operators):

- The `AND` **operator** returns `true` if and only if both expressions (conditions) are true.
- The `OR` **operator** returns `false` if and only if both expressions (conditions) are false. If either expression (condition) is true, then the `OR` operator returns `true`.
- The `NOT` **operator** simply flips the result of an expression. If an expression (condition) is true, it returns `false`, and if the expression (condition) is false, it returns `true`.

The following are some examples of compound conditions using the three logical operators:

- **Examples of the `AND` operator:** Given that `x = 15`, `y = 8`, `z = 2`,
  `(x > y) AND (x > z)` returns `true`; both conditions are true.
  `(x > y) AND (z > x)` returns `false`; one condition is false.
  `(x < y) AND (y > z)` returns `false`; one condition is false.
  `(x < y) AND (z > x)` returns `false`; both conditions are false.
- **Examples of the `OR` operator:** Given that `x = 15`, `y = 8`, `z = 2`,
  `(x > y) OR (x > z)` returns `true`; both conditions are true.
  `(x > y) OR (z > x)` returns `true`; at least one condition is true.
  `(x < y) OR (y > z)` returns `true`; at least one condition is true.
  `(x < y) OR (z > x)` returns `false`; both conditions are false.
- **Examples of the `NOT` operator:** Given that `x = 15`, `y = 8`, `z = 2`,
  `NOT(x > y)` returns `false` because the condition is true.
  `NOT(z > x)` returns `true` because the condition is false.

Combining expressions that use relational operators with logical operators allows you to test many conditions in a single statement.

Loops: The Repetition Structure

The last control structure is called a *repetition structure*, or a **loop**. A loop contains a block of statements that are executed repeatedly. Each time a loop executes its block of statements is called an

iteration. In most programming languages, there are various types of loops, but not all of them are available in every scripting languages. A common type of loop is the `while` loop, which will be discussed first. The `for` loop, a shorthand method of writing `while` loops, is also discussed in detail.

The `while` Loop

A `while` **loop** begins with the keyword `while` and a test condition. If the condition is `true`, the loop will begin, and the block of statements in the loop will repeat until the condition is no longer `true`. This means that somewhere in that block of statements, something must change the condition, or the loop will repeat forever (an infinite loop). The general syntax for a `while` loop is as follows:

```
while (test condition) do:
    Block of statements to execute
         Update/change of the test condition
end while
```

Examples of `while` Loops

The following are examples of the syntax of `while` loops in several scripting languages. Each program counts by fives and displays the following results:

```
5  10  15  20  25  30  35  40  45  50
```

> **Python:**

```
x = 5
count = 1
while count < 11:
    print(count * x, end = "  ")
    count +=1
```

> **Shell scripts:**

```
x=5
count=1
while [ $count -lt 11 ]
do
    echo "expr $x\*$count  "
    count="expr $count + 1"
done
```

> **JavaScript:**

```
var x = 5;
var count = 1;
while (count < 11)    {
    console.log(count * x + "  ");
    count++;
}
```

> **Batch files:**

```
@echo off
setlocal EnableDelayedExpansion
SET /A x=5
SET /A count=1
SET /A limit=11
:while
```

```
        if !count! LSS !limit! (
           SET /A product = !x!*!count!
           ECHO | SET /P promptString="!product! "
           SET /A count=count + 1
           Goto :while
           )
    ECHO.
```

Note: Batch files do not have a `while` loop, but you can use other batch commands to write a script that closely mimics the logic of a `while` loop, as shown.

NOTE `setlocal EnableDelayedExpansion` and the use of `!` instead of `%` accounts for the way that batch files handle variables within loops.

NOTE `/A` is a switch that is used if a value needs to be numeric.

NOTE `ECHO|SET /P` prints the result without a linefeed. `ECHO` prints a linefeed after the last product.

The `for` Loop

Most often a loop is used to repeat a block of instructions a given number of times. For example, in the `while` loop shown earlier in this chapter, you know you want the loop to repeat 10 times. However, you may not always know how many times the loop should repeat. For example, imagine that you want to check each file in various directories to see how many files are over a certain size. The number of files in each directory to be checked would probably not be known. Most scripting languages have a type of loop known as a `for` **loop** to handle such situations.

A traditional `for` loop is, in effect, a shorthand way to write a `while` loop. The general syntax is as follows:

```
for variable=value; test condition; variable increment/decrement
{
        Several statements in a block to execute
}
```

In this type of loop, you initialize a variable first—a statement that is generally done *before* entering a `while` loop. Then you set up a test condition, as you would in a `while` loop. Finally, you increment or decrement the value of the variable. In a `while` loop, this is done within the block of statements. The JavaScript `for` loop version of the `while` loop shown above is as follows:

```
var x = 5;
    for (count = 1; count < 11; count++)    {
        console.log(count * x + "  ");
    }
```

A `for` loop is sometimes referred to as a *collection-controlled loop*. In such a loop, you identify the item to be tested, the collection of items, and, at the same time, the initial value, the ending value, and how much to increment or decrement the item. The general syntax for this type of `for` loop is as follows:

```
for variable in range(start, step, end) list do:
        Block of statements to execute
end loop
```

In most languages, one or more of the `start`, `step`, and `end` values are optional. If they are not specified, the computer will normally default to a value of `0` or `1` (depending on the type of collection) for `start`, default to a value of `+1` for `step`, and end at the end of the collection of items.

There are some variations on the `for` loop in most scripting languages that allow for more flexibility. The batch file example shown in the following section demonstrates how the `forfiles` loop (specific to batch files) makes solving the problem of checking all files in a directory easier than using a traditional `for` loop.

Examples of `for` Loops

Each of the following examples shows a loop that searches through a list of filenames in a directory and returns the date each file was last modified. Each of the scripting languages has specific functions that deal with the properties of files and directories, and some of them have other ways to automate this process. Note that "directory" represents the file path to a directory on the computer running the script.

> **Python:**

```
import time
import os
directory = 'C:\\users'
for file in os.listdir(directory):
    full_file_path = os.path.join(directory, file)
    print("modified: %s " %
        time.ctime(os.path.getmtime(full_file_path)))
```

> **Batch files:**

```
forfiles /C "cmd /c echo @file @fdate @ftime"
```

NOTE Batch files also have a `for` command, but for this particular situation, the `forfiles` command works better.

> **Shell scripts:**

```
for entry in "$directory"/*
do
modDate=$(stat-c%y "$entry")
modDate=${modDate%%*}
echo $entry:$modDate
```

> **JavaScript:**

```
for(var i = 0; i < files.length; i++)
{
  console.log(files[i] + "<br>");
}
```

NOTE This program is a little trickier in JavaScript. The example here is intended to show how a `for` loop is coded in JavaScript and will only display the names of the files without all the files' properties, including the date modified. As with many other scripting tasks, JavaScript is not the best language to use for this case.

A Brief Look at VBScript and PowerShell

The examples in the preceding sections demonstrate how scripts are written in Python, JavaScript, batch files, and shell scripting. Two other scripting tools are VBScript and PowerShell. While

VBScript is used exclusively with the Windows operating system, PowerShell can be used with Windows, Linux, Unix, and macOS.

VBScript

VBScript is a Microsoft scripting language that has some commands that are part of the Visual Basic programming language. It allows Windows system administrators to manage error handling, subroutines, and other processes managed by scripting languages. VBScript files have the extension `.vbs`.

However, VBScript is mainly used to allow functionality and interaction on web pages, and it is not supported by any modern browser. JavaScript is now used instead of VBScript on web pages. For use in managing system administration tasks, any of the other cross-platform languages or batch files are preferable.

PowerShell

PowerShell was originally created in 2006 by Microsoft as a task automation and configuration management framework for the Windows operating system. A decade later, in 2016, Microsoft released an open source cross-platform version of PowerShell. Windows PowerShell runs on the full .NET Framework, and the cross-platform version runs on the **.NET Core**. PowerShell script files are identified by the `.ps1` file extension.

In PowerShell, administrative tasks are generally performed by specialized .NET classes called **cmdlets**. There are more than 200 basic cmdlets. Each cmdlet implements a particular operation, and Microsoft provides help that includes an example of how to use each cmdlet.

Some of the core cmdlets are `Get-Location` to get the current directory, `Move-Item` to move a file to a different location, and `New-Item` to create a new file. You can also create PowerShell scripts to do tasks that are not covered by a cmdlet. A PowerShell script includes a combination of cmdlets and associated logic.

The `man` command is used to get help with PowerShell. Figure 15.15 shows the `man Get-Location` command output and syntax for the `Get-Location` cmdlet.

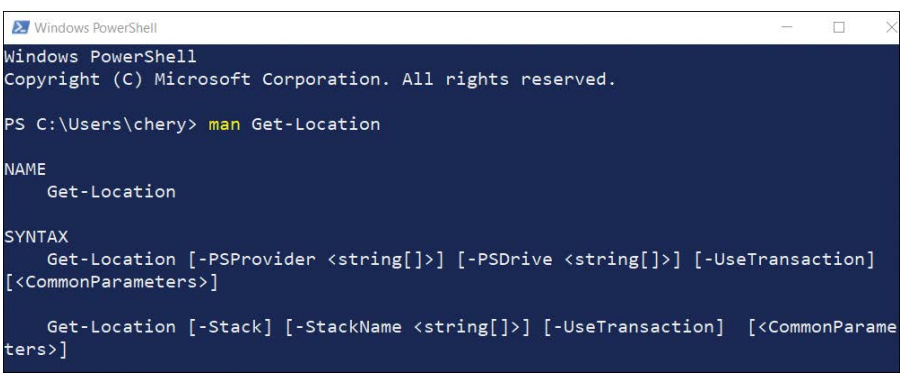


FIGURE 15.15 `Get-Location` cmdlet syntax

SOFT SKILLS: CHANGING PERSPECTIVE WHEN TROUBLESHOOTING

Troubleshooting is a hard topic to teach. Experience is the best way to learn how to tackle device problems, including problems with displays. In the classroom, teachers often rely on things going wrong during installation to teach troubleshooting. Also, broken machines can be used to encourage students to jump in and attempt repair. Changing your perspective is a great troubleshooting technique, although it's difficult to practice this technique in a classroom due to the pressure of time constraints.

When troubleshooting a problem, your perspective is that of a trained technician: You look at what is going wrong and determine what you know about that particular area that can cause the problem. Nothing is wrong with this perspective because it is a normal progression for a technician. But what happens when you are stuck or when you are faced with something you have never seen before?

One way you can change your perspective is to put yourself in the mindset of the user. Through talking with the user just a bit, you can get an idea of how the person thinks and works. Then you can try imagining the problem from that person's perspective. In addition to giving you troubleshooting ideas that you haven't thought of before, this will also make you more empathetic and help you become a better technician. See Figure 15.16.

FIGURE 15.16 See things from a new perspective

Another way to look at things from a different perspective is to imagine a great technician you know. Put yourself in that person's shoes. What would that technician try that you haven't thought of yet? What tricks have you seen tried in the past?

As technicians, we must constantly update and refine our skills because most of our day is spent troubleshooting. Perspective affects how we solve problems because it shapes how we approach problems and thus, how we approach the task of troubleshooting. Therefore, the ability to change perspective makes us better problem solvers (see Figure 15.17).

FIGURE 15.17 Changing perspectives

Chapter Summary

- Commands are used in two environments: (1) in a command prompt environment when the GUI tools do not or cannot correct a problem and (2) in a scripting environment to automate tasks such as deploying operating systems, installing updates, and restarting machines.
- Command switches alter the way a command performs or outputs information. Use *command* `/?` or `help` to receive help on any particular command.
- Important commands to know are `dir`, `cd`, `cd..`, `ipconfig`, `ping`, `tracert`, `netstat`, `nslookup`, `shutdown`, `dism`, `sfc`, `chkdsk`, `diskpart`, `taskkill`, `gpupdate`, `gpresult`, `format`, `copy`, `xcopy`, `robocopy`, `net use`, `net user`, `[command name] /?`, `msconfig`, `regedit`, `command`, `services.msc`, `mmc`, `mstsc`, `msinfo32`, `dxdiag`, and `whoami`.
- An environment variable describes the environment in which a program runs. In Windows, each environment variable has a name and a value. For example, the value can be the path to the program that is identified by the variable name.
- A script, for purposes of this chapter, is a small computer program designed to do a specific task. Common automation and configuration tasks include restarting machines, remapping network drives, installing applications, managing backups and updates, and gathering information. The ability to create and use scripts is valuable because scripts save time, ensure consistency in the execution of tasks, and allow for flexibility in responding to various conditions.
- Scripts can be written in many scripting languages. Some are designed for use on a single operating system, and others are cross-platform. While all scripting languages use the same logic to write a script for a given task, each language has its own unique and specific syntax. Scripting languages discussed in this chapter include batch files, shell scripts, VBScript, PowerShell, Python, and JavaScript.
- The building blocks of scripting include variables and data types. All scripts are written using three basic programming constructs: sequence, selection, and repetition.
- Technicians must troubleshoot a wide variety of issues. When you're working on a difficult problem, changing your perspective can help you find new ways to approach the problem.

A+ CERTIFICATION EXAM TIPS

- ✓ Be familiar with commands and how to work in the command prompt environment. The following commands are on the certification exam: navigation commands (`cd`, `cd..`, `dir`, `md`, `makedir`, `rd`, and `rmdir`) and the commands `chkdsk`, `copy`, `diskpart`, `dism`, `explorer`, `format`, `gpresult`, `gpupdate`, `hostname`, `ipconfig`, `mmc`, `msinfo32`, `mstsc`, `net use`, `net user`, `netstat`, `notepad`, `nslookup`, `pathping`, `ping`, `regedit`, `robocopy`, `services.msc`, `sfc`, `shutdown`, `taskkill`, `tracert`, `winver`, `whoami`, `xcopy`, and `[command name] /?`. You should also be familiar with commands that are available to someone with standard privileges vs. those that are available with administrative privileges. Practice these commands (and the various switches used with them) the week before taking the exam. Know when to use them. Consider what would be wrong that would force you to use a particular command.
- ✓ Be able to identify the program and file extension for each of the following script file types: batch files (`.bat`), PowerShell (`.ps1`), VBScript (`.vbs`), shell scripting (`.sh`), Python (`.py`), and JavaScript (`.js`).
- ✓ Understand and identify use cases for scripting. These include restarting machines, remapping network drives, installing applications, managing backups and updates, and gathering information.
- ✓ Understand unintended consequences of scripting.

Key Terms

`..` (navigation command), `.bat`, `.js`, .NET Core, `.ps1`, `.py`, `.sh`, `.vbs`, administrative privileges, alphanumeric character, `AND` operator, `attrib`, batch file, `cd`, `chkdsk`, cmdlet, `command`, command prompt, command switch, comments, comparison operator, compiled program, compound condition, construct, `copy`, decision structure, declaration, `defrag`, `del`, `dir`, directory, `diskpart`, `dism`, `dxdiag`, environment variable, equality operator, equals operator, `explorer`, floating-point number, `for` loop, `format`, `gpresult`, `gpupdate`, `help`, initialization, input, integer, interpreted program, `ipconfig`, iteration, JavaScript, keyword, logical operator, loop, loop structure, `md`, `mkdir`, `mmc`, `msconfig`, `msinfo32`, `mstsc`, `net`, `net use`, `net user`, `netstat`, `NOT` operator, `notepad`, `nslookup`, `OR` operator, output, `pathping`, `PATH` variable, `ping`, PowerShell, processing, Python, `rd`, `regedit`, relational operator, repetition, repetition structure, `rmdir`, `robocopy`, root directory, script, selection, sequence, `services.msc`, `sfc`, shell script, `shutdown`, standard privileges, string, subdirectory, syntax, `taskkill`, text file, `tracert`, `type`, variable, VBScript, `while` loop, `whoami`, wildcard, `winver`, `xcopy`

Review Questions

1. What command is used to create a directory?

   [`cd` | md | `dir` | `mad`]

2. What command is used to list the contents of a directory?

   _____

3. Consider the following directory structure from the `F:` drive root directory.

   `2019_Term` (directory)

   `CompRepair` (subdirectory)

   `Opsys` (subdirectory)

   `Cisco8` (subdirectory)

   `VoIP` (subdirectory)

   If the prompt is `C:\2019_Term>`, and you want to move into the `VoIP` subdirectory, what command do you type?

   a. `cd VoIP`

   b. `cd..`

   c. `cd C:\`

   d. `cd C:\VoIP`

4. The _____ and _____ file extensions are used with Windows executable files that are used to start applications.

   [`.app` | `.com` | `.exe` | `.js` | `.ps1`]

5. What command would be used on a computer where a specific application has stopped?

   [`quit` | `net stop` | `taskkill` | `stop`]

6. List one example of where you think a technician might see or use a batch file or a script file.

   _____

   _____

7. A script is created as a _____ file.

   [Word | csv | text | HTML]

8. A(n) _____ _____ tells a computer where to find a specific program.

   [batch file | environment variable | value variable | scripting language]

9. The two types of environment variables are _____ and _____.

   [experimental | external | internal | system | test | user]

10. The set of symbols and rules used to create instructions in a scripting language is its _____.

    [variable name | keywords | value | syntax]

11. What command would a technician use to apply a change to the security policy?

    [gpupdate | `mstsc` | `regedit` | `bootrec`]

12. The value of a variable is stored in the computer's memory as a specific _____.

    [integer | string | data type | ASCII code]

13. _____ are included in a script to explain what the script or a portion of the script does but are ignored by the computer when the script runs.

    [Comments | Variables | Commands | Syntax lines]

14. Which type of file would have the following command as part of it?

    `format d: /fs:ntfs /v:Corp /p:2`

    [`.py` | `.vbs` | `.js` | `.bat`]

15. To compare two expressions in a selection structure, you use _____ operators.

    [>= | logic | equals | relational]

16. The _____ operator returns `false` only if both sides of the expression are false.

    [`AND` | `OR` | `NOT` | `equals`]

17. A _____ structure contains a block of statements that is executed repeatedly.

    [decision | selection | repetition | sequence]

18. Two types of loops are _____ and _____ loops.

    [`continuous` | `decision` | `else` | `for` | `one time` | `while`]

19. The scripting languages that were developed by Microsoft are _____ and _____.

    [Basic | C | Java | PowerShell | VBScript]

20. A script that has the `.sh` extension is a _____ script and works on _____-based systems.

    [python, Apple | batch, Microsoft | shell, Unix/Linux | JavaScript, Windows]

21. The `.py` extension indicates that a script is written in the _____ language.

    [PowerShell | JavaScript | batch | Python]

Exercises

Exercise 15.1 Identifying Command-Line Commands

Objective: To recognize which command to use for a specific task

Procedure: Match each command to the appropriate task by writing the letter of the command beside the task that would use this command. Note that not all commands will be used.

Command:

a. `dir`	**f.** `robocopy`	**k.** `attrib`
b. `rd`	**g.** `md`	**l.** `sfc`
c. `del`	**h.** `gpresult`	**m.** `regedit`
d. `cd`	**i.** `type`	**n.** `tasklist`
e. `gpupdate`	**j.** `copy`	

Task:

_____ Copy a directory, its contents, all subdirectories, and attributes.
_____ Create a folder.
_____ Remove a file.
_____ Copy a file from one place to another.
_____ List all files in a particular directory.
_____ Delete a directory.
_____ Display the contents of a test or batch file.
_____ Verify and optionally repair operating system files.
_____ Move to a different directory.

Exercise 15.2 Scripting Concepts

Objective: To recognize terms related to scripting.

Procedure: Match each item to its description.

Item:

a. `.sh`	**e.** shell script
b. `.py`	**f.** PowerShell
c. `.bat`	**g.** string
d. loop	**h.** environment variable

Description:

_____ A variable that describes the environment in which a program runs
_____ A control structure used by a scripting language to write scripts
_____ The extension used by the Python language
_____ A data type that consists of alphanumeric characters
_____ The extension that identifies a batch file
_____ A script written for a Unix-based system
_____ The extension that identifies a shell script
_____ A Windows shell that was created to help with task automation and configuration management

Activities

Internet Discovery

Objective: Access the internet to obtain specific information regarding a computer or its associated parts

Parts: Computer with internet access

Procedure: Complete the following procedure and answer the accompanying questions.

1. Locate a website that has a specific usage for the `chkdsk` command.

_____

_____

2. Locate the Customize the Out of Box Experience (OOBE) page at https://learn.microsoft.com/en-us/windows-hardware/customize/desktop/customize-oobe-in-windows-11. List three customizations that you think would be useful in a business environment and explain why you think they would help the user.

_____

_____

3. Locate a website that provides a VBScript sample that could be used by a computer technician. Provide a basic description of what the script does and the URL where you found the answer.

_____

_____

4. You have been asked to add some user accounts to a domain, and the supervisor wants you to get some practice at the command line. Find a website that provides the command and specific instructions on how to use that command. Provide the command, one recommendation found on the website, and the URL of the website.

_____

_____

_____

_____

_____

5. Six scripting languages are described in the chapter. Locate a website that compares and contrasts the use of at least two of these languages. Document the URL. Briefly describe which language you would choose and explain why you made this choice.

_____

_____

_____

Soft Skills

Objective: To enhance and fine-tune a technician's ability to listen, communicate in both written and oral forms, and support people who use computers in a professional manner

Activities:

1. In a group environment, have each group member use a piece of paper or an index card to list two commands they'd like to learn how to use in specific situations. Use the internet to find reports from other technicians who have used these commands. Write what you have learned, paying special attention to any issues that were brought up. Share this information with your group. Consolidate ideas and present five of the best ideas to the class.
2. In a team environment, select two of the five ideas presented in Activity 1 to research further. Each team member should present a problem and its solution to the rest of the class. The class votes on the presentation that includes the most interesting and useful topic.
3. In a team environment, assign one scripting language to each member of the team. Each member should research the pros and cons of that language and present their findings to the group. Make a list of when each language should be used and its restrictions to present to the class.

Critical Thinking Skills

Objective: To analyze and evaluate information and to apply learned information to new or different situations

Activities:

1. Write a four-line batch file that does the following tasks:
   - Removes the path (`C:\Whatever`) shown on the screen.
   - Clears the screen.
   - Puts a message on the screen about what the batch file is doing.
   - Starts a particular application or opens a specific web browser.

   _____

   _____

   _____

   _____

   _____

2. Describe what you would do if you were hired for an IT position and asked to create a script.

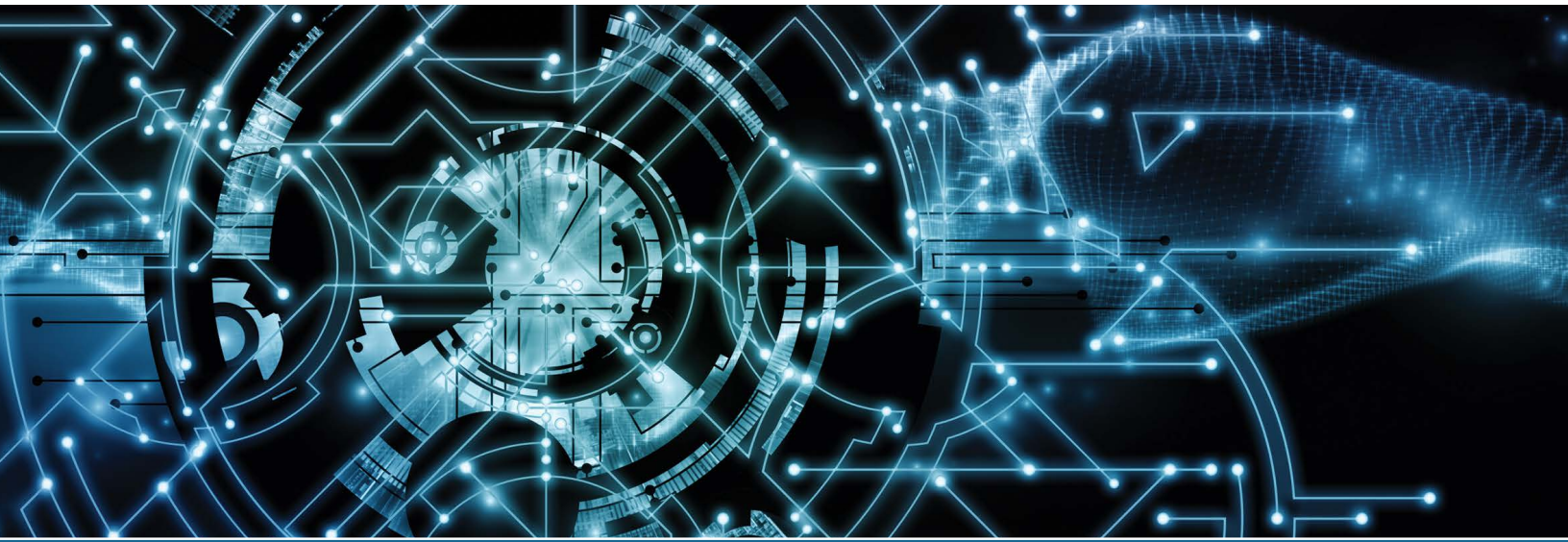
   _____

3. Describe what you would do if you were hired for an IT position and asked to display and modify the environment variable on a given system for a user-installed program.

   _____

This page intentionally left blank

16 Advanced Windows



In this chapter you will learn:

- To install, configure, and troubleshoot Windows
- To install hardware and software in the Windows environment
- To use various tools and features, such as System Restore, driver rollback, and WinRE
- To use basic security settings in the Windows environment
- To use the Control Panel utilities
- To implement the Windows boot process and troubleshoot boot problems
- To use the Computer Management console, Task Manager, and Event Viewer
- To back up and recover a Windows workstation
- How to avoid burnout in the IT field

CompTIA Exam Objectives:

- ✓ 1202-1.2 Given a scenario, perform OS installations and upgrades in a diverse environment.
- ✓ 1202-1.4 Given a scenario, use Microsoft Windows operating system features and tools.
- ✓ 1202-1.6 Given a scenario, configure Microsoft Windows settings.
- ✓ 1202-1.7 Given a scenario, configure Microsoft Windows networking features on a client/desktop.
- ✓ 1202-1.10 Given a scenario, install applications according to requirements.
- ✓ 1202-1.11 Given a scenario, install and configure cloud-based productivity tools.
- ✓ 1202-2.2 Given a scenario, configure and apply basic Microsoft Windows OS security settings.
- ✓ 1202-3.1 Given a scenario, troubleshoot common Windows OS issues.
- ✓ 1202-3.4 Given a scenario, troubleshoot common personal computer (PC) security issues.
- ✓ 1202-4.3 Given a scenario, implement workstation backup and recovery methods.

Advanced Windows Overview

Before we get into more technical issues related to Windows, let's go over some of the features you might not have heard of in Windows. Windows 10 comes in 32- and 64-bit versions, but Windows 11 is only available for 64-bit systems. Both Windows 10 and Windows 11 have different tiers available: Home, Professional (Pro), Pro for Workstations, Education, and Enterprise. Enhanced features, which depend on the version, include the following:

- **Side-by-side apps or windows:** It is possible to drag the top of a window to one side of the screen (until an outline of the window appears) to view windows or apps side by side. An alternative is to be in an active window and use ⊞+← or ⊞+→, depending on whether you want the active window pinned to the left side or the right side. Open another window and do the same for the opposite side, and the windows or apps are automatically equally sized.
- **OneDrive:** Microsoft's cloud storage allows files to be synced across multiple devices and accessible from a browser.
- **UAC (User Account Control):** You can get notifications of potential security issues before anything is added to or removed from the system.
- **Microsoft Store:** You can purchase and download apps from this store.
- **Multi-monitor taskbar:** This feature allows you to select where the taskbar apps show (All taskbars, Main taskbar and taskbar where window is open, or Taskbar where window is open.)
- **WinRE (Windows Recovery Environment):** You can use WinRE when things go wrong with Windows, such as when a system will not boot or operate properly.
- **Hyper-V:** This hypervisor runs virtual machines in Windows.

Preinstallation of Windows

Windows can be installed from either a central location using a network or locally using a flash drive or an external drive. The preinstallation of any operating system is more important than the installation. Technicians who grab a disc or just download and load a new operating system without going through a preparation process are asking for trouble. The operating system is a complex piece of software that is critical to the operation of all hardware and other software.

It is important to follow these steps before installing Windows:

Step 1. Determine whether the hardware is compatible.

Step 2. Decide whether the installation will be an upgrade or a clean install and which version of the operating system is to be loaded. Take into account software application compatibility.

Step 3. Decide whether the computer will have more than one operating system installed.

Step 4. Plan the partition/volume size and select the file system.

Step 5. Obtain any drivers, upgrades, or hardware replacements.

Step 6. Back up any data files.

Step 7. Scan for viruses, and then disable the virus protection during the installation process.

Step 8. Temporarily disable any power management or disk management tools.

Types of Installations

Windows can be installed for a variety of reasons, such as to have the latest features, to have a different operating system, to repair a system that doesn't boot, or to speed up a slow-performing operating system. Table 16.1 summarizes the various types of installations.

TABLE 16.1 Windows installation types

Installation type	Description
Clean install	An installation of an operating system when no other operating system is present.
Reset/restore	A reinstallation (reset) of Windows that gives you the option to keep your personal files (apps and settings are removed) or a restoration (restore) that brings Windows back to a previous state, such as to a time before a recent update was applied.
In-place upgrade	An upgrade of an existing operating system where the user keeps settings and files, such as moving from Windows 10 to 11.
Repair installation	Replacement of the Windows operating system when files have been corrupted or the system won't boot properly.
Recovery partition	Sometimes called a **factory recovery partition**, an area that contains the operating system and applications that came with the system when it was purchased.
Multiboot	Two or more operating systems on the same system; make sure you load the oldest operating system first.
Image deployment	Installation using a system image, which is a single file that contains a preconfigured version of the Windows operating system. The image can include all the software, drivers, updates, and/or settings needed to run the target computer. The image and any required configuration files can be stored on a network share, a flash drive, or an external hard drive. After a separate boot image starts the target computer, the image installation can take place with no human interaction (zero touch) or some interaction (lite touch).
Zero-touch deployment	A method of installing Windows in which a script or answer file (usually custom prepared for a specific company) is used. This configuration file contains settings such as the target partition, partition size, domain name, computer hostname, and required applications. Since no human interaction is required for the installation, this is sometimes called an **unattended installation** or zero touch installation (ZTI).
Remote network installation	An installation in which an image on a server or network share is deployed to a computer over a network. Because the network bandwidth is affected, this type of installation may interfere with normal business operations. For this reason, remote installations are commonly done during light network usage time or during off hours.

In-Place Upgrade or Clean Install

The first decision to make when planning to install an operating system is whether to upgrade from an existing operating system or perform a clean install. An upgrade (or in-place upgrade) occurs when a computer already has an older operating system on it, and a newer operating system is being installed. A clean install involves putting an operating system on a system that does not have one or removing the existing operating system in order to install a new one. There are three reasons to perform a clean install:

> The computer does not already have an operating system installed.
> The current operating system is not upgradable to the desired Windows version.
> The current operating system is upgradable to a specific Windows version, but the existing files and applications are going to be reinstalled.

An in-place upgrade *usually* keeps a user's files and configuration settings intact, but upgrades always come with some risk. Therefore, critical files should be backed up and configuration settings should be documented prior to an upgrade. In addition, the technician needs to ensure that source files for existing applications are available.

It is not always possible to do an in-place upgrade from one operating system to another. For example, it is possible to do an in-place upgrade from Windows 7 or Window 8.1 to Windows 10 but not to Windows 11. Going from Windows 7/8.1 to Windows 11 requires a clean install. To make sure an upgrade is possible, consult the documentation for the version of Windows you want to upgrade to and know which version of Windows you currently have installed. Figure 16.1 shows how to use the *Settings* > *About* option to see what version is currently installed. The System Information window (`msinfo32.exe`) also provides this data, along with other details about software and hardware configuration. Table 16.2 shows the upgrade paths for Windows 8.1 to Windows 10. Upgrading from Windows 10 to Windows 11 is discussed in the next section.

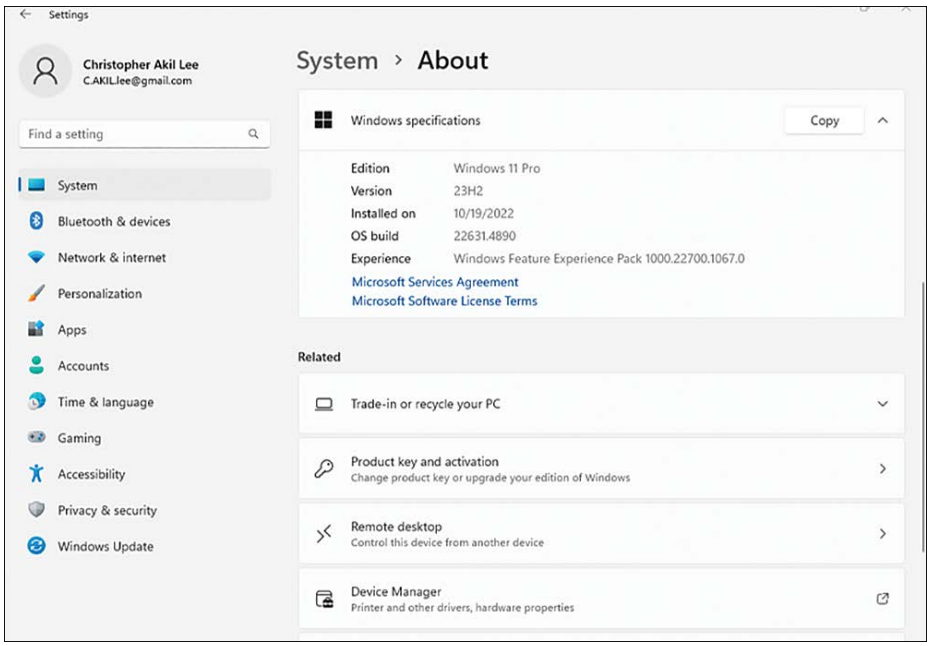


FIGURE 16.1 Windows About section of Settings: current Windows version

TABLE 16.2 Windows 10/11 upgrade paths

Original operating system	Upgrade to possibilities
Windows 8.1 Home	Windows 10 Home, Pro, Pro Education, and Education
Windows 8.1 Pro	Windows 10 Pro, Pro Education, Education, and Enterprise
Windows 8.1 Enterprise	Windows 10 Education and Enterprise
Windows 10/11 Home	Windows 10/11 Education, Pro for Workstations, Enterprise, Pro Education
Windows 10/11 Pro	Windows 10/11 Pro, Education, Pro for Workstations, Enterprise, Pro Education
Windows 10/11 Enterprise/Pro Education	Windows 10/11 Education

When you decide to upgrade, you must take into account which operating system is installed, what hardware is installed, what applications are being used, and whether those applications are compatible with the new operating system (see Figure 16.2). When Windows is installed as an upgrade, the user's applications and data are preserved if the operating system is installed in the same folder as the original operating system (normally `C:\Windows`). If Windows is installed in a different folder than the original operating system, then all applications must be reinstalled.

FIGURE 16.2 Applications are affected by an OS upgrade

Windows Update Assistant/Installation Assistant

The Windows Update Assistant application should be used before upgrading a version of Windows 8.1 or Windows 10. Update Assistant can be downloaded, installed, and executed to see whether a Windows 8.1 or 10 computer can function well with a higher version of Windows 10. At the time of this writing, the Update Assistant was available at https://www.microsoft.com/en-us/software-download/windows10. The Windows 11 Installation Assistant (https://www.microsoft.com/software-download/windows11) performs the same check for Windows 11. Update Assistant/Installation Assistant checks hardware, connected devices, and existing applications, and it makes recommendations before an upgrade. If everything is compatible, the tools can download the installation files from Microsoft and begin the installation process. Before you run Update Assistant/Installation Assistant, connect all hardware peripherals that are commonly used with the system.

In order to take advantage of Windows reliability, enhancements, and security features, sometimes a clean installation is the best choice. However, a clean installation involves formatting the hard drive, so the user's data (files and folders), applications, and configuration settings are destroyed. As with an upgrade, critical files should be backed up, and configuration settings should be documented prior to a clean installation. In addition, the technician needs to ensure that source files for existing applications are available.

TECH TIP

OEM OS cannot go to another computer

An original equipment manufacturer (OEM) version of Windows that is sold as part of a computer sale is not transferable to another computer.

Even when Microsoft states that an in-place upgrade *can* be done, there is no guarantee that all applications and settings will work after the upgrade. In a corporate environment, if custom software is involved, contact the software developer for any known issues or test the software in a test environment before deploying corporate-wide. The information may be posted on the software developer's website. Also, the Windows Compatibility Cookbook (currently available at https://docs.microsoft.com/en-us/windows/compatibility/windows-10-introduction) contains detailed information regarding hardware and software compatibility for Windows 10. Similar information is available for Windows 11 at https://learn.microsoft.com/en-us/windows/compatibility/windows-11/testing-guidelines.

Installation Media

Installation media is the storage device that contains all the necessary files to install an operating system. You can download the Windows 10 media creation tool from https://www.microsoft.com/en-us/software-download/windows10. Visit https://www.microsoft.com/en-us/software-download/windows11 for the Windows 11 tool. The tool downloads the files from Microsoft and then allows you to create a bootable flash drive or an ISO file. An ISO file is a single file that contains all the files and folders of an optical disc, such as a CD or DVD. In this case, you'll create a file that contains all the files to install the operating system.

If you choose the flash drive (or optical drive) option, the tool will create the installation media right away. To install Windows from a flash drive, plug the flash drive into an available USB port and then change the BIOS/UEFI settings to boot from the flash drive. The installation process will start after the computer boots.

If you choose the ISO option, the media creation tool will store the ISO file on your hard drive. You can then use a software tool like Rufus or balenaEtcher to create a bootable flash drive from the ISO file. Another option is to create a custom image file for deployment over a network; this option is discussed later in this chapter.

USMT and PCmover Express

The User State Migration Tool (**USMT**) and PCmover Express are two options for migrating data when an in-place Windows upgrade is not supported. See Figure 16.3 for an example of data migration. IT staff use USMT to perform large deployments of Windows as it can perform automated copying of user accounts, user files, operating system settings, and application settings. This tool is used from a command line for more control and customized settings, including registry changes. The `scanstate.exe` and `loadstate.exe` commands are used to transfer file and user settings. USMT is freely available from Microsoft.

You can use PCmover Express for smaller deployments. This application, which was created by Microsoft's partner Laplink, is not free. PCmover Express can transfer files, settings, user profiles, and applications from one PC to another. The application must be installed on both computers. Previously, the Easy Transfer program was available for free from Microsoft; it performed the same functions for Windows operating systems up to Windows 8.

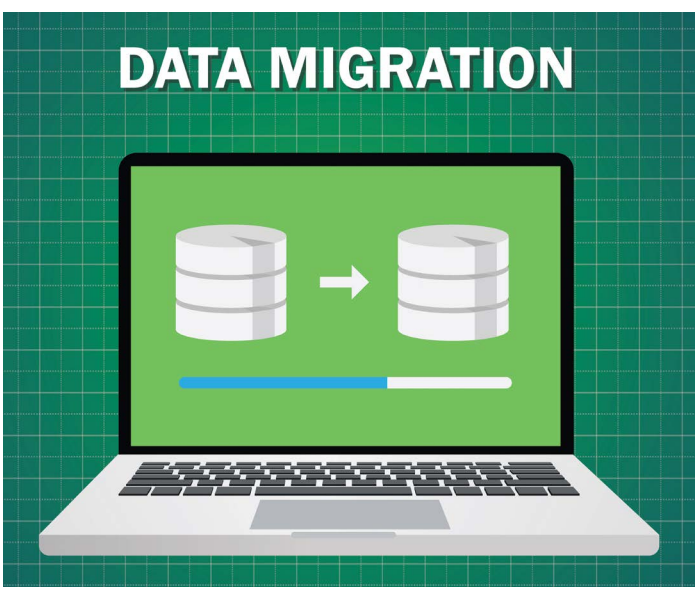


FIGURE 16.3 Local data migration

Compatibility Mode

While you're upgrading, keep in mind that not all 16- or 32-bit applications can be used in the 64-bit Windows environment. If a program seems to be incompatible, try the **compatibility mode**, which is available through the **Program Compatibility Troubleshooter**: Open the Control Panel and then locate the *Programs* section> *Programs and Features* section > *Run programs made for previous versions of windows* link.

Another way to manually configure compatibility settings for an application that was made to be compatible with an older Windows version is to find the executable file on the hard drive. You can find the executable via this process: Click the search for the application and right-click the application icon > select *Open file location*. After you find the executable file, right-click the file and select *Properties* > *Compatibility* tab > enable (check) the *Run this program in compatibility mode for* checkbox > use the drop-down menu to select the specific operating system > use the specific video and administrator options available in the *Settings* section > click *Apply* > click *OK*.

TECH TIP

Running a troublesome app in Windows 10/11

You can install an older operating system as a virtual machine in the Hyper-V hypervisor, which is included in Windows 10/11. You can then install and run an older application in the virtual machine.

Types of Partitions

Before the operating system can use a drive, it has to be partitioned and formatted. Partitioning allows you to divide a drive into multiple sections called partitions, or you can select the entire drive to be used as a single partition. The operating system will recognize each partition as a separate area in which to store data.

During formatting, you install a file system and assign a drive letter to each drive section. You are already familiar with the `C:` drive, where the operating system normally resides. Once a drive is partitioned, that section must be formatted for a particular type of file system, such as NTFS, exFAT, or FAT32. The file system determines how the operating system will save and retrieve data from the partitions. Table 16.3 reviews the types of partitions found in the Windows environment. During formatting in Windows, you have the option of doing a quick format or a full format. A **full format** identifies and marks bad sectors so they will not be used for data storage. A **quick format** skips this analysis.

TABLE 16.3 Windows partition types

Partition type	Description
Basic disk	The most common type of partition, which can contain primary partitions, extended partitions, and logical drives. Each primary partition and logical drive must be formatted for a specific file system.
Primary partition	A partition that can hold an operating system. If the operating system is used to boot the system, it must be on a primary partition that is configured as an active partition. A primary partition is assigned a drive letter and formatted for a specific file system.

Partition type	Description
Extended partition	A type of partition that allows hard drive subdivisions called **logical partitions**. Each logical partition (also called a logical drive) is assigned a drive letter and formatted for a specific file system. Extended partitions can only be used with basic disks. They cannot be used to boot the computer.
Dynamic disk	A more advanced type of disk volume that supports simple, spanned, striped, and RAID drive configuration.
MBR (master boot record partition table)	The traditional type of partition that uses primary and extended partitions.
GPT (GUID partition table)	A more advanced type of partition that requires a UEFI BIOS and allows partition sizes larger than 2 TB, improved protection of the partition table, and more partitions.
Swap partition	The Linux equivalent of a Windows paging file. Paging uses hard drive space as RAM so that programs that exceed the size of available physical memory can operate.

NOTE Use of the terms *master* and *slave* is ONLY in association with the official terminology used in industry specifications and standards and in no way diminishes Pearson's commitment to promoting diversity, equity, and inclusion and challenging, countering, and/or combating bias and stereotyping in the global population of the learners we serve.

File System Types

A file system determines how the operating system will save and retrieve data from the partitions. The most common Windows file systems are FAT16, FAT32, exFAT, and NTFS. The file system that can be used depends on what operating system is to be installed, whether the device is an internal or external device, and whether files are to be shared across a network. Table 16.4 lists file systems used with Windows and other operating systems. Keep in mind that once you go to a higher file system, you cannot go back to the lower file system.

TABLE 16.4 File system types

File system type	Description
FAT32	Supported with all versions of Windows. Commonly used with removable flash drives. Supports drives up to 2 TB. Can recognize volumes greater than 32 GB.
exFAT	Commonly called FAT64. A file system made for removable media (such as flash drives and SD cards) that extends drive size support up to 64 ZB (64 zettabytes, which equals 64 trillion gigabytes) in theory, although 512 TB is the recommended max. Made for copying large files such as disk images and media files. Supported by all versions of Windows.
NTFS	Microsoft's New Technology File System, used with Windows 7, 8, 10, and 11. Supports drives up to 16 EB (16 exabytes, which equals 16 billion gigabytes) but in practice is only 16 TB. NTFS allows faster file access and uses hard drive space more efficiently. Supports individual file compression and has the best Windows file security.

File system type	Description
ReFS	Resilient File System, Microsoft's newest file system, which is designed to maximize data availability, scale efficiently to large data sets, and provide data integrity with resiliency. Includes features such as proactive error correction to detect and repair data corruption. Intended for server-grade disks and supports partition sizes up to 35 PB (35 petabytes, which equals 35 million gigabytes). Cannot be used on a boot partition.
ext4	An update to **ext3** that allows for larger volumes and file sizes in Linux-based operating systems.

Planning Drive Space

The fourth step when planning to install Windows is to determine the size of the **drive partition** (also called the volume) and select the file system to be used. By default, an entire drive is used to create a partition; however, drives can be partitioned during the Windows installation process. One option is to place the operating system in one partition and place the data in a separate partition to make it easier to back up the data. Figure 16.4 shows this concept.

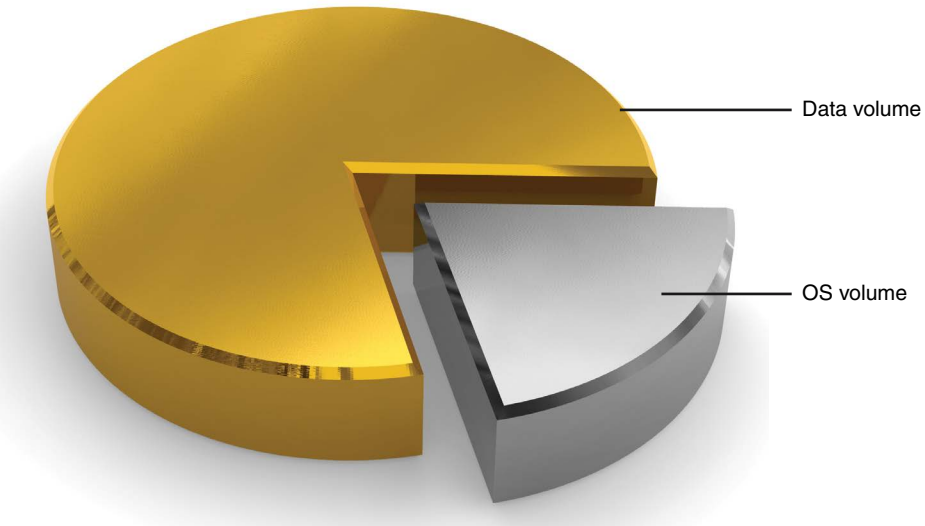


FIGURE 16.4 Partitioning (dividing) drive space during OS installation

Partitions are created and managed using the Disk Management tool. To access the tool, right-click the *Start* button and select *Disk Management*. Another method to access the tool is to type `diskmgmt.msc` at a prompt or in a search window. The Disk Management tool is covered in more detail later in the chapter.

The partition must be formatted to use a file system before the operating system can be installed. The file system for Windows 10/11 should be NTFS for the following reasons:

> It provides security (because individual files can be protected using permissions and encryption).
> It makes more efficient use of cluster space.
> It supports file compression.
> It supports larger hard drive partition sizes.
> It includes journaling, which helps in rebuilding the file system after a crash or power failure.

An issue that is relevant only when upgrading is whether to convert an old FAT16 or FAT32 hard drive partition to NTFS. Once a partition is converted to NTFS, the partition cannot be changed

back to FAT16 or FAT32. If you are unsure whether to convert a partition, leave it unchanged and later use the `convert` command to upgrade (without losing any data).

TECH TIP

Using the `convert` command

The `convert` command can be used to change a FAT16 or FAT32 partition to NTFS and keep the data from the old partition. Use `convert x: /fs:ntfs` (where `x:` is the drive to be converted to NTFS).

Hardware

The next step when planning to install Windows is to determine what computer hardware is installed. Table 16.5 lists the requirements for most Windows 10/11 installations. One thing that might influence your choice of Windows version is the amount of memory supported by the different flavors.

TABLE 16.5 Windows 10 hardware requirements

Component	Minimum
Processor	1 GHz
RAM	1 GB (32-bit)/2 GB (64-bit)
Graphics	Support for DirectX9 or higher with WDDM 1.0 driver
Hard drive space	16 GB (32-bit)/20 GB (64-bit)

Windows 11 has stricter hardware requirements than previous versions of Windows. For example, it only runs on 64-bit systems with two or more cores. See Table 16.6 for the other requirements. Your computer must meet these specifications in order for all the Windows 11 features to work correctly and for your computer to receive Microsoft updates. You can download the Windows 11 Installation Assistant to determine whether a computer's hardware is compatible. At the time of the writing, it's available at https://www.microsoft.com/software-download/windows11.

TABLE 16.6 Windows 11 hardware requirements

Parameter	Minimum Requirement
Processor	1 GHz or faster with two or more cores on a compatible 64-bit processor or System on a Chip (SoC)
RAM	4 GB
Storage	64 GB or larger storage device
System firmware	UEFI, Secure Boot capable
TPM	Trusted Platform Module (TPM) version 2.0
Graphics card	Compatible with DirectX 12 or later with WDDM 2.0 driver
Display	High-definition (720p) display that is greater than 9 inches diagonally, with 8 bits per color channel
Internet connection and Microsoft account	Windows 11 Home edition requires internet connectivity and a Microsoft account.

Drivers

Once hardware has been verified, you might have to obtain hardware device drivers specific to the operating system from the hardware manufacturer's website so that you can **load alternate third-party drivers** when necessary. That's because sometimes, a hardware device may have to be upgraded or replaced to work with the newer operating system. Also, older drivers for existing hardware often do not work properly or do not work at all when the new OS is installed. This is the cost of going to a more powerful operating system. Given the complexity of an upgrade, the customer could decide to buy a computer with the desired version of Windows already installed instead of upgrading their existing computer.

Drivers related to hard drives—for example, drivers for hardware RAID, motherboard AHCI mode, SATA hard drives, and hard drives over 2 TB—are especially critical to the installation process. Obtain any of these hard drive–related drivers *before* the installation, or you will not be able to install the operating system to that hard drive.

TECH TIP

If upgrading, ensure that Windows updates are current

If upgrading to a new version of Windows, ensure that the current version has the latest Windows updates.

Backing Up Before an OS Installation

The next step in planning to install Windows is one of the most important: In any upgrade, hardware change, or software change, you *must* back up the user data. Whether you do a clean install or an upgrade, if the user has data on the computer, it must be backed up before the installation process starts. Also, before backing up the data, remove any unwanted files and/or applications in order to free up hard drive space. To free up space in Windows 10, right-click on the drive letter in File Explorer and click *Properties*. On the *General* tab, click *Disk Cleanup* for a list of areas where files can be removed to free up disk space. In Windows 11, use *Settings* > *System* > *Storage* > *Cleanup recommendations*. Once the data is backed up from a Windows system, create a system image backup and a system repair disc.

Security Scan

The next step in planning for a Windows installation is to scan the system for viruses and malware (see Figure 16.5).

FIGURE 16.5 Do a security scan before an OS upgrade

TECH TIP

Antivirus software causes issues

Whether doing a clean install or an upgrade, disable the antivirus protection until after the installation. If possible, disconnect the computer from the network before disabling the antivirus software.

Disabling Interfering Software

The last step in the preinstallation checklist is to disable any power- or disk-management tools that are loaded. They can interfere with the new tools provided with Windows and can prevent an operating system from installing. Some security applications, including anti-malware and firewalls, can interfere with an operating system upgrade as well. Disable these utilities and applications before attempting an operating system installation or upgrade.

Installation/Upgrade of Windows

After completing all the preinstallation steps, you are ready to install Windows. The installation process is easy if you performed the preinstallation steps. The number one piece of advice to heed is to do your installation/upgrade research first. Doing so will greatly reduce the number of possible problems.

Basically, an installation involves three phases:

- In the first phase of an installation (sometimes called the Windows Preinstallation Environment, or Windows PE), the system requests a product key, the user selects a specific Windows edition and accepts the license terms, the user selects the upgrade option or the clean installation (custom) option, and the user selects a partition on which to install the operating system.
- After the user selects a partition, the second phase begins. During this process, setup files are copied from the installation media to the partition. The computer might reboot several times as the system detects hardware devices and installs the appropriate drivers.
- After the final reboot, the Windows Out-of-Box Experience (OOBE) begins. This phase is similar to what a user would see if they bought a new computer and started it for the first time. The user configures settings such as region, keyboard layout, and privacy settings. If the computer is already connected to the internet, the system prompts the user to create a new Microsoft account or log in to an existing account to access the computer. If the computer is not connected to the internet, the user creates a local account, password, and security questions. After the user answers all the questions, the computer saves the configurations and opens the Desktop; this might take several minutes.

You will probably have to set aside some time to allow the computer to receive and install updates issued since the operating system image/version you just installed was created. You may also have to install additional drivers and software apps that may not be part of the backup or image that was installed.

Part of the installation process is to select the type of network: public or private. Note that you can bypass the network configuration at this point during the installation of the operating system and configure it later. Wi-Fi networks in public places like restaurants and bookstores are usually unsecured. By default, your computer is not visible to other computers when the public network option is chosen.

Computers on private networks usually share information with each other, so they are normally visible to each other. There are two basic private types: workgroup or domain. (Table 16.7 describes the network types.) Large networks are usually organized as domains, in which all the user attributes (accounts, rights, and permissions) and computer settings are stored on a central server called a domain controller (or on multiple replicated domain controllers). Home networks and small business networks are usually organized as workgroups, where each user's account and rights are configured on each individual computer.

TABLE 16.7 Network types

Network type	Description
Public	The computer is hidden from other devices on the network, and sharing of resources is not permitted. This is the recommended network type for devices on unsecured networks, as in restaurants and coffee shops.
Workgroup	User accounts, rights, and permissions (such as file and printer permissions) must be configured on each individual computer. This type of network is usually suitable for home networks and small business networks (with 10 or fewer users or computers).
Domain	A domain is used in a corporate environment where users authenticate with a centralized user ID and password stored on a domain controller. Whatever machine the user goes to, the user ID and password are the same if the computer has been configured to be on the domain. Likewise, the individual computers' settings can be centrally stored. Every time a computer boots or restarts, it receives its settings from the domain controller.

Corporate Windows Deployment

Corporate computer installations are much more involved than any other type of deployment. Computers are installed in bulk instead of one at a time, as in a home or small business. The computers are frequently the same model and have the same software installed. Disk imaging is commonly used in the corporate environment to address these challenges.

An image can be created and deployed (copied) to multiple computers. Before a drive is copied, all the required programs, drivers, updates, and configurations are installed on the drive. Disk imaging software makes an exact copy (a binary copy) of the files loaded on the hard drive. The copy is stored on a flash drive, an external hard drive, an optical drive, or a network drive, to be deployed to other computers. When the image is copied to a target computer, the target has the exact operating system, drivers, update, and configurations as the original disk. When a computer has an issue, it is often faster to just **reimage** the computer than to troubleshoot the Windows problem.

Companies need automated installation tools to help with the corporate Windows image deployment process. Tools that can help with this are the Windows Assessment and Deployment Kit (Windows ADK), Windows System Preparation (Sysprep) tool, imaging software such as the Symantec GHOST program, Microsoft's Setup Manager, and Windows System Image Manager (SIM). Table 16.8 describes some of these tools.

TABLE 16.8 Corporate computer deployment tools

Tool	Description
Windows Assessment and Deployment Kit (Windows ADK)	The Windows ADK contains several components to customize Windows images for deployment to large networks. It also provides tools for testing systems prior to deployment.
Sysprep	When a prototype computer has Windows, Windows updates, all drivers, and applications installed, Sysprep can remove the security identifier (SID)—a unique number assigned to a computer by a network domain controller—as well as other unique information, such as the computer name or network domain. The computer is then imaged, and the image is deployed to other computers. A third-party utility such as Symantec Ghost Walker or Microsoft's `newsid.exe` can be used to reassign the SIDs after the drive image has been deployed.
SIM (System Image Manager)	SIM is used to create and configure answer files, install applications, apply service packs and updates to an image, and add device drivers. After the Windows `unattend.xml` answer file is created, you can use this file to answer the installation questions as the files are downloaded from a share or server on the network. SIM is part of the Windows ADK download.
WDS (Windows Deployment Services)	WDS is a server role that uses the corporate network(s) to deploy Windows-based operating systems, drivers, updates, and applications using a network-based installation.
MDT (Microsoft Deployment Toolkit)	MTD is a GUI shell that makes Windows deployment easier. Tools such as USMT, Application Compatibility Toolkit (ACT), Microsoft Assessment and Planning Toolkit (MAP), and the volume licensing application are inside the MDT shell.

When making a Windows image, you have to remove the unique identifiers from the computer—that is, computer name, security identifier (SID), network domain, and so on—before deploying the image to other computers. You must also reset or re-arm the Windows **activation clock** if a single activation key is used. If you do not do this, you are prompted for the Windows product key as soon as the computer boots. Re-arming the activation clock gives you a 90-day grace period before you have to re-enter the product key.

TECH TIP

Three re-arms with Windows

There is no limit to the number of times a computer can be reimaged, but there is a limit to how many times a computer can be re-armed, or have the Windows activation clock reset. You can use the Sysprep tool or the `slmgr -rearm` command to reset the re-arm count. To see how many times the computer has been re-armed, use the `slmgr /dlv` command.

When deploying Windows in an enterprise, licensing is handled a bit differently. A larger business buys a volume license key (VLK). Two other choices are MAK and KMS. With Multiple Activation Key (MAK), the internet or a phone call must be used to register one or more computers. This method has a limited number of activations, but more licenses can be purchased. The Key Management Service (**KMS**) method is used in companies with 25 or more computers to deploy.

TECH TIP

Be responsible

A technician is responsible for ensuring that any computer deployed has an antivirus application installed and that the application is configured to receive virus signature updates. Educate users about viruses and what to do if a computer gets one.

Verifying the Installation

In any upgrade or installation in both home and business environments, verification that the upgrade is successful is critical. After an upgrade has been done, verify that all applications still function. After a new installation has been completed, ensure that all installed hardware is detected by Device Manager (covered in the "Adding Devices" section, later in this chapter).

TECH TIP

Reinitialize antivirus software

If antivirus/anti-malware software was disabled through BIOS/UEFI or through an application, re-enable it after the operating system installation is complete. Verify that all settings are in accordance with the user requirements and departmental/organizational standards.

When you are satisfied that the installation is successful, don't forget to **apply updates** to the operating system, applications, and anti-malware software. You might also want to update device drivers to ensure the most up-to-date security and features for the installed hardware.

Troubleshooting a Windows Installation

Installation problems can be caused by a number of factors. The following are the most common causes of problems and their solutions:

- **No boot device available:** Access BIOS/UEFI settings and **update the boot order** so that the device that contains the operating system is listed first.
- **Incompatible hardware drivers:** Obtain drivers for the appropriate Windows version from the hardware manufacturer, if not Microsoft.
- **Incompatible applications:** Obtain upgrades from the software manufacturer, use the Program Compatibility Troubleshooter, configure a multiboot environment, or use virtualization.
- **Minimum hardware requirements not met:** Upgrade the hardware. The most likely things to check are the CPU and RAM.
- **Virus:** Run an antivirus program and remove the virus.
- **Antivirus software halting the installation/upgrade:** Disable the antivirus software through BIOS/UEFI and through the application. Restart the Windows installation and re-enable the antivirus software when the operating system installation is complete.
- **Preinstallation steps incomplete:** Go back through the list of steps.
- **Corrupt installation disc/USB drive or download (not as likely as the other causes):** Try the disc/drive in another machine and see if you can see the contents. If using an optical disc, check to see if a scratch or dirt is on the disc surface and clean the disc as necessary. Try another disc or drive. Redownload the operating system.

- **Incorrect registration key:** Type in the correct key to complete the installation. The key is located in an email or on the disc or disc case.
- **Windows installation process cannot find a hard drive:** This is most likely due to a SATA drive being used and a driver not being available for the controller. Download the driver, put it on a flash drive, or use a software program such as NTLite to create a custom installation disc that includes the downloaded driver.
- **STOP message when installing a multiboot system:** Boot from the Windows installation disc rather than the other operating system.
- **Blue screen of death (BSOD) during setup:** Check the BIOS/UEFI and hardware compatibility. Also, if an error message appears, research the error on the internet.
- **Incompatible BIOS:** Obtain and upgrade to a compatible BIOS/UEFI, replace the motherboard with one that has a compatible BIOS, or do not upgrade or install the higher Windows version.
- **BIOS upgrade needed:** Upgrade the BIOS/UEFI.
- **"NTLDR is Missing" error:** If you get an **NTLDR is Missing** error on a Windows computer during the installation process, try the clean install process over again.

TECH TIP

Installation halts

If an installation stops, try removing any nonessential hardware, such as network cards, modems, and USB devices and start the installation again. Reinstall the hardware after Windows is properly installed.

- **Message says that a device driver was unable to load:** Obtain the latest device drivers that are compatible and restart the setup program.
- **After upgrading Windows, the computer freezes:** Boot to Safe Mode and check Device Manager (covered in the "Adding Devices" section, later in this chapter) for errors. **Safe Mode** is a boot option that starts the computer with a minimal set of drivers. If no errors are present within Device Manager, disable the following devices (if present): video adapter, sound card, network card, USB devices and controller (unless using a USB keyboard/mouse), optical drive, modem, and unused ports. Enable each disabled device one at a time until the blue screen appears. When the problematic device is known, obtain the appropriate replacement driver. Another option is to try the tools in the Windows Recovery Environment (WinRE), which is discussed in detail later in this chapter.

Log files created during the Windows installation can be helpful for resolving installation issues. Table 16.9 outlines important log files for each version of Windows and briefly describes what they contain.

TABLE 16.9 Windows setup log files

Log file location	Description
`X:\Windows\setupapi.log`	Device and driver changes, **service pack**, and **hotfix** installations
`X:\$Windows.~BT\Sources\ Panther\setupact.log`	Setup actions performed during the installation
`X:\$Windows.~BT\Sources\Panther\setuperr.log`	Setup installation errors
`X:\$Windows.~BT\Sources\ Panther\PreGatherPnPList.log`	Initial capture of devices information

Log file location	Description
`X:\$Windows.~BT\Sources\Panther\miglog.xml`	User directory structure and SID information
`X:\Windows\Inf\setupapi*.log`	Plug-and-play devices and driver information
`X:\Windows\Inf\setupapi.app.log`	Application installation information
`X:\Windows\Panther\PostGatherPnPList.log`	Device information after the online configuration

System Restore

The **System Restore** program makes a snapshot image of the registry and backs up certain dynamic system files. Each snapshot is called a *restore point*. If a hardware or software installation causes a system not to boot or operate correctly, you can use the System Restore utility to return the system to an operable state so that you can retry the installation or determine a better method. You should create a restore point (covered below) soon after you install an operating system. Multiple restore points can be created on a computer; you can select which one to use when you are restoring the system. The program does not affect your email or personal data files.

System Restore requires the NTFS file system. Windows uses **Shadow Copy** technology, which employs a block-level image instead of monitoring certain files for file changes. Backup media can be optical discs, flash devices, other hard drives, and server storage (but not tape).

In Windows 10/11, System Restore is disabled by default. The *Settings* > *System* > *About* > *System protection* link is used to set up and configure System Restore, manage restore points, and manage the amount of disk space used for System Restore. You can manually create a restore point at any time. It is a good idea to create a restore point before performing an important upgrade or installation. A fixed amount of disk space is used for restore points. When a new restore point is created, the oldest one is removed automatically. System Restore is your number-one tool for solving problems within the operating system and registry.

To verify whether System Restore is on, use the following steps:

Step 1. Access the *Settings* > *System* > *About* > *System protection* link. The System Protection tab of the System Properties window opens.

Step 2. Look in the Protection Settings section to see if the system drive (C:) shows On in the Protection column.

If System Restore is turned off, you can use the following steps to turn it on:

Step 1. Access the *Settings* > *System* > *About* > *System protection* link. The System Protection tab of the System Properties window will open.

Step 2. In the Protection Settings section, locate and select the system drive (C:).

Step 3. Click Configure > enable the *Turn on system protection* radio button > set the amount of disk space to be used > OK.

Reloading Windows

Chapter 14, "Introduction to Operating Systems," has a section called "Recovering the Windows OS" that helps in a **no OS found** situation. This section provides a few more technical suggestions for such situations.

Sometimes it's necessary to do a *repair installation* (sometimes called an *in-place upgrade* or a *reinstallation*) of Windows, such as when Windows does not start normally, when it starts in Safe Mode, or when it has a registry corruption that cannot be solved with System Restore (covered earlier in this chapter). Hopefully the user has backed up existing data. The installation process should not disturb the data, but there is always a chance that it could.

Windows Resource Protection (**WRP**) protects operating system files, folders, and important registry keys, using access control lists (ACLs). An **ACL** is code that permits or denies changes to the operating system. Changes made to a monitored file or folder cannot be modified even by an **administrator** unless the administrator takes ownership and adds the appropriate access control entries (ACEs) within an ACL. Use the process described below to identify files that cannot be repaired by **System File Checker** (`sfc`) and replace them:

Step 1. **Find the corrupted files:** From an elevated command prompt, run the command `findstr /C:"[SR] Cannot repair member file" %windir%\logs\cbs\cbs. log>sfcdetails.txt`.

Step 2. **Read the list of files:** See Notepad or use the `edit` command to open the `sfcdetails.txt` file (normally located in the `C:\Windows\System32` folder). **Notepad**, as you learned in Chapter 15, "Introduction to Scripting," is a text editor that is handy for creating scripts and opening `.txt` or log files.

Step 3. **Take ownership of a file:** For each of the files listed in `sfcdetails.txt`, execute the command `takeown /f` *`filename_including_path`* (where *`filename_including_path`* is the full path and filename of the problematic file).

Step 4. **Change file permissions:** Run the command `icacls` *`filename_including_path`* `/grant administrators:m`.

Step 5. **Replace the file:** Use the `copy` command to replace the corrupted file with a known good one: `copy` *`source_filename destination_filename`* (where *`source_filename`* and *`destination_filename`* are the full path and file).

TECH TIP

Use `sfc` to solve system file problems

Use the `sfc /scannow` command as an administrator to replace any protected system files that have problems.

Windows has great tools that help with startup problems, such as a corrupt registry and missing or corrupt boot configuration files. These tools are covered later in this chapter.

TECH TIP

All existing system restore points are removed when Windows is reinstalled

The System Restore utility (covered earlier in this chapter) creates restore points that can be used to revert a Windows computer to a prior configuration. When Windows is reinstalled, no preexisting restore points are kept. Therefore, you should ensure that the System Restore utility is enabled and back up your data after Windows is reinstalled. You should also apply any service packs and patches after the reinstallation is complete.

Windows Updates

New vulnerabilities are found in every operating system almost daily. Windows makes available **Windows Update** and **Automatic Updates** for upgrading the operating system. Windows 10/11 does automatic updates by default. Microsoft provides updates according to a product's lifecycle. The Microsoft website provides support dates for the various Microsoft products.

To access the update settings in Windows 10, open *Settings* > select *Update and Security* > *Windows Update*. In Windows 11, open *Settings* > *Windows Update* (see Figure 16.6). Use these settings to pause updates, adjust active hours (times during which the system will not automatically restart after updates are applied), see your update history, and configure advanced options.

TECH TIP

Roll back Windows updates

When a Windows update causes a computer to not work properly, **roll back Windows updates** to at least one previous version. Note that you might have to do this from Safe Mode. To roll back updates in Windows 10, access the *Update and Security* setting > *Windows Update* > *View update history* > *Uninstall updates*. In Windows 11, go to *Windows Update* setting > *Update history* > *Uninstall updates*. You can also use the System Restore tool (covered earlier in this chapter) if the tool was enabled prior to the updates.

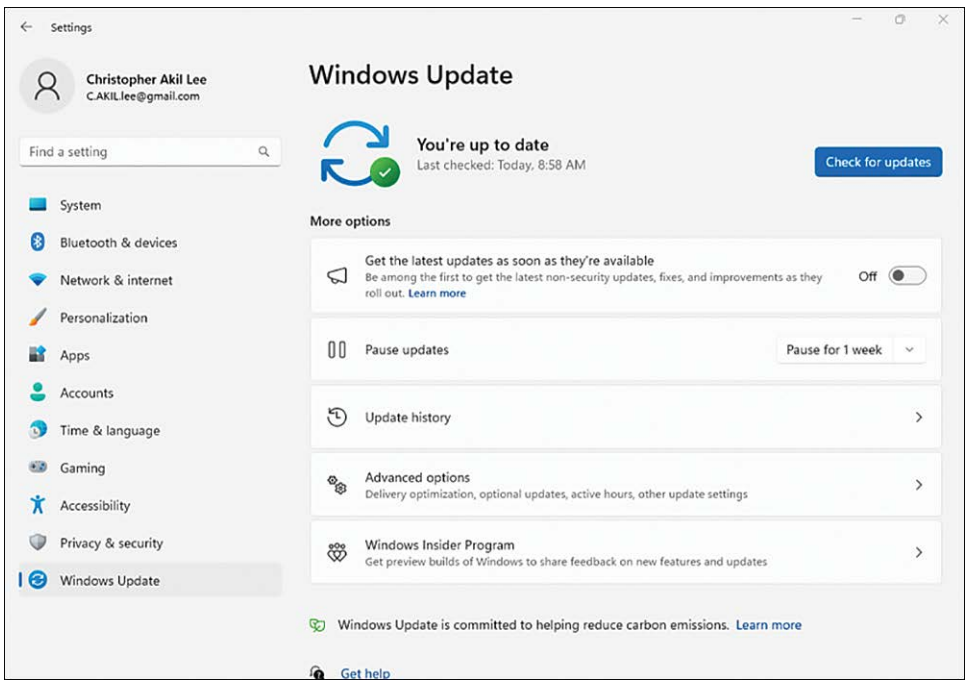


FIGURE 16.6 Windows Update options

The options to disable checking for updates and installing updates have been removed from the Windows Update utility. However, updates can be disabled via the registry or group policy. Automatic updates are often disabled in corporate environments so the system engineers can have more control over which updates are applied and when they are applied. Also, in large environments, updates are normally verified on test (development) computers before they are applied to the employees' (production) computers.

Figure 16.7 shows the advanced update options available, including whether to receive updates for other Microsoft products (such as the Microsoft Edge browser) at the same time as receiving operating system updates and the ability to download over a metered connection. By default, a Windows 10/11 device does not restart when the user is using the computer; however, the advanced options allow for restarting the computer as soon as possible (with a notice displayed prior to the restart). There are also options to show a notification when the computer needs to be restarted to finish updating and to pause updates for up to 35 days.

TECH TIP

You must be an administrator to change Windows Updates settings

You must be logged in as the administrator or as a user who is a member of the Administrators group in order to modify most Windows Update settings.

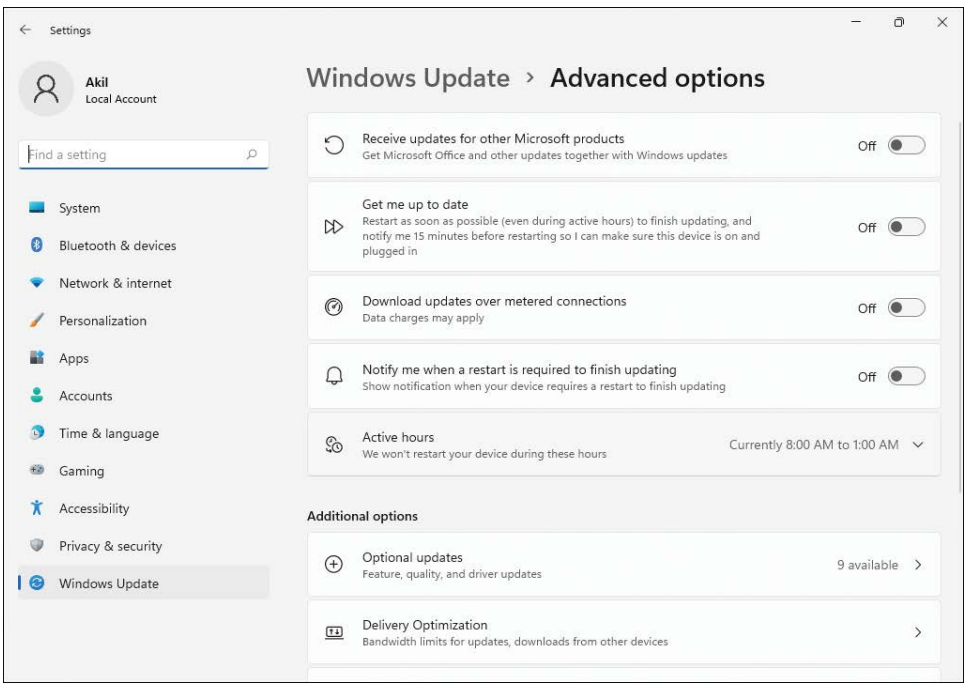


FIGURE 16.7 Advanced options for Windows Update

Backing Up the Windows Registry and Data

The **registry** is a database that contains information about the Windows environment, including installed hardware, installed software, and users. The registry should be backed up whenever a computer is fully functional, as well as before and after any software or hardware changes are made.

TECH TIP

Back up the registry

The registry should be backed up and restored on a working computer *before* disaster strikes. The time to learn how to restore the registry is not when the computer is down.

The registry can be backed up and restored in several different ways, including these:

> Using the `regedit` program
> Using the System Restore tool (covered earlier in this chapter)

The `regedit` program enables you to export the registry to a file that has the extension `.reg`. The file can be imported back into the computer if the computer fails.

Windows 10/11 uses File History backups (see Figure 16.8). **File History** enables you to back up only a specific user's libraries instead of the entire system. **File History** also allows you to schedule these backups. The feature can be accessed by opening *Control Panel* > *System and Security* > *File History*. In addition, the Windows Backup app (*Settings* > *Accounts* > *Windows backup*) can back up a user's folders, apps, settings, and credentials. The user must have a Microsoft OneDrive account in order to use Windows Backup.

Chapter 14 provides a thorough discussion of the other backup and recovery options available in Windows 10/11. A user would be best served by backing up the entire system (or at least the user's data) to an external drive and using one of the methods described in Chapter 14 to reinstall the operating system, as well as the user's data and preferences.

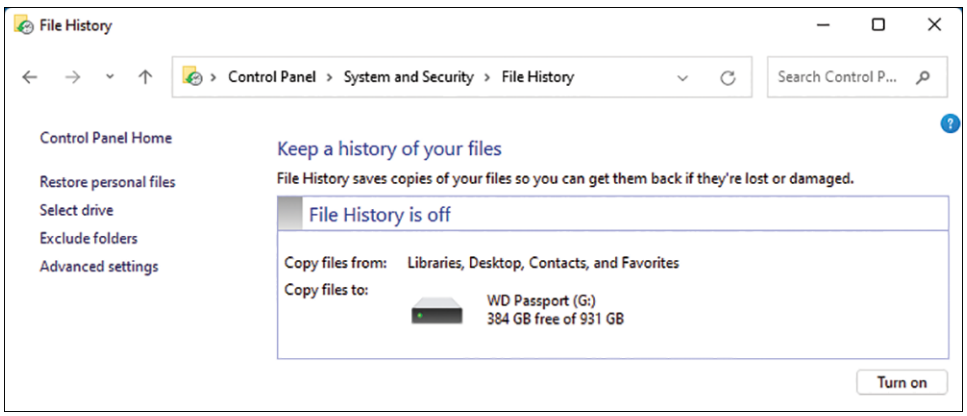


FIGURE 16.8 File History in Windows

TECH TIP

Who can use the Backup and Restore (Windows 7) program?

To use the Backup and Restore (Windows 7) program, you must be an administrator or have group rights to perform the backup.

To correct a problem with a computer's system files, registry, or booting, you may also restore from a **restore point**. A restore point is created by the System Restore utility (covered earlier in this chapter) any time a change is made to the system, such as when a program or driver is installed or a Windows update occurs. It is possible to revert to a restore point by opening the System Restore application when a change causes Windows to not operate properly or causes Windows to fail to boot. Note that System Restore must be enabled for restore points to be created.

Configuring Windows Overview

In Windows, technicians primarily use *Settings* to configure a computer. The Control Panel is the predecessor to Settings. Since Windows 10, Microsoft has been incrementally moving Control Panel utilities to the Settings app. See Figure 16.9 for the Windows 10 *Settings* home page and Figure 16.10 for the Windows 11 *Settings* home page. Technicians must know which Settings

category to use to change a computer's configuration. The options within each Settings category contain much of what is in the Control Panel utilities, but some functionality is still only available in Control Panel utilities. Windows has some configuration options that are unique to particular versions of the operating system. Several key utilities are explained in the following sections.

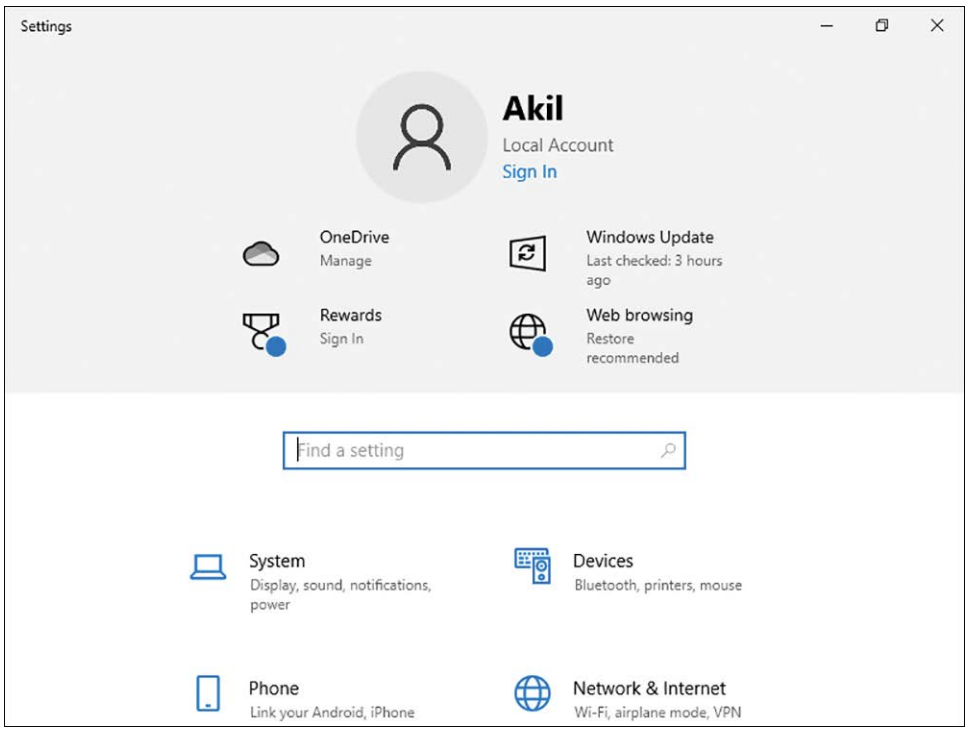


FIGURE 16.9 Settings in Windows 10

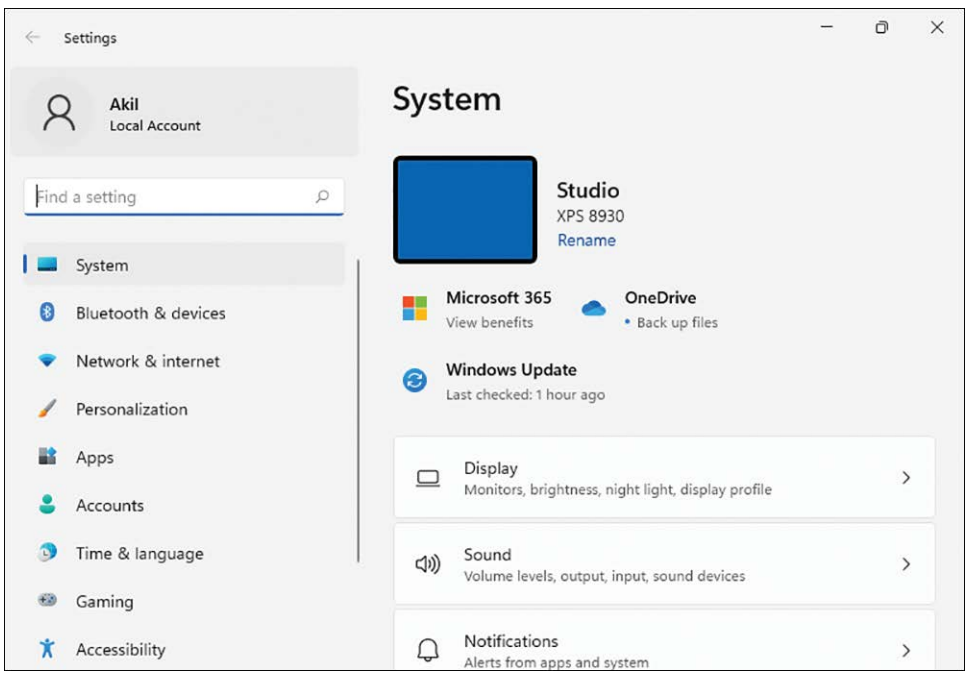


FIGURE 16.10 Settings in Windows 11

Configuring Windows

Technicians must frequently interact with the operating system when adding new hardware and software. Windows has specific tools for these functions. Using the correct procedure is essential for success. The following sections highlight tasks a technician commonly performs:

- Adding devices
- Removing hardware components
- Adding a printer
- Installing/removing software

Hardware devices are physical components that connect to the computer. A **device driver** is a piece of software that enables hardware to work with a specific operating system. Device drivers are operating system dependent. For example, a printer driver that works with Windows 10 may not work with Windows 11. Not all manufacturers provide updates for the newer operating systems. Some device drivers are automatically included with Windows and are updated continuously through Windows Updates. A technician must be aware of what hardware is installed on a system so that the latest compatible drivers can be downloaded and installed.

Adding Devices

Technicians are constantly adding devices to computers. Many devices today are plug-and-play, meaning they are designed to be automatically recognized by the operating system. Devices that attach via USB or Thunderbolt can be added or removed while the computer is powered on. Internal adapters (like PCIe video adapters) must be installed and removed with the computer powered off and the power cord removed. Let's investigate some of the Windows tools used when adding devices.

Device Manager

Devices that are recognized or at least sensed by the OS are shown in the **Device Manager** utility (see Figure 16.11). Device Manager (`devmgmt.msc`) is a technician's best friend when it comes to adding and troubleshooting devices on a Windows computer. After installing a new hardware device, use Device Manager to verify that Windows recognizes the device. Device Manager is also used to change or view hardware configuration settings, view and install device drivers, return (roll back) to a previous device driver version, disable/enable/uninstall devices, and print a summary of all hardware installed.

Once you expand a particular category, such as *Network adapters* (see Figure 16.11), you can look for symbols that indicate trouble. A down arrow beside an icon means the device is disabled. An exclamation point indicates a problem such as a resource conflict or driver issue.

To verify that a device is working properly, expand a Device Manager section. Double-click a device, and its *Properties* window appears. The *General* tab displays a message saying whether the device is working (according to Windows). The number of tabs a device has depends on the device. Figure 16.12 shows the *General* tab as well as the *Driver* tab for a USB mouse. The *Driver* tab shows the current driver version. It can be used to roll back the driver version if an updated driver does not function properly. The *Driver* tab can also be used to disable the device and uninstall the device driver.

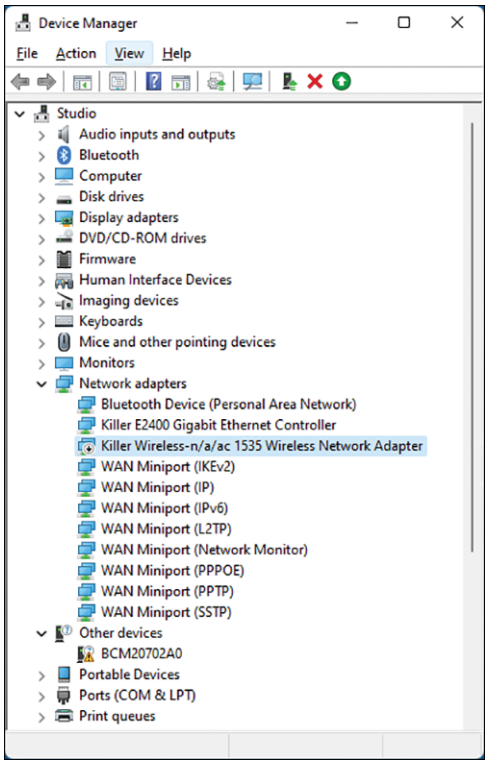


FIGURE 16.11 Device Manager in Windows

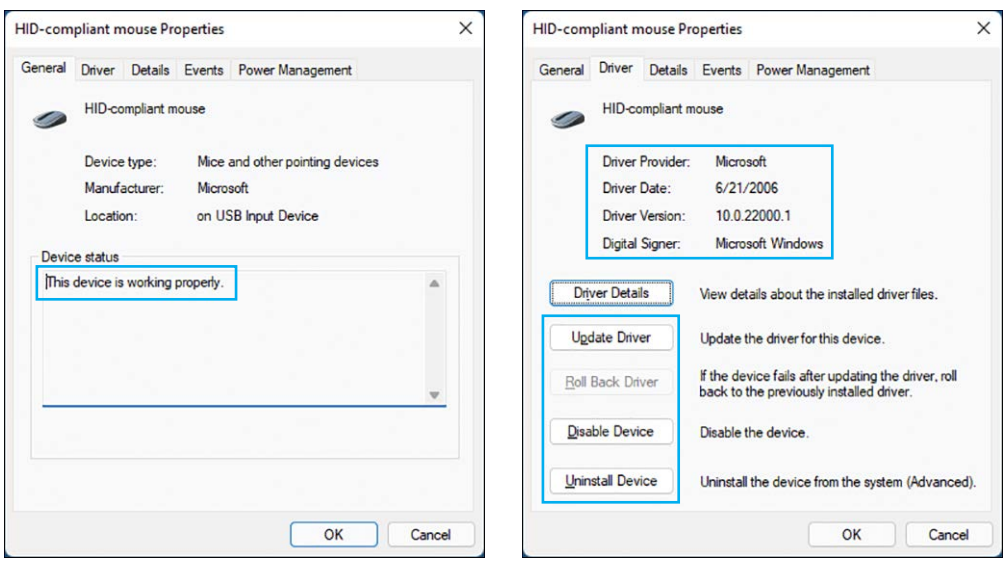


FIGURE 16.12 Device Manager > General and Driver tabs

There are two keys to a successful device installation:

> Obtaining the most up-to-date device driver for the specific installed operating system
> Following the directions provided by the device manufacturer

Windows autodetects when a new device is installed or connected and attempts to find the appropriate driver. Windows searches driver packages that are stored in an indexed database. The drivers are stored in the `Windows\System32\DriverStore\FileRepository` folder. All driver files that are not part of the operating system must be imported into this folder before the driver package can be installed. Drivers created for earlier Windows versions may need to be updated.

TECH TIP

Installing a device driver requires administrator rights

Remember that if the operating system cannot configure a device and it prompts for a device driver, you must have administrator rights to install the driver.

Some Windows device drivers use **digital signatures**; this is sometimes called driver signing or a requiring a signed driver. The digital signature confirms that the device driver for a particular piece of hardware has met certain criteria for WHQL (Windows Hardware Quality Labs) tests and is compatible with Windows. Digital signatures are required for 64-bit kernel mode drivers in Windows. Figure 16.13 illustrates this concept, and Figure 16.14 shows a signed driver in Device Manager. Notice the little certificate icon to the left of the driver.

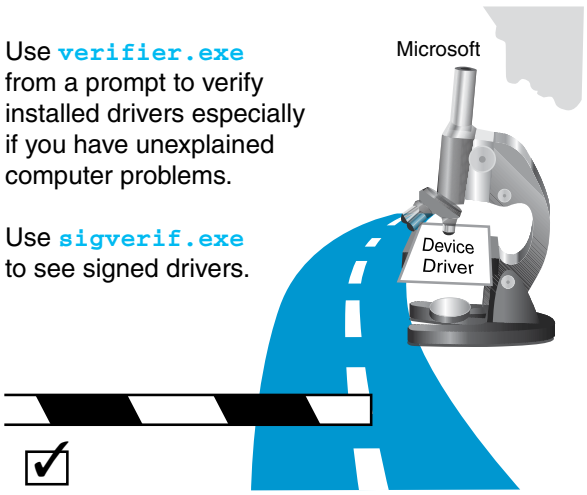


FIGURE 16.13 Signed drivers

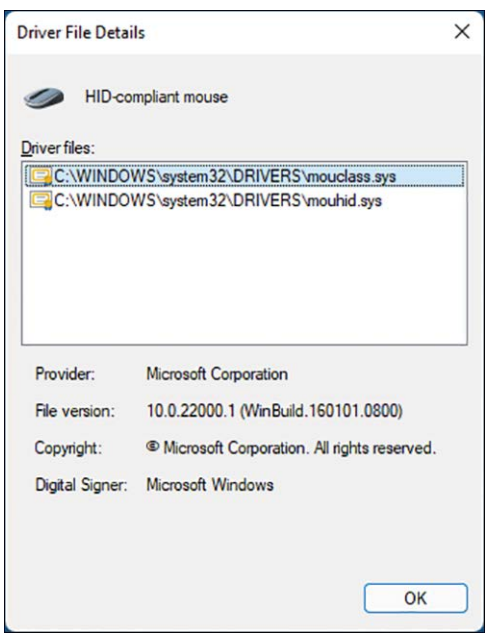


FIGURE 16.14 Signed driver in Device Manager

If you suspect that Windows is not booting because of an unsigned driver, access *Windows Recovery Environment (WinRE)* > *Troubleshoot* > *Advanced options* > *Startup Settings* > *Restart* > select the *Disable driver signature enforcement* option. The computer boots normally and not in Safe Mode.

To control the downloading of manufacturers' apps and custom icons, use the *System* setting > *About* > *Advanced system settings* link > *Hardware* tab > *Device Installation Settings* button. The options available follow:

- Yes (recommended)
- No (your device might not work as expected)

Bluetooth & Devices Settings Utility

The Bluetooth & Devices Settings utility is used to view, install, remove, and manage wired and wireless devices such as mice, multimedia devices, and speakers. When a device is added, Windows searches the Microsoft Store to see if there is an app from the device manufacturer. If an installed device isn't Detected, use the *Add device* option to initiate the process.

Audio Devices

Device Manager can also help when troubleshooting sound. Locate and expand the *Sound, video and game controllers* category. Verify that a sound card or integrated sound processor is shown (look for the words "audio device"). Right-click on the sound card > select *Properties*. Verify the device status on the *General* tab.

In Settings, the Sound utility is used to adjust volume output and manage sound-related devices, including speakers, headsets, microphones, and integrated audio devices. Select the *System* setting > *Sound.* Use the options in the *Output* section to configure and manage headsets and speakers. Use the *Input* section to view and manage the properties of microphones and headset microphones. The *More sound settings* option opens a window that provides other ways to manage speakers and microphones. The window also includes a *Sounds* tab to select a sound scheme and test particular sounds, as well as a *Communications* tab to filter unwanted sounds during phone calls. Refer to Chapter 8, "Video and Multimedia Devices," for sound troubleshooting tips.

Display Setting

The *Display* setting is used to adjust the size of text on the screen (without changing the resolution), to control and configure multiple monitors, to adjust the resolution, and to configure the refresh rate. To access the *Display* setting, you can open *Settings* > *System* > *Display* or you *right-click* a blank area of the desktop and then click *Display settings.*

Let's look at the most common settings:

- **Rearrange your displays:** If multiple displays are connected to the computer, a panel appears at the top of the *Display* window that allows you to rearrange them. The panel contains numbered rectangles. You might need to click *Detect* (which is listed under *Multiple displays*) to force the system to recognize older displays. When you click *Identify*, a number appears on each physical monitor so you can associate the rectangles with the displays. You can then drag the rectangles to match the physical layout of the actual displays. Click *Apply* after you rearrange the displays.

TECH TIP

Some displays don't appear in the *Display* setting

If multiple displays are connected to the computer, but they don't appear in the *Display* setting, make sure the correct drivers are installed for the display adapters and confirm that the adapters are enabled in *Device Manager*. Also, a motherboard may have a BIOS/UEFI setting that must be enabled for the motherboard to recognize multiple displays.

If you have multiple displays, you must select one in the display arrangement area to adjust the settings described below:

> **Display resolution: Resolution** is the number of pixels, shown as a *horizontal* × *vertical* number, such as 1,920×1,080. A display's native resolution is the best resolution that it could be set to.

> **Display orientation:** Orientation is the direction in which the display is rotated: landscape (horizontal) or portrait (vertical). Most displays are in the landscape orientation. There are also landscape/portrait (flipped) options for displays that are turned upside down, such as displays that are suspended from a ceiling.

> **Multiple displays:** For situations when multiple displays are connected to a computer, a drop-down allows you to show video output on only one display, duplicate video on multiple displays, or extend the output across multiple displays. If the *Extend desktop to this display* option is chosen, the system treats the individual displays as one big monitor (based on the layout in the display arrangement area), and different output can appear on the different monitors. For example, if Monitor 1 is to the left of Monitor 2, the cursor goes from Monitor 1 to Monitor 2 as the user moves the mouse from left to right. If Monitor 3 is above Monitor 1, the cursor travels from Monitor 3 to Monitor 1 as the user moves the mouse down. To choose the monitor where the taskbar appears, select a monitor in the arrangement area and then click *Make this my main display*. Click *Connect* to connect to a wireless display on your network.

TECH TIP

Show taskbar on all displays

The taskbar might appear on only one display when the *Extend desktop to this display* option is chosen. To show the taskbar on all displays, right-click the taskbar > *Taskbar settings*. In Windows 10, turn on *Show taskbar on all displays* in the *Multiple displays* section. In Windows 11, open *Taskbar behaviors* > *Show my taskbar on all displays*.

> **Advanced display:** This option is used to view the properties, memory, **refresh rate** (a value shown in hertz [Hz] that describes how many times a screen is redrawn in one second; note that the higher the refresh rate, the smaller the pixel/icon appears on the screen), and color settings such as the bit depth (the number of bits that control color, thus determining the maximum number of colors that can be displayed). Click *Display adapter properties for display* to access additional information and configure some settings.

Troubleshooting a Device That Does Not Work or That Is Not Detected

Use Device Manager to view installed hardware devices, to enable or disable devices, to troubleshoot a device, to view and/or change system resources such as IRQs and I/O addresses (see

Chapter 4, "Introduction to Configuration"), to update drivers, and to access the *Roll Back Driver* option. The *Roll Back Driver* option is available in all versions of Windows. When you roll back a device driver, the older driver can be reinstalled if you suspect that the new driver causes the device to not start, not be detected, or not work properly.

TECH TIP

Driver rollback requires administrator rights

You must have administrator rights to use the *Roll Back Driver* option in Device Manager.

To **roll back the device driver**, open *Device Manager* > expand the appropriate category > right-click on the hardware device > *Properties* > *Driver* tab > *Roll Back Driver* button > *OK*.

If the device driver has not been updated, driver rollback is not possible, so the *Roll Back Driver* button in Device Manager is disabled.

Sometimes Windows installs the wrong driver for an older device or adapter. The solution to this is to disable the device and then manually install it. To disable the driver in Device Manager, right-click the device icon and select *Disable*.

Drivers can be manually installed by running an installation program or by installing a driver installation package. A driver installation package usually includes a setup information file, which has the `.inf` extension. The setup information file contains the information needed to install a driver package on the computer. Follow these steps to manually install a device driver package through Device Manager:

Step 1. Obtain the driver package files and save them in a folder on your computer.

Step 2. Open the Device Manager utility.

Step 3. Expand categories as needed to locate the device for which the driver is to be installed. To display hidden devices in Device Manager, select *Show hidden devices* from the *View* menu option.

Step 4. Right-click the device name and select *Update driver*.

Step 5. Select *Browse my computer for drivers*, select *Let me pick from a list of available drivers on my computer*, and select *Have Disk*. Click the *Browse* button to locate the driver files that you saved in step 1. Click the `.inf` file that is designed to work with the device.

Step 6. Follow the dialogs to update the driver. If you are prompted with a warning about driver compatibility, you can click *No* and continue installing the driver. You can always remove it or roll back the driver if it does not install correctly or if it does not work.

If an `.inf` file cannot be found in a folder from your driver download, look in subfolders or other folders for the file. You could also download the driver again and pay attention to the name of the folder in which the driver is stored. If there are multiple `.inf` files in the folder, you may have to try them one at a time until you find the one that works with your hardware. Always **reboot** Windows after a driver installation, even if the system does not prompt for a reboot.

Driver installation programs usually have the extension `.exe`. They do not require *Device Manager*. When a driver installation program runs, it usually installs additional software or operating system features, in addition to the base driver files. For example, the driver installation program for a display adapter might install a custom feature to configure the adapter.

If you cannot install a device driver by using its installation program, you can try running the installation program in compatibility mode (using administrator credentials) or by manually installing it using Device Manager.

To run the driver installation program in compatibility mode, locate and right-click the executable file for the driver installation program. Select *Properties* > *Compatibility* tab > enable the *Run this program in compatibility mode for* checkbox > select a version of Windows that it is known to work on (see Figure 16.15) > click *OK*.

To use administrator credentials, locate the executable file used to start the driver installation process. Right-click its filename and select *Properties* > *Compatibility* tab > enable the *Run this program as an administrator* checkbox > click *OK*. After configuring the file to run in compatibility mode and to run with administrator credentials, double-click the executable file icon to start the installation process. Provide the administrator password, if required. Click *Continue*. Follow the normal installation instructions.

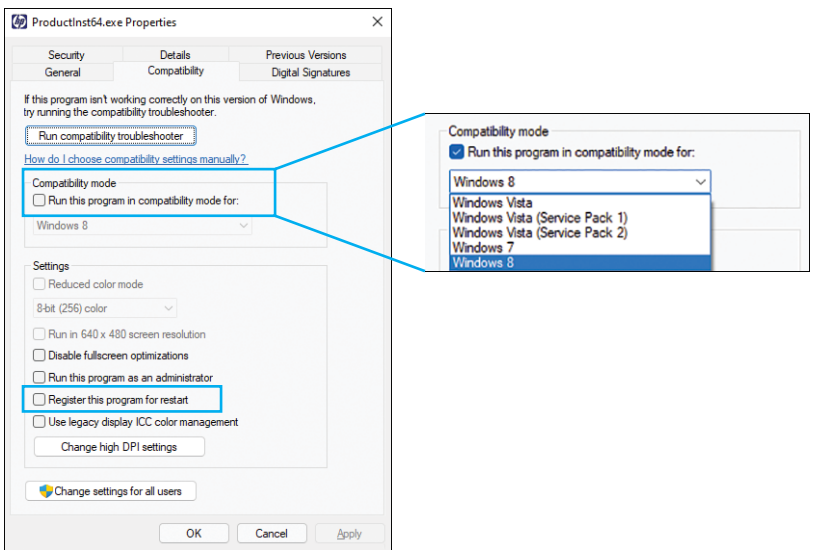


FIGURE 16.15 Installing a driver/application in compatibility mode

TECH TIP

Too many tray icons

To remove unused icons from the notification area in Windows 10, right-click on an empty space in the taskbar > *Taskbar settings* > *Select which icons appear on the taskbar* link. Alternatively, select *Turn system icons on or off* link > select *On* or *Off* as needed. In Windows 11, use *Taskbar settings* > *Choose which icons appear in the system tray* or *Other system tray icons*.

Not Enough USB Controller Resources

If you get the message "Not enough USB controller resources," you've probably exceeded the maximum number of endpoints for a USB controller or a specific port. USB endpoints are similar to lanes of data in PCIe. While USB 3.2 and USB4 are faster than USB 2.0, a USB 2.0 controller actually has twice as many endpoints. To resolve the error, try one of these solutions:

- Use USB 2.0 ports as much as possible, reserving USB 3.2 and USB4 ports for devices that benefit from the increased speed.
- Connect USB hubs to USB 2.0 ports instead of the faster ports, since the USB 2.0 controller will offer more endpoints to the hub's ports.
- Use Device Manager to uninstall and then reinstall the USB controller. Consider obtaining updated drivers.

- Disable the *xHCI Mode* option in UEFI/BIOS to turn off USB 3.2 or USB4.
- Run the *Hardware and Devices* troubleshooter: Run `msdt -id DeviceDiagnostic` from a command prompt > check *Advanced* > click *Next*.

Correcting Clock Drift

Synchronization, authentication, subscription, and logging issues can occur if a system's time is not correct. The system might even stop working altogether. Check these items to correct clock drift:

- Replace the CMOS/RTC battery on the motherboard.
- Set the time manually by right-clicking the time in the taskbar > *Adjust date and time* > turn off *Set time automatically* > *Change* (or *Sync now* if you have access to a time server).
- If using automatic synchronization, confirm the following:
  - Local network access or internet access to a time service is available.
  - *Set time automatically* is on (see the second bullet above).
  - *Set time zone automatically* is on or the correct time zone is selected.
  - *Adjust for daylight saving time automatically* is set appropriately for the computer's location.
  - The Windows Time Service is running in **Services**.

More Troubleshooting: Using Wizards and Troubleshooting Links

The Windows Troubleshooting Wizard can help you diagnose and/or repair a problem with a device, a software application, or a system utility. You can also configure troubleshooters to run automatically, and you can control the level of notification. In Windows 10, go to *Settings* > *Update and Security* > *Troubleshoot*. In Windows 11, use *Settings* > *System* > *Troubleshoot*. In either operating system, you can enter `troubleshoot` in the *Search* textbox; the troubleshooting tool appears first in the output list. In troubleshooting tool, select the appropriate option in *Recommended troubleshooters* (if any are listed) or click *Additional troubleshooters* (*Other troubleshooters* in Windows 11) to resolve common hardware and system issues.

Installing/Removing Software

Software makes a computer useful. One thing you should know about the newer Windows versions is that they may not support some of the older 16-bit software. If you have issues when running older applications, try the suggestions in the "Compatibility Mode" section, earlier in this chapter. Another option is to use the Hyper-V virtual environment to run older applications on older operating systems.

Most software today comes on a flash drive or is downloaded from the internet. An installation file often has the extension `.exe` or `.msi`. When the program is run, an installation wizard steps you through the process of installing the software. While most software today is 64-bit, older applications might be 32-bit. Table 16.10 shows common locations for 32- and 64-bit applications.

TABLE 16.10 Default locations for 32- and 64-bit files

Folder	Description
`System32`	Used for 64-bit Windows system files
`Program Files`	Used for 64-bit application files
`SysWOW64`	Used for 32-bit Windows system files (Note that the `WOW` in the folder name stands for Windows 32-bit on Windows 64-bit.)
`Program Files (x86)`	Used for 32-bit application files

The *Apps* section of *Settings* is used to uninstall and manage applications. This utility is also used to configure default programs for functions such checking email or opening websites.

TECH TIP

Launch an application

After an application is installed, launch the application by clicking the *Start* button > locate the application name and click it.

Before installing an application, you need to make sure the computer meets all **system requirements** (such as the minimum hardware and software requirements). You should look out for the following (keeping in mind that these concepts relate to all operating systems, including Windows, Linux, and macOS):

> **Compatibility:** Is the application compatible with the type of computer it is being installed on? Does it require a Windows, Mac, or Linux machine?

> **OS requirements:** Is the application 32-bit or 64-bit? If 64-bit, are you installing it on a 64-bit computer? If not, the application will not run.

> **Central processing unit (CPU) requirements:** In addition to system type (32-bit or 64-bit), some applications require specific levels of CPU features, such as clock speed, cache, threading, and number of cores.

> **RAM:** Does the computer have enough RAM for the application? Note that the minimum RAM might not provide the performance the customer wants.

> **Drive space:** Does the storage device that will be used to hold the application and files generated by the application have enough room? Do you need to remove some applications, delete unwanted files, or back up old files and delete them?

> **Dedicated graphics card vs. integrated:** An integrated graphics processor within the CPU handles video data quickly with reduced power consumption. However, a dedicated graphics card is required for most intensive graphical applications like CAD/CAM, video editing, and gaming. Furthermore, an integrated CPU shares RAM with the overall system, thus reducing the memory available for the operating system, applications, and documents.

> **Video random-access memory (VRAM) requirements:** VRAM is physical memory dedicated to graphics data. It can be located on a CPU or on a dedicated graphics card. Generally, the more VRAM available in a system, the more graphics data can be stored, especially 2-D and 3-D images.

> **External hardware tokens:** External hardware tokens (also called dongles) are often used to enhance system security. For example, a token can display a unique number that changes over time. A VPN application may require the user to enter that number along with their username and password in order to log in. Another type of token is a read-only USB device with an encrypted security certificate. The user must insert the device in the computer in order to log in.

Local methods of installing an application include using a flash drive or an optical disc, as well as installing an application that was downloaded from the internet. Software can also be installed via a network-based method, in which the application is installed from a shared folder on a network server.

One common type of downloaded software installation file is an ISO image. An ISO image is a single file that contains an exact copy of an optical disc, such as a CD. After the file is downloaded, you can double-click it to give it a drive letter and access the contents as if you had inserted an optical disc into the optical disc drive. This process is called *mounting*.

When installing an application, other considerations also have to be taken into account:

- What local security permissions need to be assigned? Chapter 18, "Computer and Network Security," covers how to make these assignments.
- Which files or folders are needed to install the application? Do the users need access to do it themselves, or does just the technician who will install it need access?
- What other security considerations are important? What impact does the application have on the computer or network?
- What other devices might be needed as a result of having access to this application? Is a printer, plotter, digitizer, second monitor, or some other device needed?
- What additional financial or personnel resources will be required to support the application? For example, will users contact the in-house IT department to address issues, or will they contact the vendor? How much does vendor support cost, and how long will it last?

Synchronization

Synchronization is the process of keeping things together or the same. Windows 10/11 has a **Sync Center** Control Panel utility that can be used to synchronize files with other computers and devices on the same network. After a file is selected for synchronization between two computers, if it changes on one computer, then the latest version of the file is put on the other computer. Even if a computer is not connected to the network, you can work on a synchronized file and then, when the computer connects, the file is updated (if it is not open). If the file is open on one machine and another computer is modifying the file, a conflict might occur. There is a *Resolve* option to help with this situation.

Windows 10/11 allows the syncing of files, apps, and user preferences through *Settings* > *Accounts* > *Windows backup*. These features require a Microsoft OneDrive cloud account. The user will have access to the same files, folders, apps, and preferences on all their synced devices. Synced preferences include the personalization settings, account passwords, language preferences, accessibility settings, Wi-Fi networks and passwords, and other Windows settings.

Apps & Features/Apps

The *Apps & Features* (*Apps* in Windows 11) Settings utility is used to change an application's options, uninstall an application, or view the installation date, size (disk space consumption), and version of a particular application.

Figure 16.16 shows a list of the currently installed applications on a Windows 11 computer. It also shows the *Advanced options*, *Move*, and *Uninstall* options for one of the programs. These options appear when you click the ellipses (three dots) to the right of the application size. *Advanced options* displays the app's specifications and allows you to change the program's functionality options or to repair, reset, or uninstall the program. *Move* allows you to change the drive on which the app is installed. The *Uninstall* option deletes the program from the computer. Not all programs have *Advanced options* or *Move*. Some programs have a *Modify* option. If you suspect that an installation has been corrupted, you can use *Modify* (if available) to repair the installation or uninstall the program.

Similar actions are available in *Control Panel* > *Programs and Features* (see Figure 16.17). *Apps & Features* also provides the *Turn Windows features on or off link*. Figure 16.18 shows the *Turn Windows features on or off* window. A check in a feature's checkbox means that feature is enabled. A cleared checkbox means that option is not turned on.

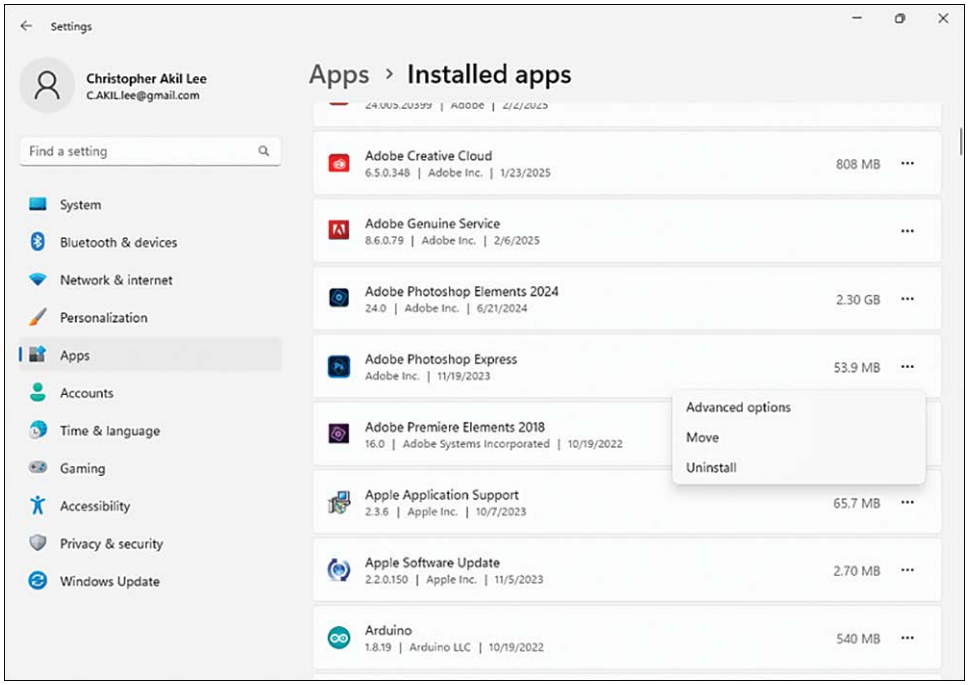


FIGURE 16.16 Apps Settings category > *Installed apps* window

TECH TIP

Handling application misbehavior

To **repair an application** that is not working or that is not working properly, click the ellipses for an application in *Settings* > *Apps* > *Installed Programs* > select *Modify*.

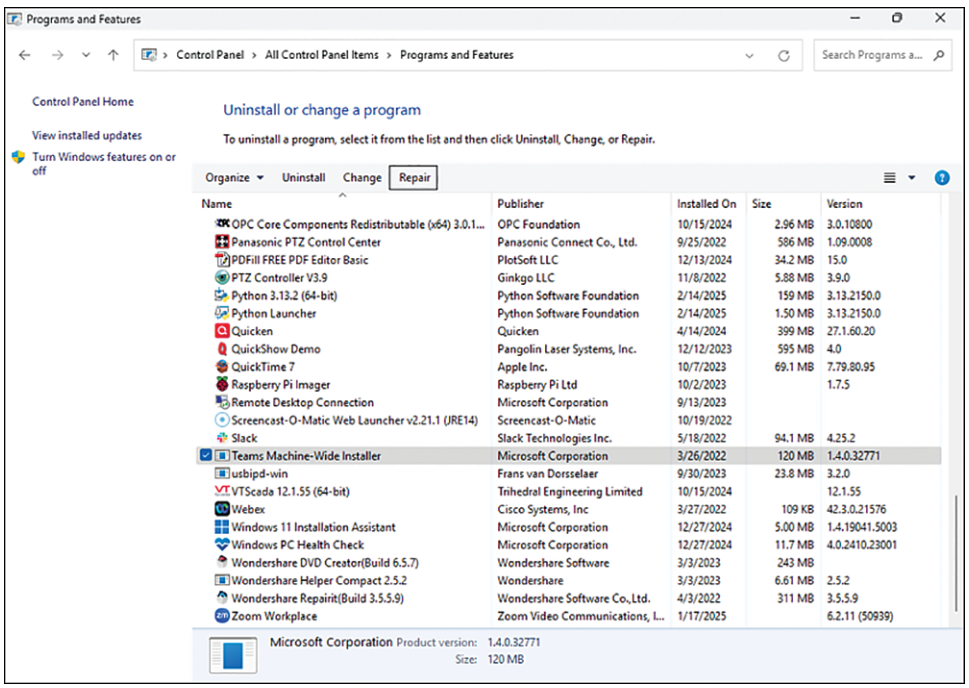


FIGURE 16.17 Programs and Features section of Control Panel

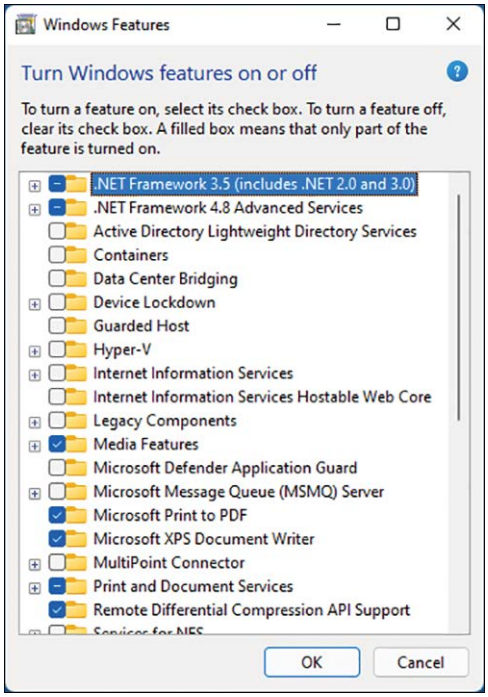


FIGURE 16.18 Programs and Features section of the Control Panel > Turn Windows features on or off window

Another software-related issue involves dynamic link libraries (DLLs). DLL files contain reusable code that can be used by multiple applications. A DLL must be registered with the Windows registry in order to function. Sometimes, DLL registry links get broken, and the links must be reestablished. You can use the following techniques to resolve DLL errors:

> Run the built-in System File Checker (`sfc`) to replace missing or corrupted operating system files.
> Repair or reinstall the software if an application reports a DLL error.
> Download Windows 10/11 operating system files from Microsoft.
> Copy the DLL file from another system and restore it on your PC. Then re-register the DLL file by using the `regsvr32.exe` command.

Computer Management Console

The **Microsoft Management Console** holds snap-ins, which are tools that are used to maintain a computer. Open this tool by using the `mmc` command or searching for `mmc` in the search textbox. You can then add snap-ins via *File* > *Add/Remove Snap-in.* After you add the snap-ins you need, you can save the customized console. Later, you can start the Microsoft Management Console and open a saved console by using the `mmc` *`path\filename`*`.msc` command.

The **Computer Management** console is a preconfigured console that provides a number of technical tools for an IT technician. The Computer Management console allows a technician to manage shared folders and drives, start and stop services, look at performance logs and system alerts, and access Device Manager to troubleshoot hardware problems. Access the Computer Management console by using one of the following methods:

> Right-click *Start* button > *Computer Management.*
> Use the search textbox to search for `computer management` or `compmgmt`.

> In Windows 10, *System and Security* category of the Control Panel > *Administrative Tools* > *Computer Management*.

> In Windows 11, *System and Security* category of the Control Panel > *Windows Tools* > *Computer Management*.

Figure 16.19 shows the Computer Management console. The three major tool categories in this console are System Tools, Storage, and Services and Applications. Expand the *System Tools* section to see some of the most technical utilities available to a technician. Expand the *Storage* section to find the Disk Management utility. The expanded *Services and Applications* section shows access to Services and Message Queuing; other items may appear this section, depending on the applications that have been installed on the computer.

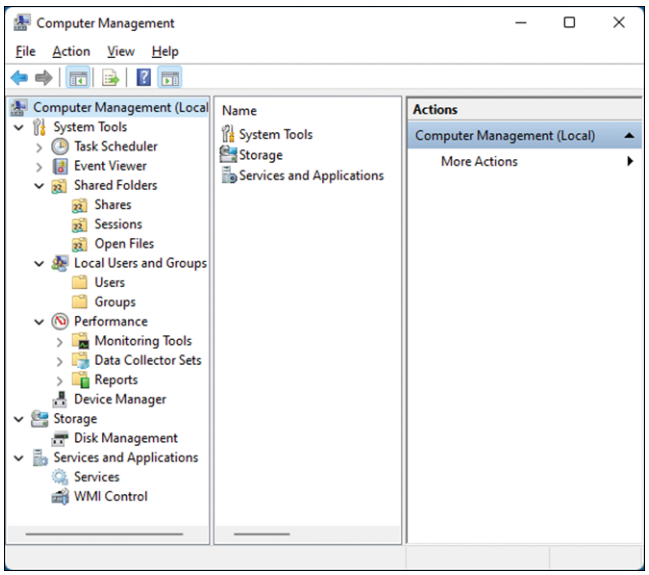


FIGURE 16.19 Computer Management console

TECH TIP

Using Component Services?

You can use the **Component Services** snap-in to view, configure, and administer Component Object Model (COM) components, COM+ applications, and Distribution Transaction Coordinator (DTC). COM applications are a group of components within applications that were designed to work together. When deployed, Component Services can be used to track services and assess performance measures.

System Tools

The *System Tools* section of the Computer Management console includes Task Scheduler, Event Viewer, Shared Folders, Local Users and Groups, Performance, and Device Manager. Each of these tools is important when supporting Windows computers. Let's dive into each one of them.

Task Scheduler

Task Scheduler (`taskschd.msc`) enables you to plan and execute apps, scripts, and utilities on a regular basis. Use the Actions pane to create a new task, show what tasks are running, and import a task from another machine (see Figure 16.20). If a company has an executable it wants to run at 2 a.m. every week on Wednesday or every time a user logs on, Task Scheduler is the tool to use.

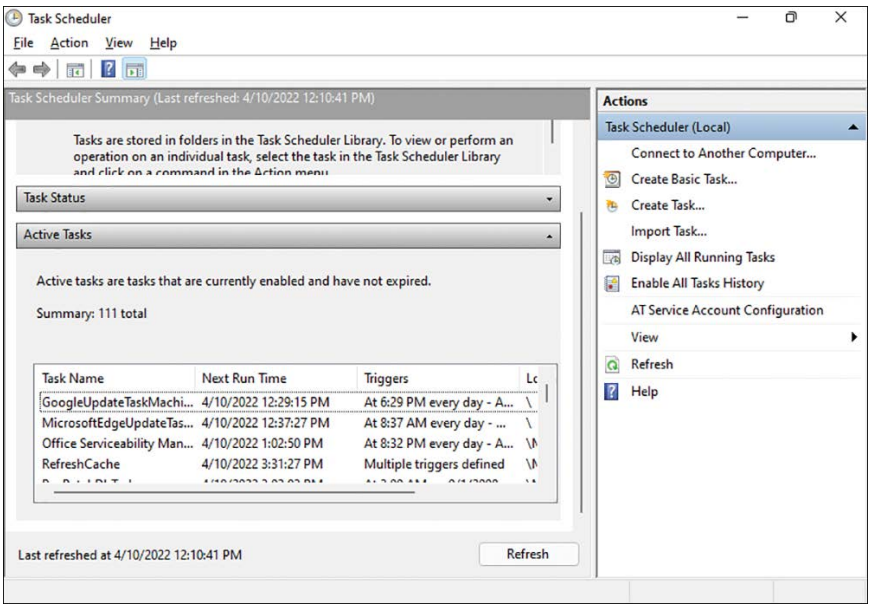


FIGURE 16.20 Task Scheduler

Event Viewer

The Windows Event Log service starts automatically every time a computer boots to Windows. Logs are created every time something happens in a Windows system. The Windows Event Log service allows the events to be logged. **Event Viewer** (`eventvwr.msc`) is a Windows tool that is used to read these logs so you can monitor various events on a computer, such as when a driver or service does not start properly (see Figure 16.21).

Windows Event Viewer shows two types of logs: Windows logs and applications and services logs. In the Windows Logs section, there are the application, setup, security, system, and forwarded events logs, along with setup and forwarded events. The Applications and Services Logs section contains logs from specific applications or Windows components. Table 16.11 summarizes the types of things you might see in these logs. Event Viewer can display five different types of events; these events and related symbols are shown in Table 16.12.

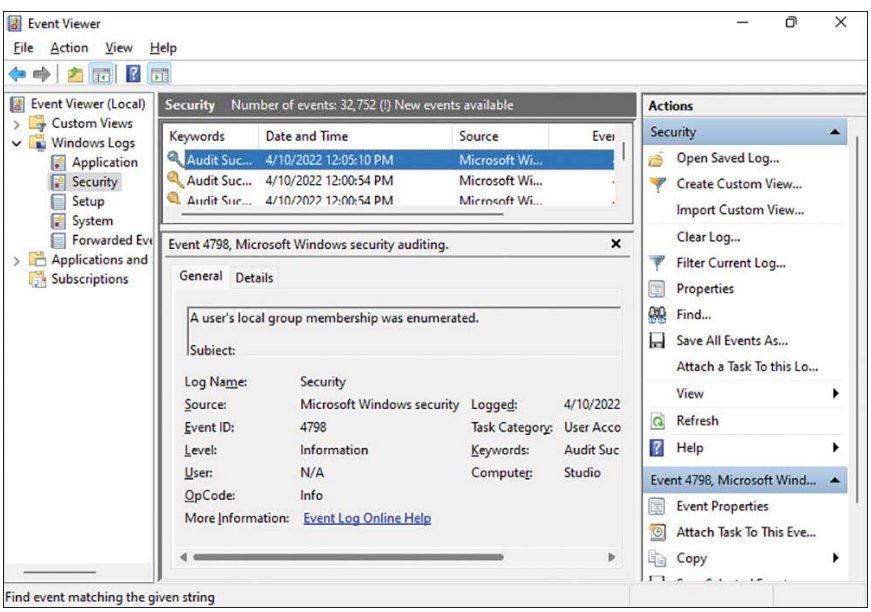


FIGURE 16.21 Event Viewer

TABLE 16.11 Windows Event Viewer logs

Major log category	Log	Description
Windows Logs	Application	Contains events logged by software applications. The company that writes the software applications decides what to log.
	Security	Contains events specified by administrators, such as valid and invalid logon attempts and network share usage.
	Setup	Contains setup events logged by software applications.
	System	Contains Windows system events such as when a driver or service fails to load or start.
	Forwarded events	Contains events from remote computers.
Applications and Services Logs	Vendor specific	Contains logs from a specific application or Windows component. The logs can be one of four types: admin, operational, analytic, or debug. The admin log is for normal users and technical support staff. The operational log is used by technical staff to analyze a problem. The analytic and debug logs would likely be used by the application developer; both of these logs create a large number of entries and should be used for a short period of time only.

TABLE 16.12 Event Viewer symbols

Symbol	Type of event	Description
Lowercase "i"	Information	Normal system operations, such as the system being initialized or shut down.
Exclamation point (!)	Warning	An event that is not critical but that you might want to take a look at. The system can still function, but some features may not be available.
X	Error	A specific event failed, such as a service or device failing to initialize properly.
Yellow key	Audit success	You can audit a specific event. This symbol indicates a successful audit.
Yellow lock	Audit failure	When you specify a particular event to audit and the event fails, the yellow lock appears. For example, if you are auditing a system login and someone tries to log in without having a valid username or password, the system creates an audit failure event.

The application log displays events associated with a specific program. The programmers who design software decide which events to display in Event Viewer's application log.

TECH TIP

Application hangs, crashes, or doesn't respond

If an application hangs, crashes, or shows a "not responding" message, take a look at the Event Viewer application log. Research any messages or error codes found. Ensure that the application does not need to be updated. Any proprietary crash screens should be researched in Event Viewer.

The security log displays events such as users login attempts, including both valid and invalid logins. A technician can pick which events display in the security log. All users can view the system log and the application log, but only a member of the Administrators group can enable security log information. Event Viewer logs can be saved as files and viewed later. This is especially useful with intermittent problems. Use the *Actions* section of the Computer Management console to save and retrieve Event Viewer log files.

TECH TIP

What to do with a blue screen

Sometimes when Windows crashes, a **blue screen** with an error code and numbers appears. Check the Event Viewer for a system event. Try to reboot with the power button. Note that this may require you to remove the computer's power cord, re-insert the power cord, and once again power on the computer. When the computer has been restarted, you can research the error message and problem on the internet.

The most commonly used log is the system log. The system log displays events that deal with various system components, such as drivers or services that load during startup. The type of system log events cannot be changed or deleted.

Access **system log** errors whenever you want detailed information about Windows-controlled events; look at the **application log** errors when troubleshooting a particular program. Figure 16.22 shows the filters applied to see only system error events. Figure 16.23 shows the results. Notice in Figure 16.23 that you can select a particular event. The *General* tab shows the gist of the error. Select the *Details* tab for even more details.

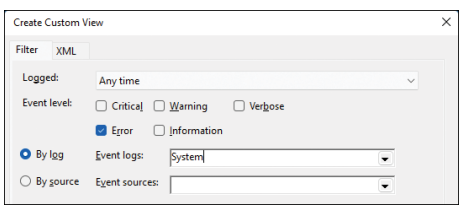


FIGURE 16.22 Event Viewer filter

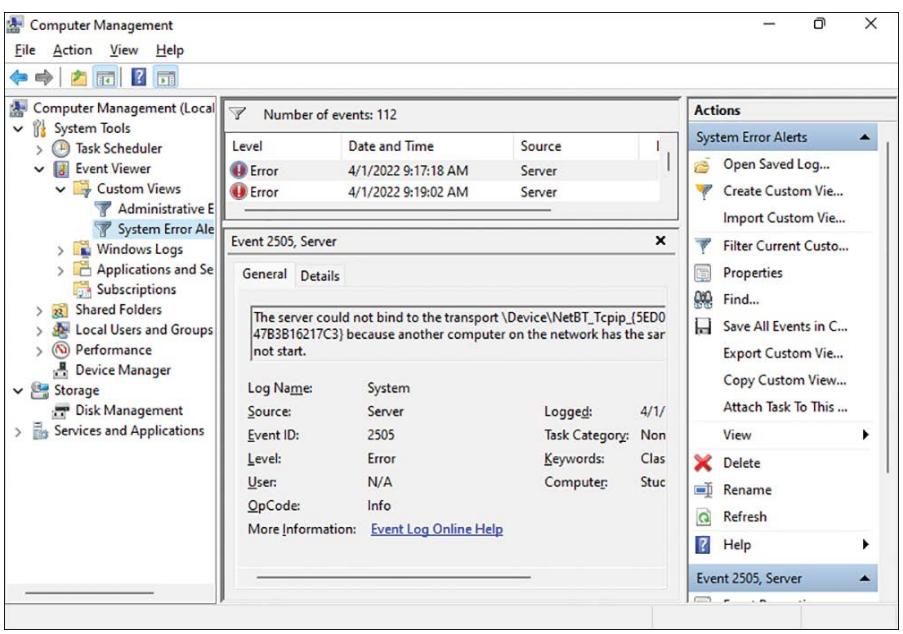


FIGURE 16.23 Event Viewer filter results

TECH TIP

What to do if the Event Viewer log is full

You can clear the log or adjust the log settings. To clear the log, start *Event Viewer* > select a log > *Action* menu option > *Properties* > *General* tab > *Clear log* button. Some settings that might need to be adjusted include *Maximum log size* and *When maximum event log size is reached*.

Shared Folders

The **Shared Folders** tool is used to view shares, sessions, and open files. **Shares** are network resources (such as computers, printers, and scanners) that have been shared on a network. *Sessions* lists network users who are currently connected to the computer, as well as each network user's computer name, the network connection type (Windows or Mac, for example), how many resources have been opened by the network user, how long the user has been connected, and whether this user is connected using the Guest user account. Open files are files that are currently open by network users.

In the left Computer Management pane, expand the *Shared Folders* option and click the *Shares* option. The network shares appear in the right pane. Double-click any of the shares to view its *Properties* window. The shared resource's permissions can be set from this window, using the *Share Permissions* or *Security* tabs. Permissions are covered later in this chapter.

User Account Management

User account management in Windows involves creating accounts, managing accounts, and putting people into groups that are used in different situations. This is an important function for a technician. Windows 10/11 stores credentials information for Windows and web accounts. You can make configuration changes by using the *User Accounts* Control Panel.

Credential Manager

Have you ever gone to a website or accessed a remote computer and been asked if you want your username and password saved? If you agree to such a request while using a Windows computer, your information is saved using Credential Manager. **Credential Manager** is where Windows stores login credentials. You can back up Windows credentials to protect yourself in the event that the computer crashes, and you can view or remove forgotten or old credentials.

To locate Credential Manager, search for `credential` using the search function in the taskbar or in *Settings*. Notice in Figure 16.24 that there are two sections: Web Credentials and Windows Credentials. Windows and other applications use the information stored in Credential Manager, which may be of several varieties:

- **Windows credentials:** Windows services use Windows credentials when you access a specific computer or server with a username and password.
- **Certificate-based credentials:** Certificate-based credentials are mainly used in complex business network environments with smart cards.
- **Generic credentials:** Apps such as Microsoft 365, OneDrive, and Xbox Network use generic credentials. Websites that require usernames and passwords also use generic credentials.
- **Web credentials:** Web credentials include username and password information stored by Windows for specific websites. Your machine might store your web credentials for logging in to the main portal where you work, a gaming website, email, and shopping sites. Web credentials are also used for password reset links.

TECH TIP

Stored credentials pose a security risk

Storing usernames and passwords saves all of us time. If someone gains access to your computer, however, they can quickly use *Back up Credentials* to save all your Windows credentials to the cloud or removable media and then use that information from another computer to access accounts.

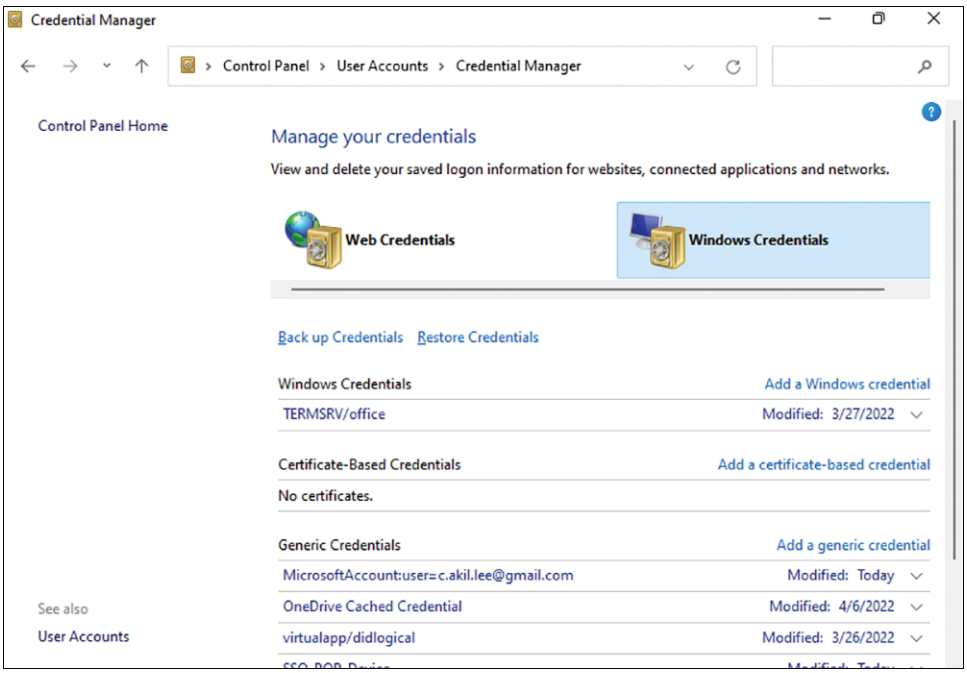


FIGURE 16.24 Credential Manager

How to Add a Windows Credential

As a technician, you might need to manually add a credential for Windows to use. To do this, access *Credential Manager* > *Windows Credentials* > locate the area that contains the specific type of credential > click *Add a Windows credential*, *Add a certificate-based credential*, or *Add a generic credential*. For example, Figure 16.25 shows the link to use if you want to add a Windows credential.

Before adding the information to Windows Credential Manager, you should access the server, network device, network share, or website and verify that the username and password work. Then you can enter that information into the appropriate textboxes, as shown in Figure 16.26.

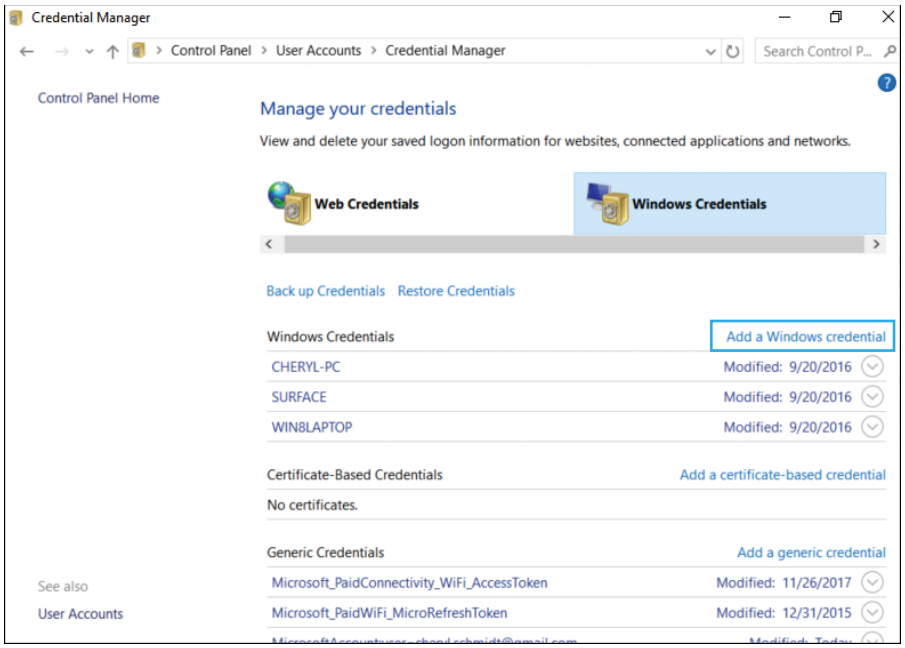


FIGURE 16.25 Adding a Windows credential, step 1

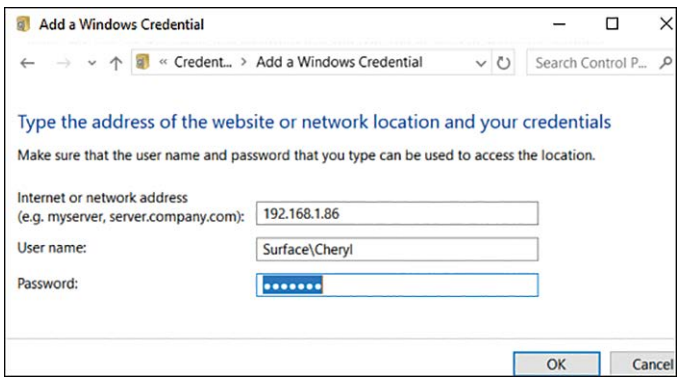


FIGURE 16.26 Adding a Windows credential, step 2

How to Remove a Windows Credential

If you want to remove a specific credential, such as when you see one that you do not recognize or that you no longer use, click the arrow to the right of that credential to expand the section. Then click the *Remove* link, as shown in Figure 16.27.

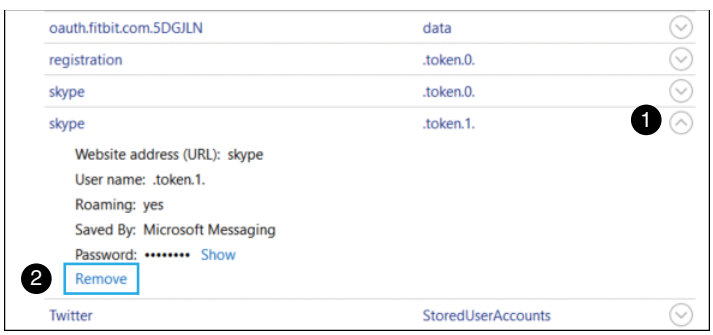


FIGURE 16.27 Deleting a credential

How to Edit an Existing Credential

In some cases, you might be required to change a password. When doing so, if you decline the dialog that asks if you want to update the password, you will then have to type the credentials each time rather than have them prepopulated for you. You can edit credentials in Credential Manager by clicking the arrow to the right of the credential to expand the section and then clicking the *Edit* link (see Figure 16.28).

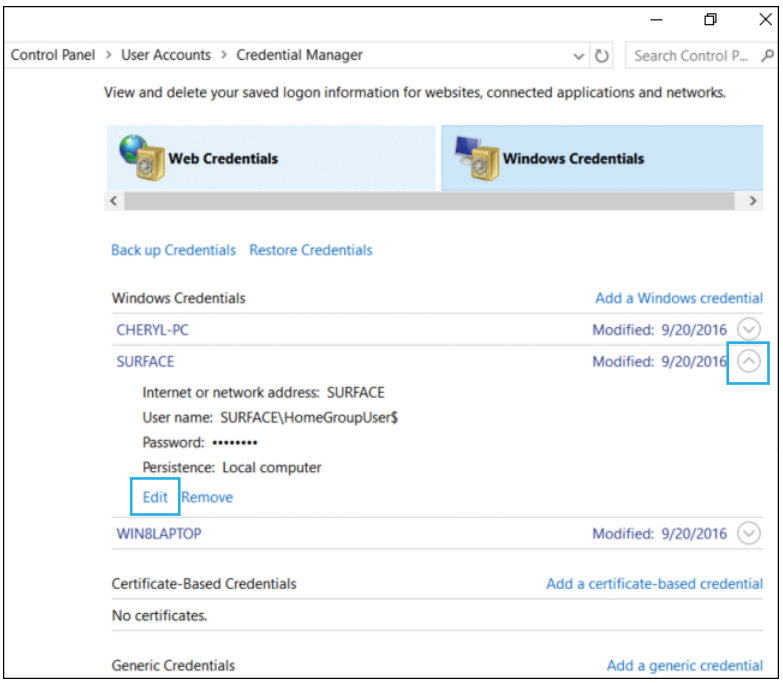


FIGURE 16.28 Editing a credential

TECH TIP

Use the specific application to change the credentials

Not all applications respond well to editing credentials within Credential Manager. Be especially cautious when editing credentials used to access virtual machines.

Local Users and Groups

The **Local Users and Groups** tool (`lusrmgr.msc`) is located in the Computer Management console. It is available only in Windows Pro versions and above. It is used to create and manage accounts for those who use the computer or those who use the computer resources from a remote network computer. These accounts are considered local users or local groups and are managed from the computer being worked on. In contrast, domain or global users and groups are administered by a network administrator on a network server. Permissions are granted or denied to files, folders, and network resources such as a shared printer or scanner. Rights can also be assigned. **Rights** give different users the ability to execute certain computer actions such as performing a backup or shutting down the computer.

Open the *Local Users and Groups* option by expanding the *Local Users and Groups* selection in the *Computer Management* window. Click on the *Users* option, and a list of current users appears

in the right pane. Figure 16.29 shows an example of local users. To create a new user, click the *Action* menu option and select *New User*.

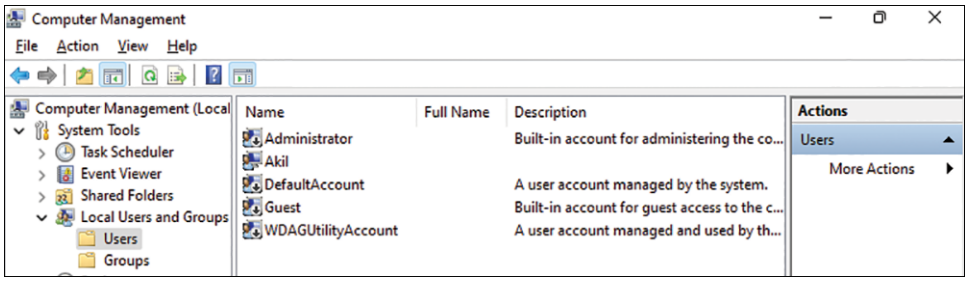


FIGURE 16.29 Local users and groups

Notice in Figure 16.29 that the Guest account has a small down arrow in the lower-right corner of its icon. This means the account has been disabled. Double-click the *Guest* icon. Look at the *Account is disabled* checkbox to see if the account is disabled. The box is checked by default, meaning that the Guest account is not available for use.

TECH TIP

Where are the local user settings?

Windows local user settings are found in the following folder: `%userprofile%\AppData\Local` (for example, `C:\Users\Cheryl\AppData\Local`). You might have to enable *Show > Hidden items* in File Explorer to see the `AppData` folder.

Windows has two basic types of user accounts available in the different Windows editions: Standard user and Administrator. The Administrator account has full control over the system in Windows. By default, a **Standard user** account cannot install most applications or change system settings. Every user on the computer should have a Standard user account that is used for everyday use. Any account designated as an Administrator account should be used only to log on to the system to make system changes and install new software.

In Windows Pro and higher versions, additional types of user accounts can be used for various security levels. These user groups are covered elsewhere, but one user group that should be mentioned here is Power Users. In older Windows versions (Windows XP and earlier), users who were in the Power Users group had elevated permissions to perform common configuration tasks such as changing user-related Control Panel settings and changing the time zone. Today, the Standard user group has most of these permissions.

Account Recovery Options: Local Account

Windows **account recovery options** are limited for security reasons. You should always have a backup account that is an Administrator account on a local (workgroup) computer. Here are some other ways that you can recover a Windows user account:

- Use the Windows password reset disk that was previously created.
- Have someone who has an Administrator account log in to Windows and reset your password for you.
- In Windows 10/11, use an online Microsoft account as a login or a local account and reset that password.
- Boot from a Windows installation disk, boot to a command prompt, and use the `net user` command to create an Administrator account. (You will have to do research on this one.)

> If there are accidentally no users with administrator rights, boot the computer into Safe Mode and change one of the accounts to an Administrator account type.
> Use the *I Forgot My Password* link and take the necessary steps to reset the password.
> Reload Windows. Use this option as a last resort as it will cause you to will lose everything that is stored on the hard disk or SSD.

UAC

The Administrator and Standard user accounts are affected by a feature in Windows called User Account Control (**UAC**). UAC works with Edge, Windows Defender, and Parental Controls to provide heightened awareness of security issues. A UAC message appears any time something occurs that normally would require an administrator-level decision to make changes to the system. An application that has a security shield icon overlay displays a UAC prompt when executed. If a Standard user is logged in, a message appears, stating that the task is prohibited, access is denied, or administrator credentials must be provided in order to proceed (see Figure 16.30). UAC is meant to protect users from themselves as well as from software that tries to change the system. Even if a person is logged in with an Administrator account, the UAC prompt appears to confirm the action that is about to be performed.

FIGURE 16.30 Administrator credentials required

The following configurations help with UAC:

> To configure a specific application to run in an elevated mode—meaning it has the administrator access token given to it or permission given to it to run—right-click the application and select *Properties* > *Compatibility* tab > under Privilege Level select *Run this program as an administrator* > *OK*.
> If a user demands that UAC be disabled, search for `uac` in *Settings* > select *Change User Account Control Settings*. The User Account Control Settings dialog appears (see Figure 16.31). The dialog box is also available through the System Configuration window (`msconfig`) *Tools* tab. Select *Change UAC Settings* and click *Launch*.

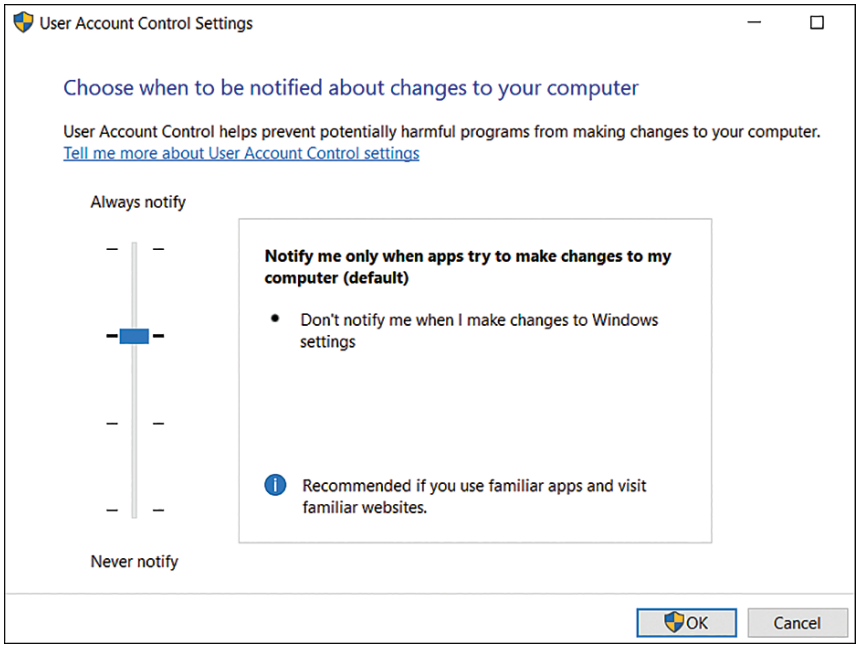


FIGURE 16.31 UAC configuration in Windows

Managing Storage

Mechanical hard drives and SSDs can be managed using the *Storage* Computer Management console option, which includes the Disk Management tool. The **Disk Management** tool (`diskmgmt.msc`) is used to manage hard drives, including volumes or partitions. With it you can initialize drives; create volumes; format volumes for FAT, FAT32, and NTFS; configure RAID; and manage remote drives. You must be a member of the Administrators group to perform tasks using Disk Management.

Chapter 7, "Storage Devices," introduces Disk Management, but let's review the basics here. Figure 16.32 shows the Disk Management utility. Disks are numbered starting with 0 (Disk 0), and a disk can be segmented into separate volumes. Notice that the drive volumes display in the top window as well as at the bottom. The volumes' attributes are listed in the top window. Each volume appears as a section of a disk in the bottom window.

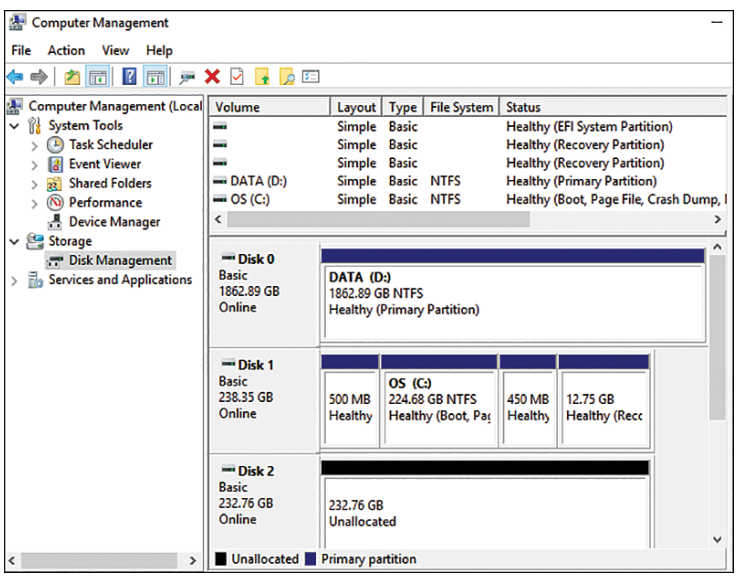


FIGURE 16.32 Disk Management utility

Figure 16.33 shows the options that are available if you right-click inside the unallocated space in Disk 2. Because the disk is currently a basic disk, only a simple volume can be created. When you create a volume, you are prompted to select a file system as well as assign a drive letter. See Chapter 7 for more information on volumes and partitions.

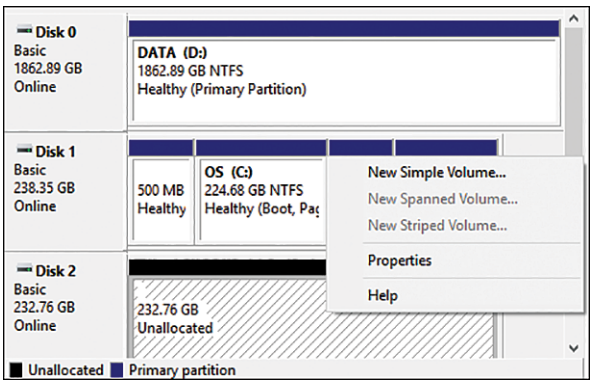


FIGURE 16.33 Managing drive space on a new drive

Figure 16.34 shows that you can right-click or tap and briefly hold on a particular disk on the far left to control the disk via a context menu. The menu shown in this figure is for a drive that is already in use and online. If a drive shows a **drive status** other than online, appropriate actions can be taken from the context menu.

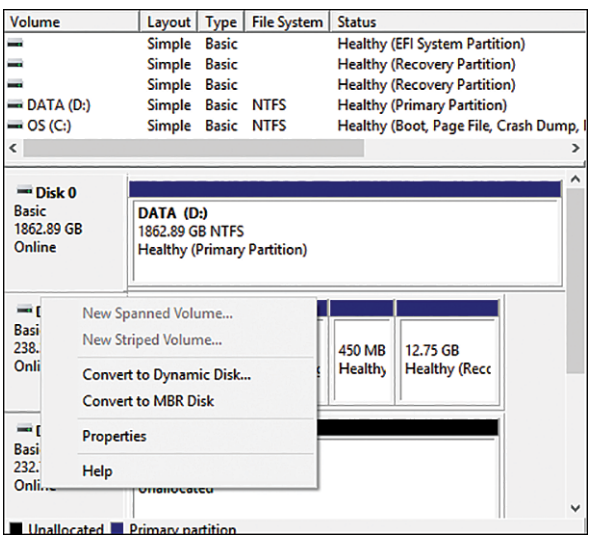


FIGURE 16.34 Controlling a particular disk

Figure 16.35 shows the context menu that appears when you right-click within a disk volume, such as within the slanted lines of the `D:` drive (Drive 0). Notice that you can delete, extend, or shrink a volume. You can also change the drive letter. Table 16.13 describes the tasks that are commonly accomplished with the Disk Management tool.

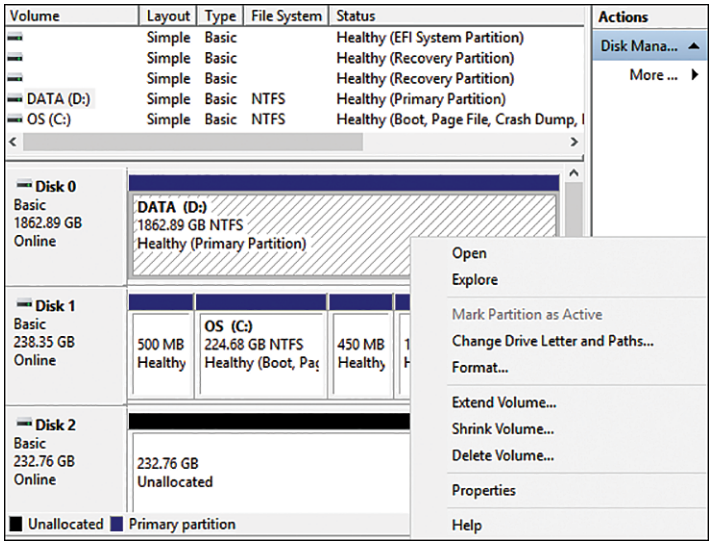


FIGURE 16.35 Controlling a particular volume

TABLE 16.13 Disk Management tasks

Task	Description
Initializing	Make a new disk available to be used by right-clicking a drive > *Initialize Disk*.
Adding a volume	Ensure that the drive is recognized by the BIOS/UEFI and then create a partition and format it for a particular file system.
Assigning/ changing drive letter	Right-click on a drive volume > *Change Drive Letter and Paths*.
Mounting	Map an empty folder on an NTFS volume by right-clicking a partition or volume > *Change Drive Letter and Paths* > *Add* > *Mount in the Following Empty NTFS Folder* and either type the path or browse to an empty folder > *OK* > *OK*.
Extending a partition	Increase the size of a partition by right-clicking on the drive letter > *Extend Volume*. Some volumes cannot be extended.
Shrinking a partition	Decrease the size of the partition by right-clicking the drive letter > *Shrink Volume*. Some volumes cannot be shrunk.
Splitting a partition	To divide space on a hard drive or make one partition smaller, right-click the drive > *Shrink Volume*. Then create a new partition with the relinquished drive space.
Adding an array	Right-click inside unallocated space of a drive > *New Spanned Volume, New Mirrored Volume, New Striped Volume*, or New RAID 5 volume. Then select another drive to be added and select a drive letter and file system.

TECH TIP

All Windows disk management tools require administrator rights

You must be a member of the Administrators group to perform any disk management tasks.

Storage Spaces

Another Control Panel utility that is used with Disk Management is Storage Spaces (*Control Panel > System and Security > Storage Spaces*). The **Storage Spaces** Control Panel is used for data storage using two or more drives that the operating system sees as one drive; this combination of drives is called a *storage pool*. The unusual thing about Windows Storage Spaces is that the drives can be different types of drives; for example, an eSATA drive and a USB flash drive can be used to create a virtual disk that is seen as one drive. A logical drive (pool) created through Storage Spaces is formatted for either the NTFS or ReFS file system. Note that if you use drives in a logical drive created through Storage Spaces, each of those drives cannot be given an individual drive letter. In addition, the drives no longer appear in Disk Management, and they can only be used in Storage Spaces. The new pool appears in Disk Management as a disk.

Use the steps below to create a new pool:

Step 1. From the *Storage Spaces* Control Panel, select the *Create a new pool and storage space* link.

Step 2. Ensure that at least two drives that you want to use for the virtual drive created using Storage Spaces are attached. Select the drives by clicking in the checkbox beside each drive that is to be used. Note that any existing files on a selected drive will be erased and cannot be recovered.

Step 3. Click the *Create Pool* button.

Step 4. Name the storage space and select the drive letter, file system, resiliency type, and pool size > select *Create storage space*.

Use the *Change Settings* button within the *Storage Spaces* Control Panel to manage or modify a logical drive.

Disk Maintenance

Mechanical hard drives get sluggish over time. The good news is that disk management and maintenance are now done for you automatically in Windows 10/11. Let's look at the tools that are available to keep mechanical drives running smoothly.

In Windows 10, right-click a drive letter in File Explorer > select *Properties*. On the *General* tab, you can access the **Disk Cleanup** tool (`cleanmgr /d drive`, for example), which scans the drive volume to see what files could potentially be deleted. In Windows 11, use *Settings > System > Storage > Cleanup recommendations*.

In Windows 10/11, the *Tools* tab in a disk's Properties window provides access to two additional tools: Error Checking and Optimize Drives. The Check button opens the **Error Checking** tool, which is extremely important to Windows. The tool checks the drive for file system errors, bad hard drive sectors, and lost clusters. Using Error Checking is the equivalent of running the `chkdsk` command.

Windows 10 and 11 do not need to have the drive checked as often as earlier versions because certain disk errors are fixed immediately and do not need a utility executed to make that happen. Microsoft integrated some of the new features of Resilient File System (ReFS), which is expected to eventually replace NTFS as the file system used on Microsoft Windows systems, but at the time of press, ReFS volumes cannot be used to boot the system.

The Optimize button opens the **Optimize Drives** tools. Files and folders become fragmented over a period of time due to file creation and deletion cycles. That is, the bits that comprise a file can be located in non-contiguous portions of the disk. Because mechanical drives have moving

parts, a defragmented volume provides better performance than a volume with files and folders located throughout the drive. Therefore, with a mechanical drive, you should **defragment the hard drive** to get better drive performance after you have used the Error Checking tool or the `chkdsk` command. The Optimize Drives tool—which you access by clicking the *Optimize* button or using the `dfrgui` command or the `defrag` command—places files in contiguous clusters on the hard drive. Microsoft automatically runs a defragment operation once a week, but you can adjust the frequency or defragment the drive volume manually.

Defragmentation is not required for SSDs because they don't have moving parts. However, an SSD performs better and lasts longer if the operating system occasionally sends a TRIM command to tell the SSD which pieces of data can be deleted from the drive. As with defragmenting mechanical drives, Windows 10/11 automatically trims SSDs once a week, but you can adjust the frequency or trim an SSD manually.

TECH TIP

Defragmentation and trimming require administrator rights

Only a member of the Administrators group can manually defragment a hard drive or trim an SSD.

Use the *Optimize* button in Optimize Drives to manually defragment or trim a drive. If you want to implement your own automatic optimization schedule (to control scheduling for both defragmentation and trimming), select *Change settings in Optimize Settings* and then select the best options for your situation:

- **Run on a schedule:** Select how often the drive optimization executes.
- **Frequency:** Choose daily, weekly, or monthly. By default, optimization runs weekly during automatic maintenance.
- **Drives:** Click the *Choose* button to select drives.

Managing Services and Applications

The *Services and Applications* section of the Computer Management console can contain a multitude of options, depending on the computer, what is installed, and what is running. Common options include Telephony, WMI Control, Services, and Indexing Service. A frequently used option is Services. A **service** is an application that can be started by using this window or configured so that it starts when the computer boots. It runs in the background and is often a vital component of the operating system. When you click the *Services* option, a list of services installed on the computer appears in the right window. Double-click any service, and the service's *Properties* window appears. In this window, you can use the *General* tab to start, stop, pause, resume, or disable a service on the local computer or on a remote computer. You must be logged on as a member of the Administrators group to change a service. Figure 16.36 shows the Computer Management console Services window and some examples of installed services.

If you double-click a service, you can use the *Recovery* tab to select what should happen when a service fails a first time, a second time, and even a third time. For example, if the print service fails the first time, a restart of the service occurs. After the print service fails a second time, the print server can be restarted automatically. The third time the print service fails, an executable file that pages a technician can be executed.

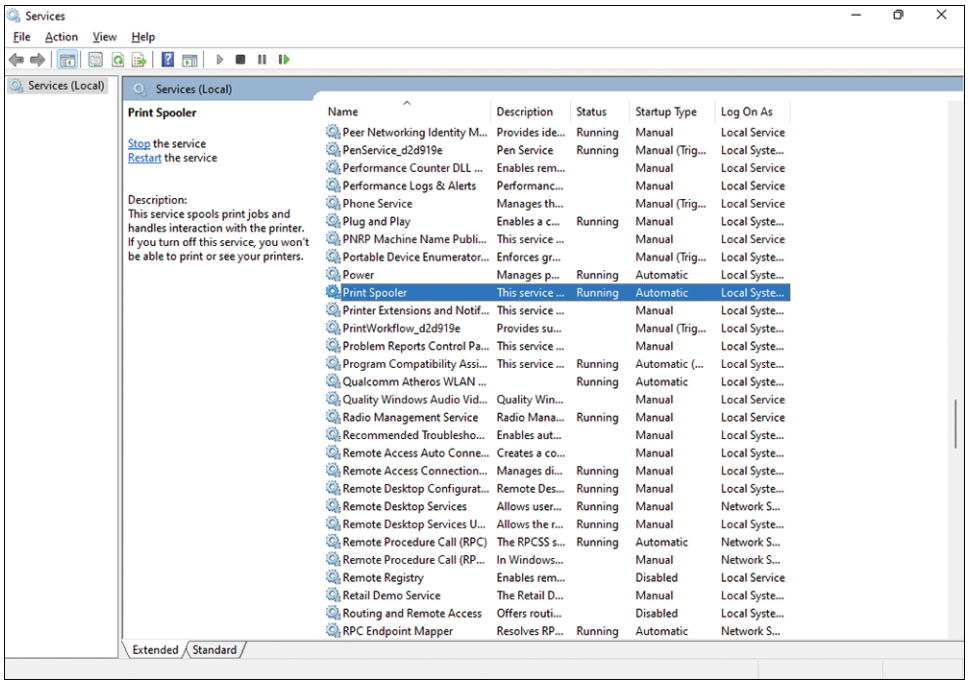


FIGURE 16.36 Computer Management console: Services window

Data Sources (ODBC)

Open database connectivity (ODBC) is a programming interface that enables applications to access data from a database. Use the ODBC **Data Sources** administrative tool to select which application drive is associated with a particular type of file. Access the *ODBC Data Sources* section of the Control Panel by searching for the *Administrative Tools* section of the Control Panel > double-click on *ODBC Data Sources (32-bit)* or *ODBC Data Sources (64-bit)*. Figure 16.37 shows the User DSN (where DSN stands for *data source name*) tab of the *ODBC Data Sources (64-bit)* window. Figure 16.38 shows the *Tracing* tab, which can be used to create logs that help when applications misbehave.

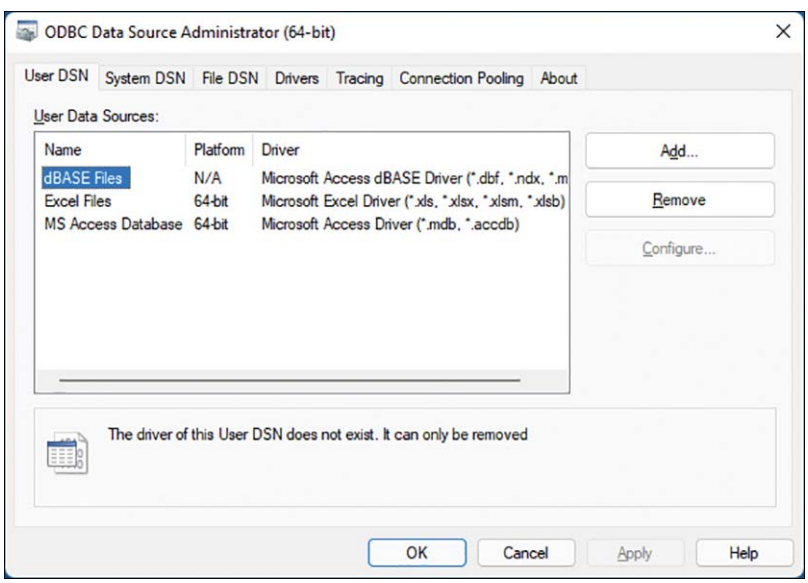


FIGURE 16.37 Data Sources (ODBC) section of the Control Panel

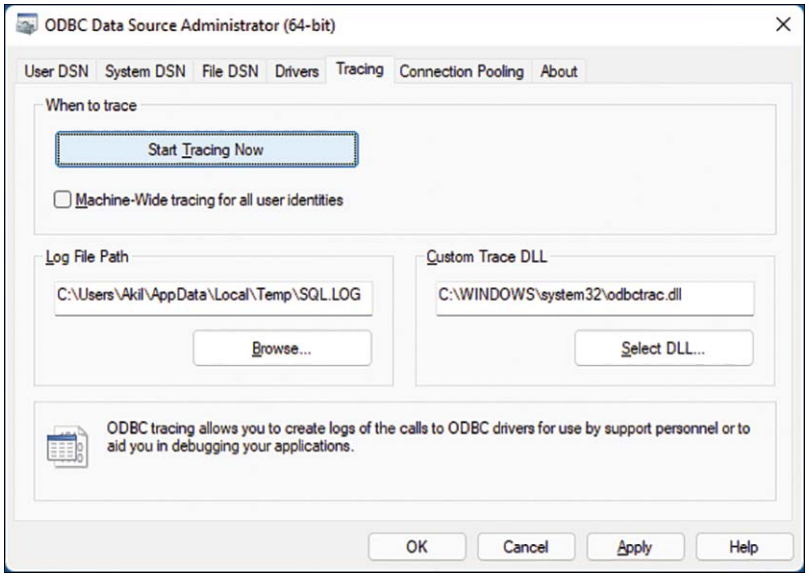


FIGURE 16.38 Data Sources (ODBC) Tracing tab

Print Management Console

The **Print Management** console is used to manage printers in Windows 10/11 Pro and higher versions. To access the console, use one of the following methods:

> Access the *System and Security* section of the Control Panel > select *Administrative Tools* > double-click *Print Management*.

> Use the `printmanagement.msc` command.

Figure 16.39 shows the Print Management console window. On the left, expand *Custom Filters* to see all the printers, all drivers, the printers that show a not ready status, and printers that currently have print jobs. In the center of the screen is a list of printers in a home or small business environment. In a corporate environment, there would be more; in addition, you can use the *Print Servers* option in the left pane.

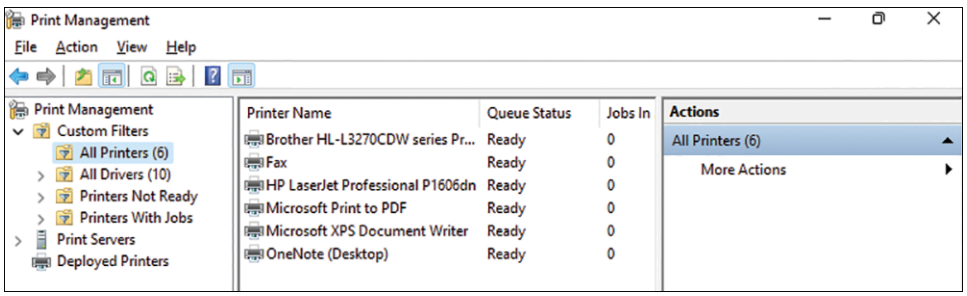


FIGURE 16.39 Print Management console

Printing Issues

Chapter 9, "Printers/Multifunction Devices," is an entire chapter devoted to printers of all types, with a section on troubleshooting for each type. Here are some recommendations specifically related to Windows **printing issues**:

> Try printing a test page from an application. If that doesn't work, use the printer's *Properties* window (*General* tab) to print a test page.

- Use the Windows troubleshooting tool. In Windows 10 or 11, search for `printer` in *Settings* and select the *Find and fix problems with printing* option.
- Ensure that the user is printing to the correct printer. Companies commonly have multiple network printers.
- Clear the print spooler (queue) files and restart the print spooler service from the printer's *Properties* window.

Overview of the Windows Boot Process

When a computer boots, it executes the power-on self-test and then it looks for an operating system. The Windows operating system can be loaded using several boot methods, and you might have to use an alternative boot method to solve a problem. Here are the most common boot methods, but remember that the boot order set within BIOS/UEFI affects which methods the computer looks for first, second, and so on:

- An **internal hard drive partition** on an **internal fixed disk** that could be a hard disk drive (HDD), solid-state drive (SSD), or M.2 SSD. Note that the partition must be a bootable partition.
- An **optical disc** such as a CD, DVD, or Blu-ray disc. Note that this will work only if the BIOS/UEFI boot option is configured correctly and listed before a hard drive.
- An **external hard drive** such as a USB or eSATA drive. Check BIOS/UEFI boot options.
- **Network boot**, sometimes called pre-boot execution environment (**PXE**) boot, where the system boots from an image shared on a network. Configure BIOS/UEFI for the appropriate setting, which might be listed as PXE, PXE Boot, Boot to Network, or LAN Boot ROM Enabled, as well as the network boot option, which might be placed before any of the other options.
- Internet-based booting, which is similar to network booting except that the image is retrieved from the internet.

Every operating system needs specific files that allow the computer to boot. These files are known as **system files**, or startup files. The **system volume** is the active drive partition that holds the files needed to load the operating system. The **boot volume** is the partition or logical drive where the operating system files are located. One thing that people sometimes forget is that the system volume and the boot volume can be on the same partition. These partitions are where certain boot files are located.

Windows goes through four basic phases to get started:

1. **Preboot:** BIOS/UEFI controls the process of looking for, finding, and allowing an operating system to load.
2. **Windows boot manager (`bootmgr.exe`):** Windows locates and executes the Windows loader (`winload.exe`) from the boot partition/volume.
3. **Windows operating system loader:** Some drivers that are needed by the Windows kernel are loaded.
4. **Windows OS kernel (ntoskrnl.exe):** More drivers are loaded, services are start, group and local policies are applied, and the logon screen is shown.

Table 16.14 lists the system files and their specific locations on the hard drive.

The Windows installation media usually contains drivers for the most common types of hardware. Some devices (such as RAID controllers) require specialized drivers that are not included on the media. During the installation process, the system prompts the user to supply the required drivers. Alternatively, the locations of the drivers must be included in an automated installation process.

TABLE 16.14 Windows system files

Startup filename	File location
bootmgr.exe	Root directory of system partition
hal.dll	%*systemroot*%\System32*
ntoskrnl.exe	%*systemroot*%\System32*
winload.exe	%*systemroot*%\System32*
winresume.exe	Root directory of system partition
bcd (boot configuration data)	%*systemroot*%\Boot
system (registry file)	%*systemroot*%\System32\Config\System
winlogon.exe	%*systemroot*%\System32

* %*systemroot*% is the boot partition and the name of the folder where Windows is installed (normally C:\Winnt or C:\Windows).

Reading about Windows files can be confusing because the file locations frequently have the entries %*systemroot*% and %*systemdrive*%. This is because computers can be partitioned in a variety of ways. If you install Windows onto a drive letter (a partition or logical drive) other than the active partition (normally C:), the startup files can be on two different drive letters. Also, you do not have to use the default folder name Windows to install Windows. To account for these different scenarios, Microsoft uses %*systemroot*% to represent the **boot partition**, which is the partition and folder that contains the majority of the Windows files. %*systemdrive*% represents the root directory. On a computer with a single operating system, this would be C:\.

If a computer shows *Invalid Boot Disk*, ensure that the BIOS/UEFI boot order settings are correct, ensure that no virus is installed, and make sure the first boot device has a valid installed operating system or has a valid installation image. Depending on the installed version, you can also use bootrec /fixmbr or bootrec /fixboot. Use other bootrec command options if multiple operating systems are installed. Following is a breakdown of the commands you should try after using the Startup Repair option:

> **bootrec /fixmbr:** Used to resolve MBR issues; writes a Windows-compatible MBR to the system partition.
> **bootrec /fixboot:** Used if the boot sector has been replaced with a non-Windows boot sector, if the boot sector has become corrupt, or if an earlier Windows version has been installed *after* Windows was installed and the computer was started with ntldr instead of bootmgr.exe.
> **bootrec /scanos:** Used when any Windows operating system has been installed and is not listed in the Boot Manager menu; scans all disks for any and all versions of Windows.

Windows Recovery Environment (WinRE)

Windows Recovery Environment (**WinRE**) is used when Windows 10/11 does not boot and other tools and startup options do not solve a problem. Figure 16.40 shows the initial screen of Windows Recovery Environment. WinRE has a list of recovery options, including a command prompt–only environment. The WinRE environment provides access to tools to troubleshoot the operating system when the tools in the operating system cannot be accessed or don't work properly. The WinRE tools are stored on a special recovery partition when the operating system is installed. Some of the troubleshooting options mentioned in this section are available in WinRE.

You can launch WinRE in a variety of ways:

Option 1. At the login screen, press and hold the ⇧Shift key > click the *Power* icon > *Restart*.

Option 2. While logged into Windows:

a. *Settings* > *Update & Security* (*System* in Windows 11) > *Recovery* > locate the *Advanced startup* section and click the *Restart now* button.

b. Click *Start* button > press and hold the ⇧Shift key > click *Restart*.

Option 3. If you can't get to the login screen or to the desktop, boot from the original Windows installation media, select *Repair Your Computer*, and select the *System Recovery Options*.

Option 4. There are also two command-line methods (which must be used by an Administrator account):

```
> reagentc /boottore
> shutdown /r /o
```

Table 16.15 describes the initial WinRE options.

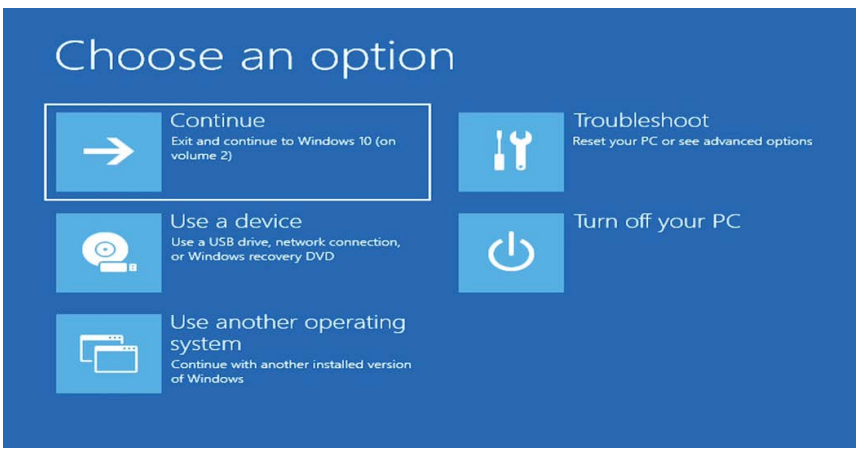


FIGURE 16.40 Windows Recovery Environment

TABLE 16.15 Initial WinRE options

Option	Description
Continue	This option exits the WinRE and attempts to boot the computer as normal.
Turn off your PC	This option shuts down the computer.
Use a device	This option allows you to boot from another device, such as a USB drive, an optical disk, or a network share. You can then use tools from the external device to troubleshoot or repair the computer.
Troubleshoot	This option opens another screen that gives you options to reset the PC or launch advanced options.
Use another operating system	This option appears if more than one operating system is installed on the hard drive (dual booting, not virtualization).

As mentioned in Table 16.15, the Troubleshoot option allows you to reset the PC or launch advanced options:

> Resetting the PC reinstalls Windows and gives you a choice of whether to keep the user files, remove everything, or, on some computers, restore to factory settings (including Windows and the apps that originally came with the computer).

> The advanced options are the primary tools use to troubleshoot, repair, and recover a Windows installation, including a command prompt. You must be careful when using these tools because they may allow you to permanently misconfigure, delete, or overwrite important files (the operating system, applications, user documents, drivers, and so on). Some of the advanced options tools are shown in Figure 16.41 and explained in Table 16.16. Note that *UEFI Firmware Settings* appears only if the motherboard uses UEFI (not legacy BIOS) and the disks use the GPT partitioning style. The other tools available vary by Windows edition and PC manufacturer.

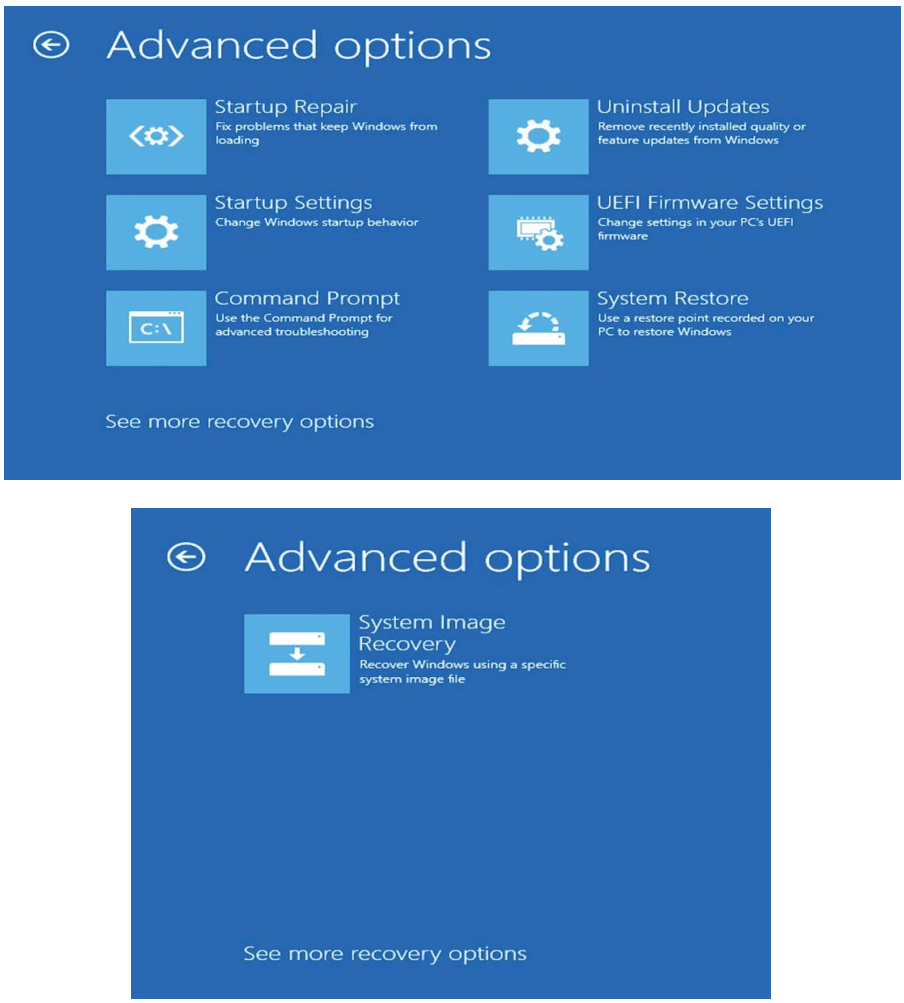


FIGURE 16.41 Windows 10/11 Advanced options tools, first screen (top) and second screen (bottom)

TABLE 16.16 WinRE > Troubleshoot > Advanced options tools

Tool	Description
Startup Repair	Startup Repair analyzes a computer and tries to fix any missing or damaged system files or Boot Configuration Data (BCD) files. This tool can be run multiple times. After a single repair and system reboot, try the tool again (and again). The system could have multiple problems.
Startup Settings	This option eventually takes you to the *Startup Settings* menu, a non-GUI menu that includes options like Safe Mode, Low-Resolution Video, and Disable Driver Signature Enforcement.

Tool	Description
Command Prompt	This option allows execution of any command-line program.
Uninstall Updates	This option makes it possible to uninstall the latest quality update or the latest feature update. Use this option if you suspect that an update is preventing the computer from booting.
UEFI Firmware Settings	This option launches the motherboard's UEFI configuration system. This option is useful if you don't have time to press the designated UEFI hotkey while the computer is starting up, especially when booting from an SSD.
System Restore	This option returns the system to an earlier time, such as before a service pack or an update was installed and the system stopped booting.
System Image Recovery	This option is available in all versions of Windows 10/11 to restore the contents of the hard drive from some type of backup media, such as another hard drive or DVDs.

Startup Settings Menu

When Windows does not boot properly, you can use the Windows **Advanced Boot Options** menu to select special modes to diagnose the issue. The menu is accessible via *WinRE* > *Troubleshoot* > *Advanced options* > *Startup Settings* > *Restart*. The Advanced Boot Options menu appears when the computer reboots. Table 16.17 briefly describes these options. Note that the options available vary depending on the version of Windows used.

TECH TIP

Press F8 during startup

When Windows is booting, press F8 to access the Windows Advanced Boot Options menu. Note that this feature is disabled by default in Windows 10/11. To enable it, run this command from an elevated command prompt: `bcdedit /set {default} bootmenupolicy legacy`. Disabling the feature speeds up the boot process. To disable it, run this command from an elevated command prompt: `bcdedit /set {default} bootmenupolicy standard`.

TABLE 16.17 Windows Advanced Boot Options window

Boot option	Description
Repair Your Computer	This option launches WinRE if system recovery tools are installed on the hard disk. Otherwise, these tools are available when booting from the Windows installation media.
Safe Mode	This option uses a minimal set of drivers and services to start Windows; it is a commonly used option.
Safe Mode with Networking	This option is the same as Safe Mode but includes a NIC driver.
Safe Mode with Command Prompt	This option is the same as Safe Mode except that Windows Explorer (GUI mode) is not used; instead, a command prompt appears. This option is not used often.

Boot option	Description
Enable Boot Logging	This option enables logging for startup options. The logging file is `ntbtlog.txt`.
Enable Low-Resolution Video (640×480)	This option is used when Safe Mode does not work and you suspect that the default video driver is not working.
Debugging Mode	This option enables debugging information to be sent through the serial port to another computer that is running a debugger program. This option is not used often.
Disable Automatic Restart on System Failure	This option prevents Windows from automatically rebooting after a system crash.
Disable Driver Signature Enforcement	This option allows drivers that are not properly signed to load during startup.
Disable Early Launch Anti-malware Driver	This option disables anti-malware protection for booting. Sometimes driver files might be flagged as malware, causing the system not to boot; disable this option to boot the system to fix it.
Start Windows Normally	This option restarts Windows and attempts to boot normally.

Safe Mode enables you to access configuration files and make necessary changes, troubleshoot installed software and hardware, disable software and services, and adjust hardware and software settings that may be causing problems. In other words, Safe Mode puts the computer in a "bare-bones" mode so that you can troubleshoot problems. As it is a reduced environment, most applications will not work in Safe Mode.

The **System Configuration utility** (`msconfig.exe`) is used to troubleshoot Windows startup problems by disabling startup programs and services one at a time or several at once. This graphical utility reduces the chances of making typing errors, file deletions, and other misfortunes that occur when technicians work from a command prompt. Only an administrator or a member of the Administrators group can use the System Configuration utility.

To start the System Configuration utility, type `msconfig` in the search textbox.

The first System Configuration utility tab is *General* (see Figure 16.42). The *General* tab has three radio buttons: Normal Startup, Diagnostic Startup, and Selective Startup. *Normal Startup* is the default option, and all device drivers and services load normally when this radio button is selected. Select the *Diagnostic Startup* radio button when you want to create a clean environment for troubleshooting. When *Diagnostic Startup* is chosen and Windows is restarted, the system boots to Safe Mode, and only the most basic device drivers and services are active.

The *Selective Startup* radio button is the most commonly used troubleshooting option on the General tab. When you choose *Selective Startup*, you can pick which startup options load. Use the divide-and-conquer method of troubleshooting to find the startup file that is causing the boot problems. Start with the first checkbox, *Load System Services*, and deselect it > *OK* and restart the computer. When you determine which file is causing the problem (that is, when the problem reappears), select the System Configuration utility tab that corresponds to the problematic file and deselect files until the exact problem file is located.

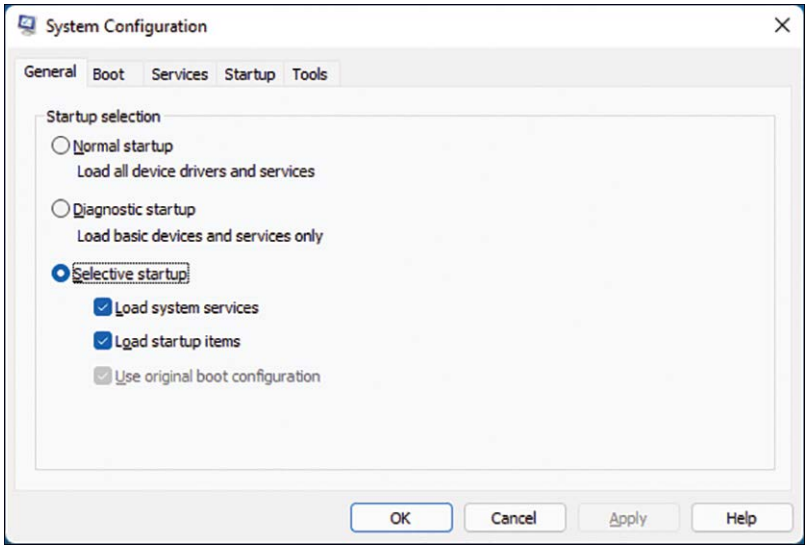


FIGURE 16.42 System Configuration utility: General tab

TECH TIP

File fails to open

If a file does not open, check the *System Configuration* utility to verify if *Selective Startup* is used and a file has been left unchecked. Otherwise, ensure that the application is still installed and other files from this application open properly. Finally, change folder options so that extensions can be seen and verify that the file's extension has not been altered.

The *Boot* tab of the System Configuration utility (see Figure 16.43) enables you to control and modify the Windows boot environment. The functions available on this tab include selecting the default operating system and the time allotted to wait for the default operating system to load if no other operating system is chosen from the boot menu in a multiple–operating system situation. Notice that **Safe Boot** and other options are available at the bottom of the window. Table 16.18 describes the *Safe Boot* options on the *Boot* tab.

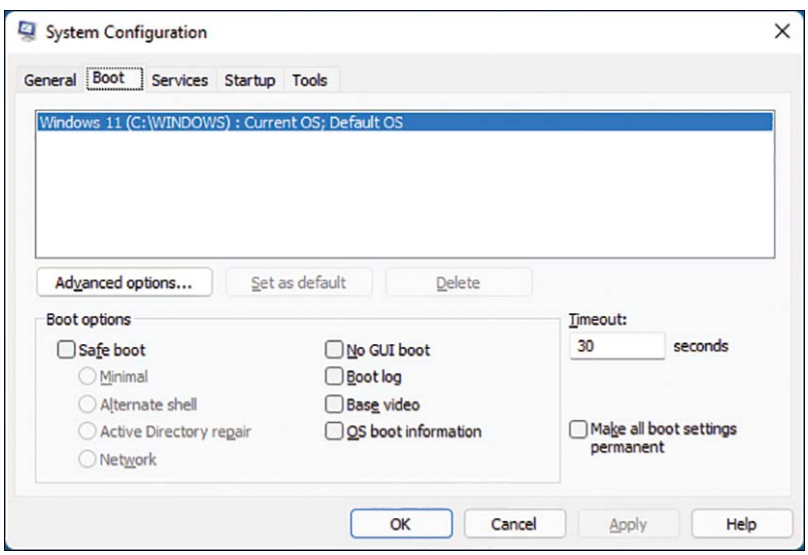


FIGURE 16.43 System Configuration utility: Boot tab

TABLE 16.18 System Configuration Boot tab > Safe Boot options

Safe Boot option	Description
Minimal	Boots in Safe Mode with only critical system services operational (no networking)
Alternate Shell	Boots into a command prompt without a GUI or networking
Active Directory Repair	Boots into Safe Mode, running critical system services and Active Directory
Network	Boots in the Safe Mode GUI with networking enabled
No GUI	Does not display the Windows welcome screen
Boot Log	Stores information about the startup process in the `ntbtlog.txt` file
Base Video	Starts in low-resolution VGA mode
OS Boot Information	Displays driver names during the boot process
Timeout	Controls how long the boot menu shows before the default boot entry executes

TECH TIP

Computer boots into Safe Mode for no obvious reason

If this happens, check the *System Configuration* utility *Boot* tab to see if some form of *Safe Boot* is enabled.

Click the *Advanced Options* button on the *Boot* tab to define the number of processors and maximum memory used to boot the system if you want fewer than the maximum (see Figure 16.44). When the *PCI Lock* option is enabled, it prevents Windows from changing I/O and IRQ assignments from those set by the system BIOS/UEFI.

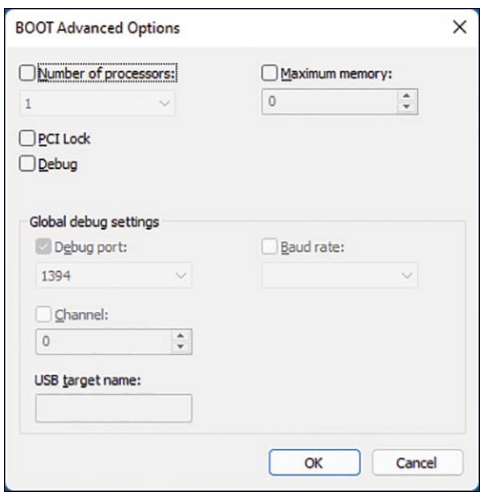


FIGURE 16.44 Windows System Configuration utility: BOOT Advanced Options

The *Services* and *Startup* tabs in the System Configuration utility window are also quite useful when troubleshooting boot problems. Certain applications, such as antivirus programs or printer software, run as services, meaning they run in the background and usually do not require user interaction. Many of these services are started during the boot process. Use the *Services* tab (see Figure 16.45) to disable and enable these boot services. Enable the *Hide All Microsoft Services* option to view and manipulate third-party (non-Microsoft) services.

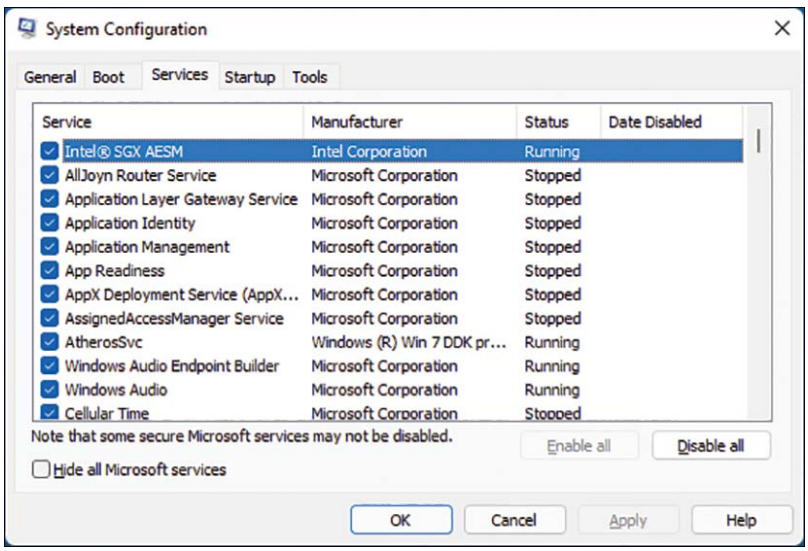


FIGURE 16.45 Windows System Configuration utility: Services tab

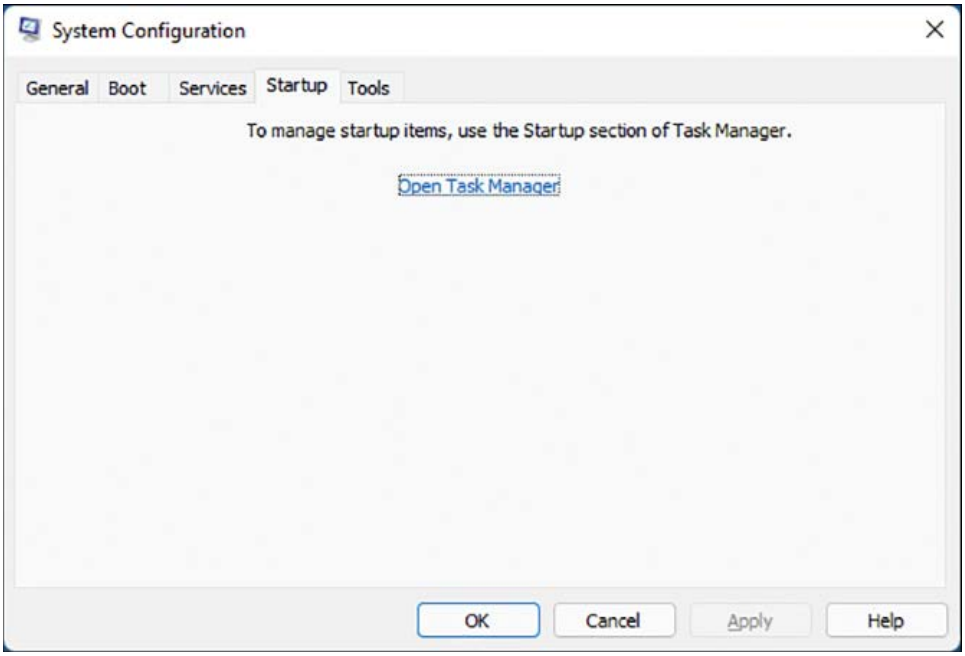
Prior to Windows 8, the *Startup* tab allowed you to enable and **disable Windows applications** that start automatically when Windows boots. This function is now available in the *Startup* tab of Task Manager. When you click *Startup* in the System Configuration utility, you can click *Open Task Manager* to reach the startup settings (see Figure 16.46). Task Manager is covered in the next section.

TECH TIP

The *Tools* tab is useful

The System Configuration utility *Tools* tab allows you to launch options—such as Task Manager, Performance Monitor, and Internet Options—that might need to be changed as a result of a startup issue.

The System Configuration *Tools* tab allows you to launch the majority of the Windows utilities, such as Task Manager, About Windows, Computer Management, System Information, Event Viewer, Programs, Performance Monitor, Registry Editor, System Restore, Command Prompt, and so on, as shown in Figure 16.47.



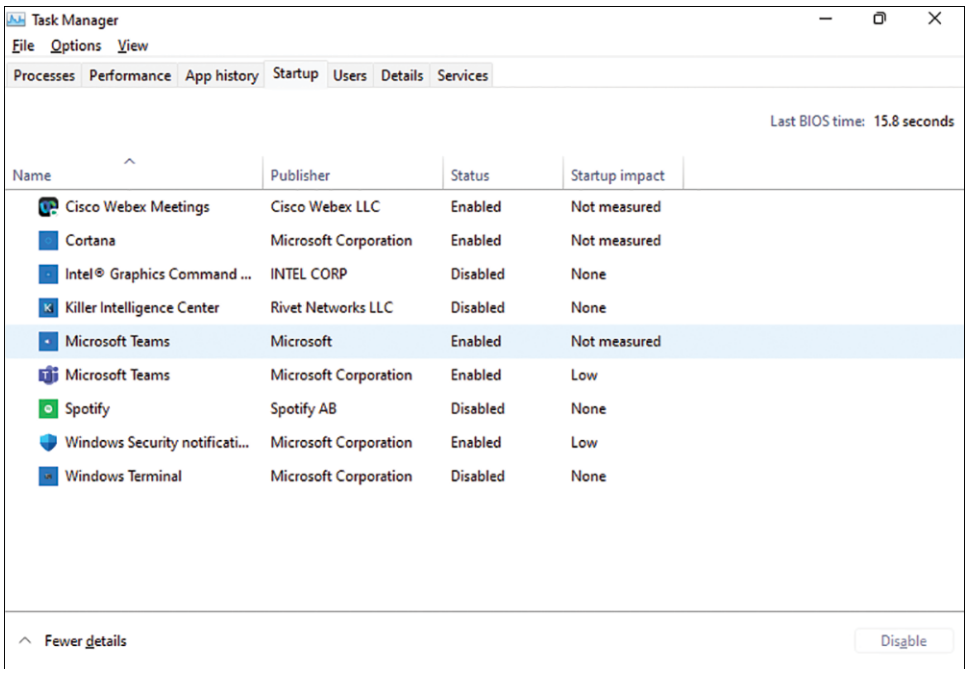


FIGURE 16.46 Windows System Configuration utility: Startup tab (top); Windows Task Manger: Startup tab (bottom)

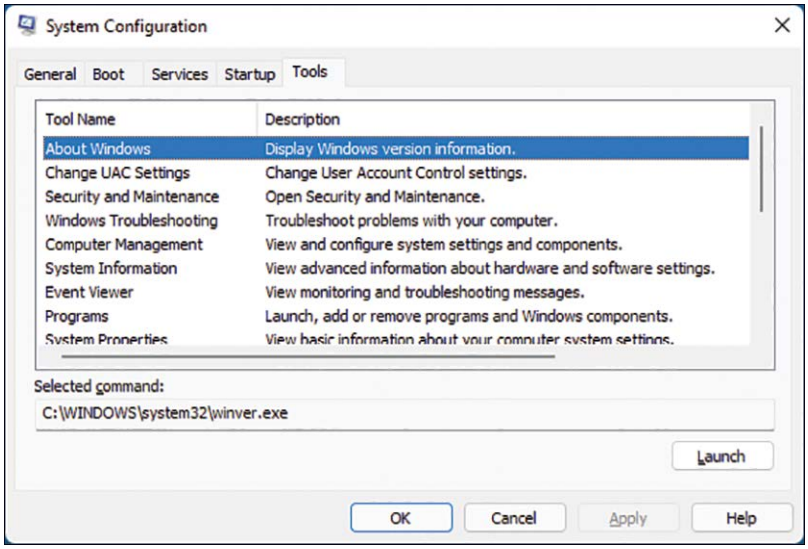


FIGURE 16.47 Windows System Configuration utility: Tools tab

Task Manager

Task Manager is a Windows utility that displays applications that are currently loaded into memory, processes that are currently running, processor usage, and memory details. To activate Task Manager, right-click an empty spot on the taskbar and select *Task Manager*. Task Manager is commonly used when an **application crashes**. Access Task Manager to **kill task** (stop) one or more programs that have stopped responding. Using Task Manager is also a great way to get a graphical overview of how the system performs or which programs use a lot of memory. Windows 10/11 Task Manager has the following tabs: Processes, Performance, App history, Startup apps, Users, Details, and Services. If the tabs are missing, select the *More details* option.

Figure 16.48 shows the Windows 11 Task Manager *Processes* tab, which lists the applications currently running on a computer. You can highlight an app and then click the *End task* button to stop the application. Notice in the figure that there is a green leaf by the Google Chrome app. The leaf indicates that this app is in Efficiency mode, which helps make the process more power efficient. The pause symbol next to the Calculator app indicates that this app is suspended, so it isn't using a lot of system resources. Suspended apps—often minimized apps that you haven't used in a while—run as background apps.

TECH TIP

Task Manager tabs are missing

If the menu bar and tabs are missing from Task Manager while you are looking at a resource in the Performance tab, then Task Manager is in Tiny Footprint mode. Double-click an empty space in the top border to make the menu and tabs reappear.

The Task Manager *Performance tab* (see Figure 16.49) shows performance indicators for key computer components, including the CPU, disks, Ethernet and Wi-Fi for network connectivity, Bluetooth, and GPU. When a user complains about a computer being slow, this is one of the first places a technician should look.

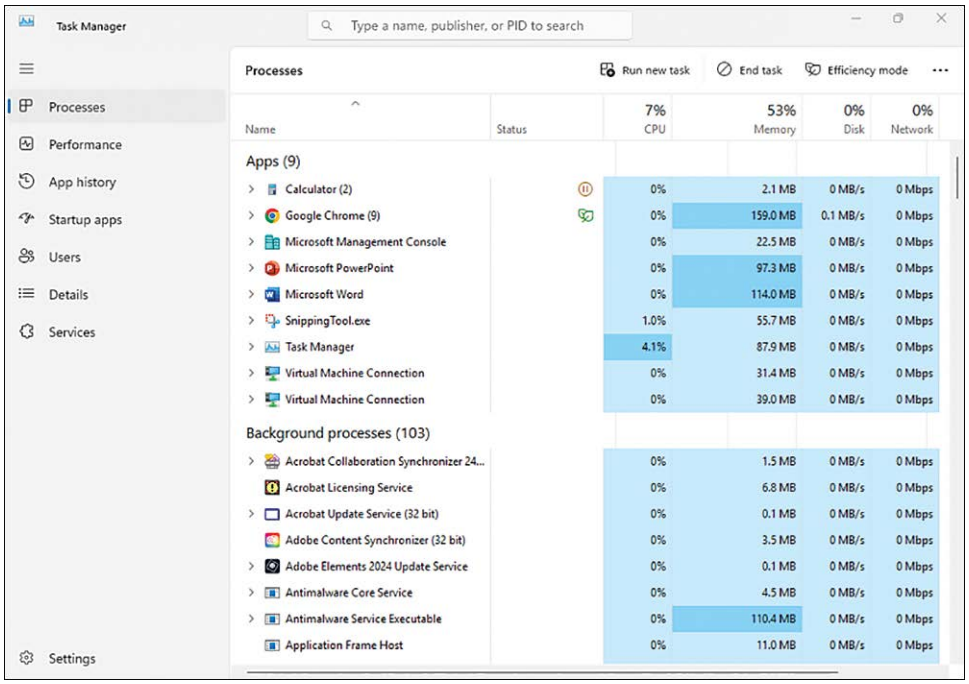


FIGURE 16.48 Windows Task Manager: Processes tab

The Task Manager *App history* tab shows resource usage for individual applications, including parameters such as CPU time, network utilization, downloaded data, and metered network utilization. This is especially helpful with mobile devices to identify which applications are using resources so that you can disable them to conserve battery power.

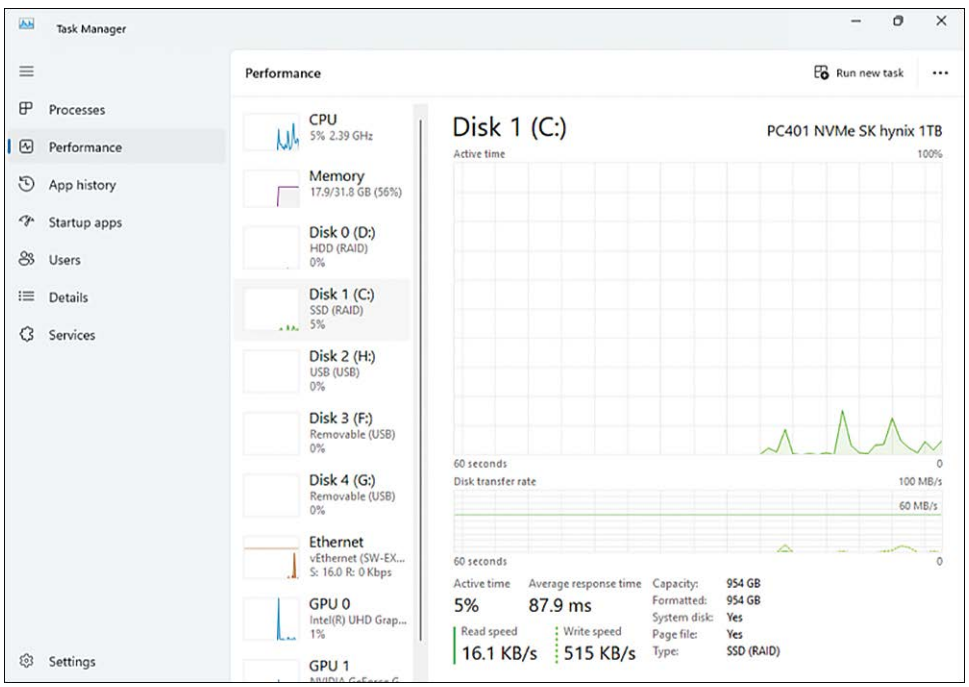


FIGURE 16.49 Windows Task Manager: Performance tab

The Task Manager *Startup apps* tab is used to see any app that executes as part of the Windows startup routine. The *Startup impact* column lets a technician know how much the application impacts the startup time. By right-clicking on a particular application, you can disable or enable the item, view its properties, or open the location of its `.exe` file or script file.

TECH TIP

Windows 10/11: Start an application during startup

In Windows 10/11, you can use the *Settings* > *Apps* > *Startup* option to turn on any app that you would like to start automatically as part of the Windows boot process.

The Task Manager *Users* tab shows which users are logged on. You can also use this tab to disconnect another user who is logged on, such as when two people share a work cubicle and the other person forgot to log out. The *Users* tab shows, in table format, what resources that user is using.

The Task Manager *Details* tab shows more information on the processes that are running. Note that the processes that appear here may not be shown in the *Processes* tab or *Performance* tab. The process ID (PID) is also shown here.

The Task Manager *Services* tab is a handy place to see what services are currently running or stopped. You can also start, stop, and restart services from this tab. Note that not all services are shown here and that services cannot be fully configured here. The *Open Services* link provides access to *Services*, where you can see a list of all services available on the computer, including services that were started but that have a delayed startup type.

TECH TIP

What to do if a system appears to lock up or is slow

If a system appears to lock up or is slow, give the system some time to try to respond. If you get no response, access Task Manager by pressing Ctrl+Alt+Del. Keep in mind that it might take a bit of time for Task Manager to open. Access the *Processes* tab > locate and select the troublesome application > *End task* button. Normally, if an application is causing a problem, the status shows the application as "not responding." If Task Manager never appears, power down the computer and reboot.

Monitoring System Performance

It is important for a technician to understand how a computer is performing and to analyze why a computer might have **slow performance** (see Figure 16.50). A technician must know what applications are running on the computer and their effects on the computer's resources. A technician must also monitor the computer's resource usage when problems occur, change the configuration as needed, and observe the results of configuration changes. Utilities commonly used to monitor system performance include Task Manager, Performance Logs and Alerts, Reliability Monitor, and Performance Monitor.

Sometimes computers seem sluggish. The most common causes of a slowdown are that the computer's resources are insufficient or an application is monopolizing a particular resource, such as memory. Other causes of slowdowns include a resource such as a hard drive not functioning properly or being outdated, a resource not being configured for maximum performance and needing to be adjusted, and resources such as hard drive space and memory not sharing workloads properly and needing adjustment.

FIGURE 16.50 Slow performance

Viewing system performance when a problem occurs is good, but it is easier to figure out what is happening if the normal performance is already known. A baseline can help with this. A **baseline** is a snapshot of computer performance during normal operations (before the computer has problems). Task Manager can give you an idea of what normal performance is. The Windows Performance Monitor and Reliability Monitor tools are better suited to capturing and analyzing specific computer resource data.

TECH TIP

When do I need to do a baseline of a computer?

A baseline report is needed before a computer slowdown occurs.

Using Task Manager to Measure Performance

Although Task Manager is discussed earlier in this chapter, how to use it to monitor computer performance has not yet been discussed. Using Task Manager is the easiest and quickest way for anyone to quickly and visually see how a computer is performing. If you access *Task Manager* and select the *Performance* tab, Task Manager immediately starts gathering CPU and memory usage statistics and displays them in a graph. You can see graphs for CPU performance, memory, disk drives, Ethernet, and Wi-Fi performance, as shown in Figure 16.49.

TECH TIP

What to do if you think memory is the problem

To address a memory problem, make sure each RAM module is properly installed in the motherboard. After that, you can run the Windows Memory Diagnostics Tool, replace or add RAM, create multiple paging files if multiple hard drives are installed in the system, manually set the paging file size, run one application at a time, close unnecessary windows, upgrade or add another hard drive, delete unused files, and defragment or optimize the hard drive. See "Troubleshooting Memory Problems" in Chapter 6, "Memory," for more details about each of these methods.

The *CPU* tab shows the processor usage percentage—that is, the percentage of time the processor is working. Actually, it is more accurate to say that *CPU* shows the percentage of time the processor is running a thread. A *thread* is a type of Windows object that runs application instructions. The window on the right in the Task Manager is a graph of how busy the processor is over a period of time (Figure 16.49).

Memory is frequently a bottleneck that causes computer performance issues. When available memory is extremely low, you might get the error message "Your Computer is running low on memory." You can use the *Memory* option on the left side of the *Performance* tab in Task Manager to see the total amount of RAM installed, how much RAM is available, and statistics regarding memory. The amount of physical RAM installed appears in the upper-right corner. If you suspect that a RAM module is not working properly, you can use the Windows Memory Diagnostics Tool to check the health of the modules.

The information at the bottom of the *Memory* tab shows the physical RAM and virtual memory (hard drive space called a paging file that is used as if it were RAM). Note that virtual memory might be referred to in articles, documentation, or the CompTIA certification as system **performance (virtual memory)** because any computer's virtual memory affects performance. If you think the paging file for virtual memory is too small, you can adjust it with the following steps:

Step 1. Search for and access the *System* section of the Control Panel > *System protection* > *Advanced* tab > *Performance* section *Settings* button.

Step 2. Select the *Advanced* tab.

Step 3. In the *Virtual memory* section, look at the total size of the paging file. Click the *Change* button, deselect the *Automatically manage paging file size for all drives* checkbox, and make appropriate adjustments (see Figure 16.51).

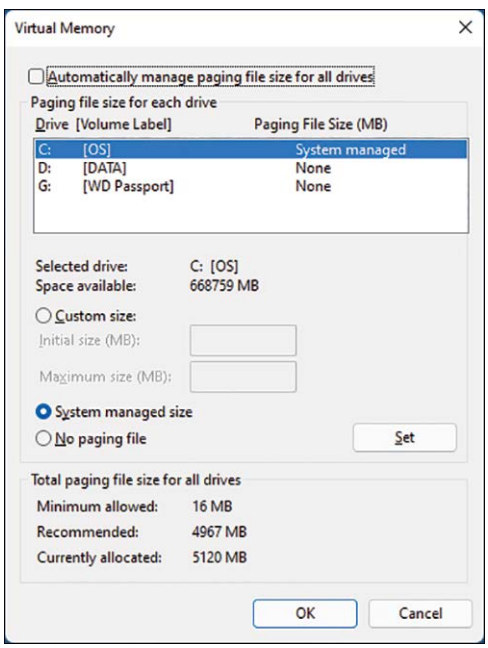


FIGURE 16.51 Manually configuring the paging file (virtual memory) size

To see how much memory an individual process is using, select the *Processes* tab of Task Manager and locate the program executable file. The CPU and memory usage are shown in separate columns on the *Processes* tab. To display additional columns (such as GPU or Power usage), right-click on an existing column and then enable the desired columns.

Click on a particular network card (including Bluetooth) on the left side of the *Performance* tab to see a graph of network performance for that interface. Figure 16.52 shows the Task Manager *Performance* option for an Ethernet card.

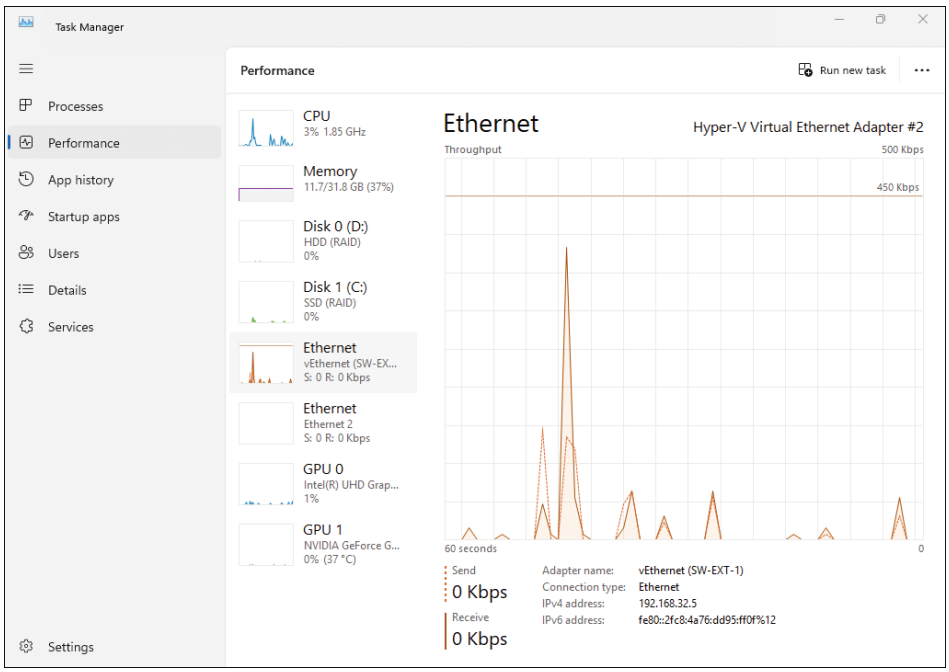


FIGURE 16.52 Task Manager: Performance tab, Ethernet

The Task Manager *Users* tab shows users that are logged on to the computer and specific performance statistics regarding CPU, memory, disk, and network for each particular user. This is probably one of the least used Task Manager tabs in both corporate environments and at home. However, if multiple people are logged on, one of them might have a particular application or service running that is causing the machine to slow down, so it is important to know about this tab.

Performance Monitor

Performance Monitor (`perfmon.msc`) is a visual graph based on real-time data saved in a log file that provides information on specific computer components. Use the *System and Security* section of the Control Panel > *Administrative Tools* > double-click *Performance Monitor*. After the Performance Monitor window opens, click *Performance Monitor* under *Monitoring Tools*. Performance Monitor shows counters, which provide specific measurements for objects. Common objects include cache, memory, paging file, physical disk, processor, network interface, system, and thread. Use the green + (plus sign) in Performance Monitor to select various counters. At the bottom of the window is a legend for interpreting the graph, including what color is used for each of the performance measures and what counter is used. Table 16.19 shows common counters used in Performance Monitor, and Figure 16.53 shows an example of Performance Monitor.

TABLE 16.19 Performance Monitor counters

Computer component	Object name	Counters
Memory	Memory	Available Bytes and Cache Bytes
Hard disk	Physical disk	Disk Reads/sec and Disk Writes/sec
Hard disk	Logical disk	% Free Space
Processor	Processor	% Processor Time (All Instances)

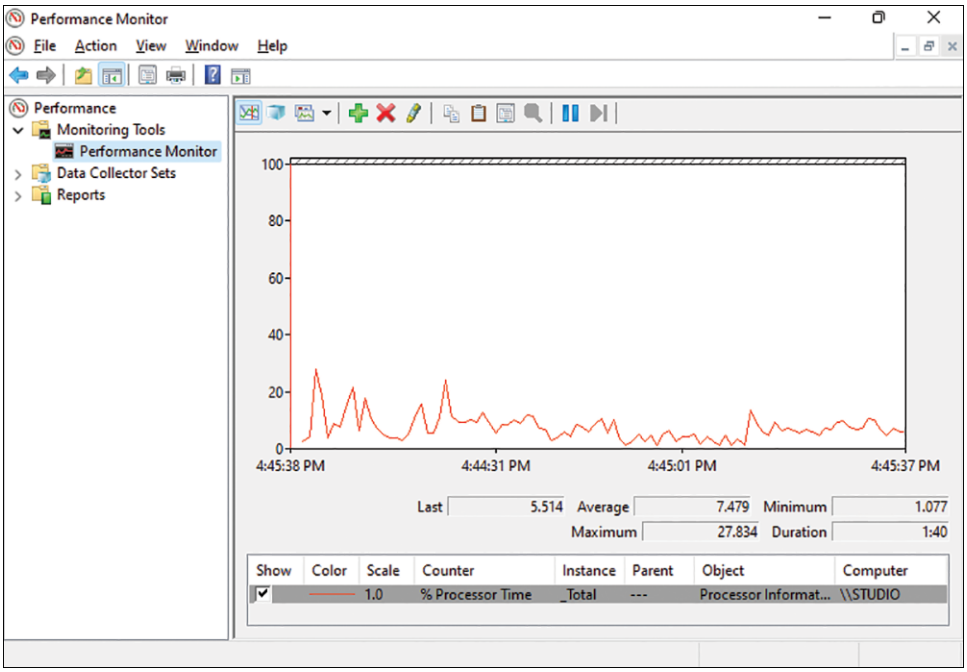


FIGURE 16.53 Windows Performance Monitor

Resource Monitor

The Windows **Resource Monitor** (`resmon.msc`) is a nice graphical tool that requires little work and shows the main components of a system. Access the tool by selecting the *Open Resource Monitor* link from within the Performance Monitor window or access the *System and Security* section of the Control Panel > *Administrative Tools* > double-click *Resource Monitor*. Figure 16.54 shows Resource Monitor.

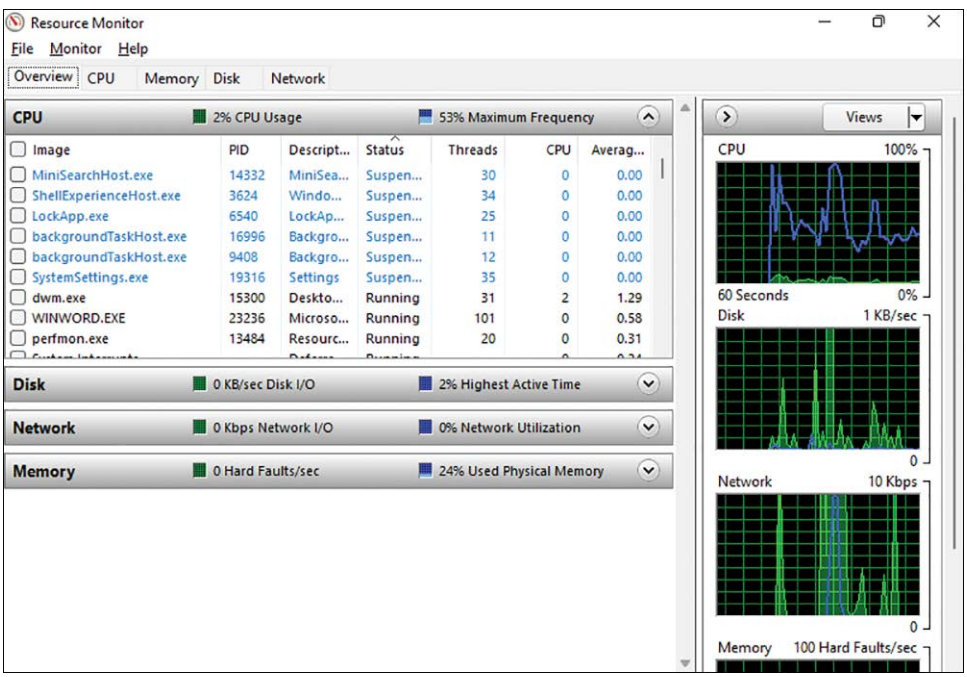


FIGURE 16.54 Windows Resource Monitor

Running any performance monitoring tool affects a computer's performance, especially when using the Graph view and sampling large amounts of data. The following recommendations help when running any performance monitoring tool:

> Turn off any screen saver.
> Use Report view instead of Graph view to reduce resource use.
> Minimize the number of counters monitored.
> Sample at longer intervals, such as 10 to 15 minutes, rather than at short intervals, such as a few seconds or minutes.

Windows **Reliability Monitor** provides a visual graph and detailed report of system stability, as well as details on events that might have affected the computer's reliability. The details can help technicians troubleshoot what has caused the system to become unreliable. You can open Reliability Monitor by entering `reliability monitor` in the *Search* box on the taskbar. Figure 16.55 shows this tool.

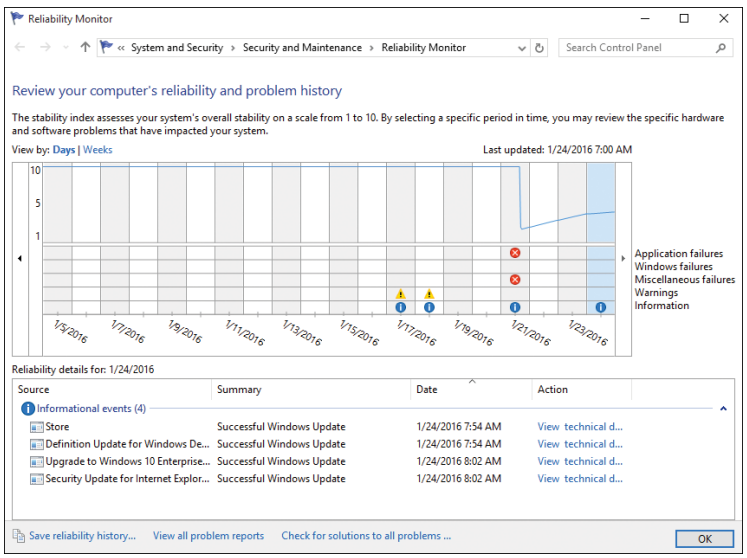


FIGURE 16.55 Windows Reliability Monitor

Speeding Up the Windows Boot Process

Windows can seem to take forever to boot (especially if you do not have an SSD), but there are things a technical person can do to help speed up the OS boot process (see Figure 16.56).

FIGURE 16.56 Fine-tuning the startup process

The following tips can help reduce the time it takes Windows to become operational:

- Configure BIOS/UEFI boot options so that the drive used to boot Windows is listed as the first option.
- Configure BIOS/UEFI for the fast boot option or disable hardware checks.
- Enable *Turn on fast startup* in *Power Options* > *Define power buttons* > *Choose what the power buttons do*. See the section "Power Options," later in this chapter.
- If multiple operating systems are installed, use the `msconfig` utility *Boot* tab to reduce the boot menu timeout value.
- Remove unnecessary startup applications by using the `msconfig` utility. Use the *Startup* tab in *Device Manager.*
- Ensure that you have hard disk space available and keep the drive defragmented or optimized. Note that Windows is automatically configured to defragment or optimize the hard drive at 1:00 a.m. on Wednesday. If the computer is powered off at that time, the maintenance occurs when the computer next boots.
- Disable unused or unnecessary hardware by using Device Manager.
- Use Windows **ReadyBoost** to cache some startup files to a 256 MB+ flash drive, SD card, or CF card. Right-click the storage device to access the *Properties* option and select the *ReadyBoost* tab. Note that ReadyBoost does not increase performance on a system that boots from an SSD, so Windows disables the ReadyBoost option when an SSD is in use.
- Use the *Administrative Tools* Control Panel > access *Services*. Change services that are not needed the moment Windows boots to use the *Automatic (Delayed Start)* option instead of *Automatic*.

Troubleshooting the Windows Boot Process

Troubleshooting the boot process when Windows will not load (**failure to boot**) is sometimes easier than troubleshooting other types of problems that can occur in the operating system. You can try several tools, but keep in mind that you may need to reload the operating system.

TECH TIP

Troubleshooting, repair and recovery

There is risk associated with all troubleshooting, repair, and recovery options. Therefore, you should be sure to back up any critical files, software, drivers, and operating system installation media.

If a computer locks, has a BSOD, becomes unstable, or will not start, try the following:

- If Windows fails to load the login prompt two consecutive times, it automatically runs Automatic Repair on the third boot attempt. Automatic Repair gives you two options: Restart the system immediately (which might fix the problem) or enter the Windows Recovery Environment.
- Check the BIOS/UEFI setting to ensure that the boot order is correct.
- Remove the power cord and leave the computer powered down for one to two minutes. Then reinsert the power cord and power on the computer again. Make note of any beeps or error codes. Use these symptoms to start your troubleshooting process.

- Determine the last thing that was done before the computer refused to boot. If possible, boot the computer to Safe Mode. Use the System Restore utility to bring the computer back to a date before the issue occurred. The following are some questions to ask the user:
  - Did a Windows Update just occur?
  - Was an application recently installed?
  - Was any hardware added recently?
  - Did any type of application update just occur?
- Examine the list of startup items. Use the *Startup* tab in *Device Manager* to remove unfamiliar or unexpected entries.
- Disconnect any unnecessary peripherals from the computer, leaving just the power and monitor connected. If the computer starts, connect peripherals one by one while (restarting after device is added) to see which item is causing a boot to fail.
- Boot to Safe Mode and run the System File Checker (`sfc`) to replace missing or corrupt operating system files or load an appropriate graphics driver.
- Use the **Reset this PC** option in *Settings* > *Recovery*. This option reinstalls Windows and gives you the choice of whether you keep the files, remove everything, or, on some computers, restore to factory settings (including Windows and the apps that came with the computer when you bought it).
- Use the *System Image Recovery* option that is available in the Windows Recovery Environment. This option reloads a specific Windows image file. If the image is loaded onto the same volume as an existing Windows installation, all files (operating system, software installations, drivers, user documents, and so on) are deleted.

Quite a few things can cause Windows to fail to boot into the graphical interface properly. For example, a nonbootable disk listed as the first boot device or nonbootable media inserted into an optical drive (and listed as a boot device) can cause Windows not to boot. If none of the hard drives contain an active partition or if the hard drive's boot sector information is missing or corrupt, any of the following messages or events could appear:

- *Invalid Partition Table*
- *Error Loading Operating System*
- *Missing Operating System*
- `BOOTMGR` *Is Missing*
- *Windows Has Blocked Some Startup Programs*
- *The Windows Boot Configuration Data File Is Missing Required Information*
- *No OS found*
- *Windows Could Not Start Because the Following File Is Missing or Corrupt*

Also, if you receive a message indicating that you have an invalid boot disk, a disk read error, or an inaccessible boot device, troubleshoot your hard drive and/or BIOS/UEFI settings.

TECH TIP

How to stop programs that automatically load at startup from running

To disable startup programs, go to *Task Manager* > *Startup* > select a program > click *Disable*. You can also go to *Settings* > *Apps* > *Startup*. Locate each program that you don't want to load at startup and slide its switch to *Off*.

If a startup problem occurs before the Starting Windows logo appears (**graphical interface fails to load**), the cause is typically missing startup files, corrupt files, or hardware problems.

You can use the Windows command `bootsect /nt60 all` (or a drive letter instead of `all` if multiple operating systems are installed) to manually repair the boot sector. The `bootsect.exe` file is available from the `Boot` folder of the Windows installation media and can be executed from WinRE (covered earlier in this chapter) or from within Windows.

If the Windows logo appears but there is a problem before the logon prompt appears, the problem is usually with misconfigured drivers and/or services. If problems occur after the logon window appears, investigate the startup applications or see if the `userinit.exe` file has issues. Use the *Advanced Boot Options* startup menu, and from a command prompt, use the `sfc /scannow` command to fix the `userinit` file.

Black Screen/Video Issues

During the boot process, Windows loads a default video driver to avoid issues due to video driver incompatibility. If video is a problem while working in Windows (that is, if you get a **black screen** or a blank screen), check your video power and cabling, boot to *Safe Mode* or restore a restore point, and load the correct driver. You could also perform a driver rollback if a new driver has just been installed.

To save time booting into Safe Mode, you could use the *System Configuration* (`msconfig`) tool > *Boot* tab > enable the *Base video* checkbox > *OK* (see Figure 16.57).

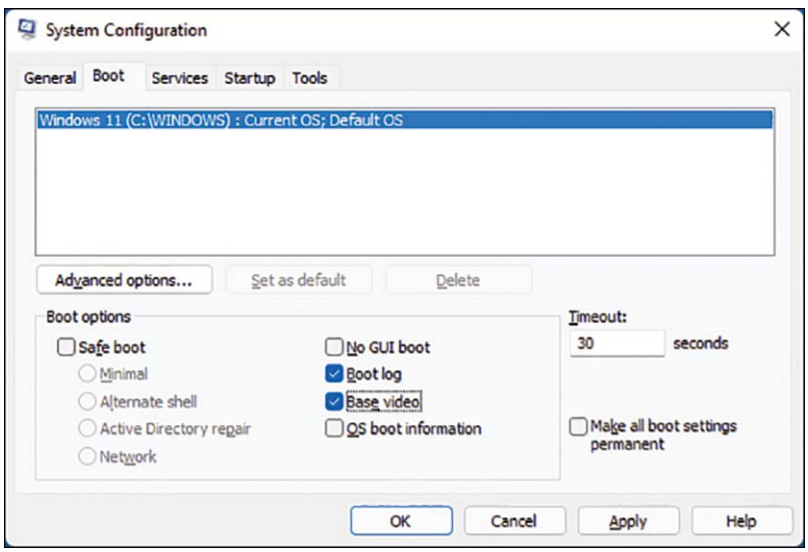


FIGURE 16.57 System Configuration > Boot tab

If multiple monitors are installed, another option is to verify that each monitor has power and the data cable attaches securely. Check the monitor settings to verify that the monitor detection is accurate. In Windows 10/11, use the *Settings* > *System* > *Display* option. You can also right-click on an empty space on the Desktop and click *Display settings*.

TECH TIP

Display is dark

If the display is dark, check to see whether the computer is in sleep mode or won't come out of sleep mode. Check the video cable. Hold down the power button and try restarting. Check the power management settings.

TECH TIP

BSOD after a Windows update

Always research the error code associated with a failed update. Windows updates include device driver updates. If a computer fails to boot after a Windows update, reboot the computer to WinRE Safe Mode and use the System Restore tool to restore the registry to an earlier time so that the problem can be researched. If multiple updates were installed, try loading the updates one at a time.

Use System Restore if you suspect that the registry is corrupt. For example, if an application worked fine yesterday but today displays a message that the application cannot be found, you may have a virus, a corrupt application executable file, or a corrupt registry. Run an antivirus check first with updated virus definitions. If free of viruses, use the System Restore utility to roll back the system to yesterday or the day before this problem occurred. Sometimes System Restore works best if executed from Safe Mode. If System Restore does not fix the problem, reinstall the application.

Access the window to configure System Restore by searching for the *System* section of the Control Panel > *System protection* link > *System Protection* tab. Figure 16.58 shows how you can select a specific date during the System Restore process. You can also select the *Show more restore points* checkbox at the bottom of the window to see more restore points.

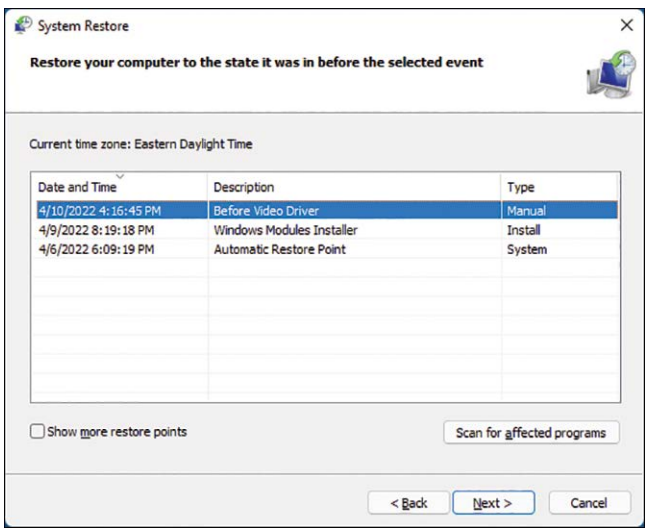


FIGURE 16.58 Windows System Restore

TECH TIP

You can run System Restore from a command prompt

If Windows does not load properly, you can execute System Restore from a command prompt with the command `%systemroot%\system32\rstrui.exe`.

Troubleshooting a Service That Does Not Start

Some Windows services start automatically each time the computer boots. If one of these services has a problem or if a particular **service fails to start**, normally an error message appears during the boot sequence. You can use the System Configuration utility (`msconfig`) discussed

previously to enable, disable, or **restart services**. You can also use Event Viewer to see if the service loaded properly.

Another program that you can use is the Services snap-in. You can access it from the Computer Management tool, or, at a command prompt, type `services.msc` and press [Enter]. The *Services* tool allows you to fully configure and monitor the services, including what services have started and stopped and, if desired, enables you to **disable a service**. In the *Services* snap-in (see Figure 16.59), the services are listed in alphabetical order. You can click the column headings to change the sort order.

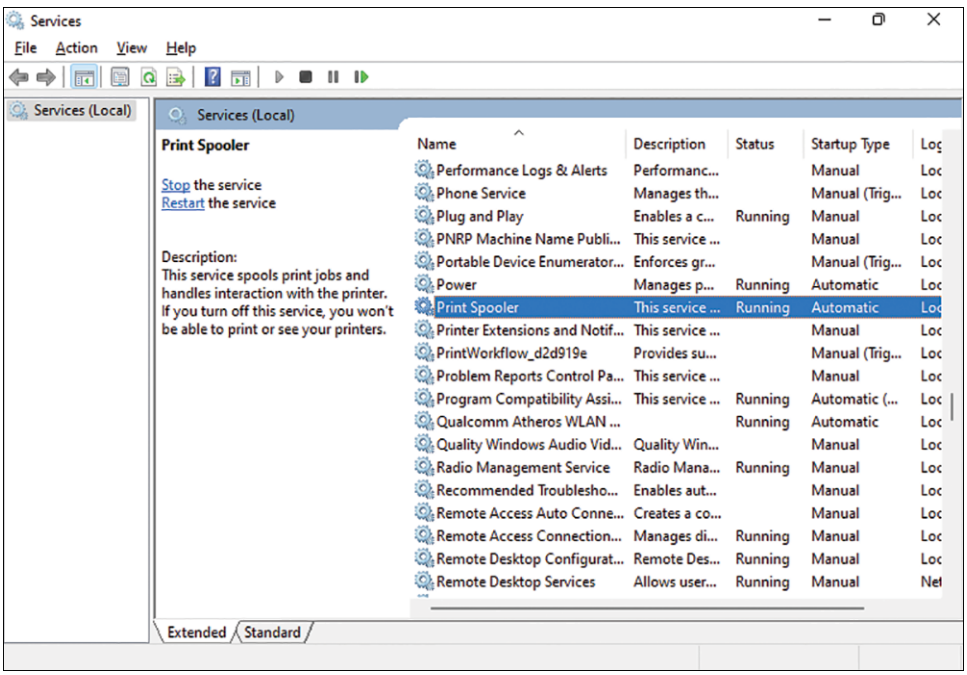


FIGURE 16.59 Windows Services

Double-click a service to learn more about it. Through the window that appears, as shown in Figure 16.60, you can control whether the service starts automatically, starts manually, or is disabled. Notice in Figure 16.55 that, because the Print Spooler service is already running, the only action that can be performed is to stop the service.

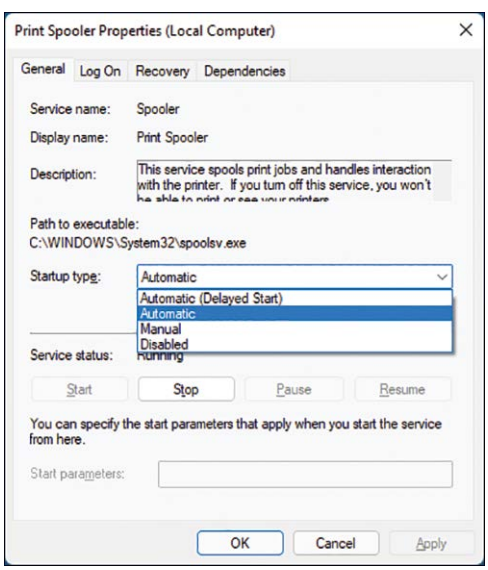


FIGURE 16.60 Controlling a Windows service

Slow Boot

When a **slow boot** problem is reported to you, several issues could be the culprit. The operating system could be running slowly, the hard drive could be lacking free hard drive space, there might be too many startup applications or services running, or there might be too many startup login scripts. If you recently installed an app, restore the system from a system restore point. If you just received a Windows update or an application update, remove that update.

If you suspect that the operating system is the problem, use Safe Mode when the computer stalls, slows down, or does not work correctly or when there are problems caused by improper video, intermittent errors, or newly installed hardware/software. Safe Mode can start Windows with minimal device drivers and services. Software that automatically loads during startup is disabled in Safe Mode, and user profiles are not loaded.

Two other tools that are really helpful with a slow boot are the System Configuration utility and the *Services* tool in Computer Management, both of which are covered earlier in this chapter. In the System Configuration utility, use the *Startup* tab to determine which applications are configured to load as part of the startup process. See if some of them can be disabled (unchecked). One application in particular might be causing the slowness. With the *Services* Computer Management tool, look in the *Startup Type* column to see if any of the services that automatically start can be changed from *Automatic* to *Automatic (Delayed Start)*. To change the startup type, double-click the service and use the *Startup Type* drop-down menu.

You can also use the *Reset This PC* option in *Settings* > *Recovery* to reinstall the operating system. If you have a recovery drive, you might need to use it to restore or reset the PC. The best approach is to take care of the problem as soon as you can and prevent it from getting worse.

Slow Profile Load or Profile Problems

Companies use login scripts that run every time a user logs on to a computer. Such a script can reference a local profile, a domain profile, or both. (Profiles are covered in detail in Chapter 18.) A problem that might be reported to you as a slow boot problem may actually relate to a **slow profile load**. Loading a large profile or multiple profiles (for example, a personal one, one that is part of a group, and/or a local one) can cause the user to have to wait a long time for the computer to execute.

The operating system might also display a message indicating that the user profile cannot be loaded. The user profile could be corrupted; in this case, you have to **rebuild a Windows profile**. One way to fix this is to create a new account and copy the files from the old user account. Otherwise, you will have to make changes to the registry, as described in the following steps:

Step 1. Use an account that has administrator rights to log in to the computer in Safe Mode.

Step 2. At a command prompt, use the `set` command to look for `USERPROFILE=` to see the problematic user profile.

Step 3. Rename the folder associated with the user profile, such as `C:\Users\CSchmidt`, to something like `Cschmidt.old folder`.

Step 4. Look to see if a temporary profile was created in the `C:\Users\TEMP` folder. Delete the profile if there is one.

Step 5. Access the registry and export it to an external drive as a backup.

Step 6. Locate the key `Hkey_Local_Machine\Software\Microsoft\Windows NT|CurrentVersion\ProfileList`.

Step 7. Click on each SID key (folder) under `ProfileList` and find the `ProfileImagePath` that matches the user that has the profile issue.

Step 8. Delete or rename the SID registry key with the matching path. For example, if the SID S-1-5-21-3423371916-2792405005-1110847961-1008 contains the `ProfileImagePath` value `C:\Users\CSchmidt`, you delete that SID.

Step 9. Restart the computer and log in with the user profile that had the problem. You will have to copy the user's data from the `.old profile` folder.

Troubleshooting Windows Network Settings

Remember that most corporate devices connect to a wired or wireless network. (Troubleshooting network settings is covered in detail in Chapter 13, "Networking.") If a user cannot access the network, be sure to check the Windows network settings and keep in mind that you might have to **update network settings** to fix the problem. Check the following:

- For a wired network, confirm that the network cable is securely connected to the computer and the network jack. If the link lights on the computer don't come on, check the connections from the network jack to the switch and make sure the switch is working properly.
- If the device is a wireless one, see if the device is connected to the appropriate wireless network.
- Use the *Settings* > *Network and internet option* to see if the network is connected to the internet.
- Use the `ipconfig` command to see if the device has the appropriate IP address, subnet mask, and default gateway. Remember that without a default gateway, the device cannot access any resource outside its own network. In most situations, the required servers and connectivity will be outside the local network.
- If the device is supposed to use static addressing, obtain the appropriate IP settings from the system administrator and use this procedure:
  1. Right-click on the wired or wireless NIC in the *Network Connections* section of the Control Panel > *Properties* > select *Internet Protocol Version 4 (TCP/IPv4)* > *Properties* > *Use the following IP address* radio button.
  2. Input the appropriate settings > *OK* > *OK*.
  3. Enter the `ipconfig` command to verify that the settings were applied to the appropriate adapter.
- If the device has an IP address that starts with 169 and it's supposed to have a DHCP address, use the `ipconfig /release` and `ipconfig /renew` commands to get a proper DHCP IP address.
- Another way to force the computer to request a new DHCP address is to configure the computer for static addressing and then switch to dynamic address. Use this procedure:
  1. Right-click on the wired or wireless NIC in the *Network Connections* section of the Control Panel > *Properties* > select *Internet Protocol Version 4 (TCP/IPv4)* > *Properties* > *Use the following IP address* radio button.
  2. Input any valid IP address and mask > *OK* > *OK*.
  3. Re-access the same TCP/IPv4 settings window and enable the *Obtain an IP address automatically* radio button to receive IP address settings from a DHCP server > *OK* > *OK* (see Figure 16.61).
  4. Use the `ipconfig` command to verify that the appropriate adapter received (at a minimum) an IP address, subnet mask, and default gateway, as shown in Figure 16.62.

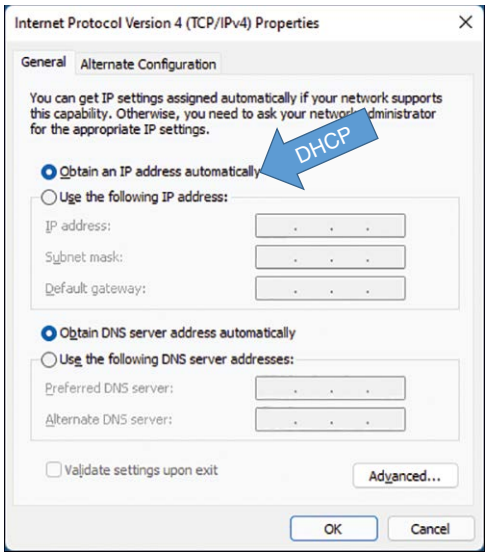


FIGURE 16.61 Configuring a Windows PC for DHCP services

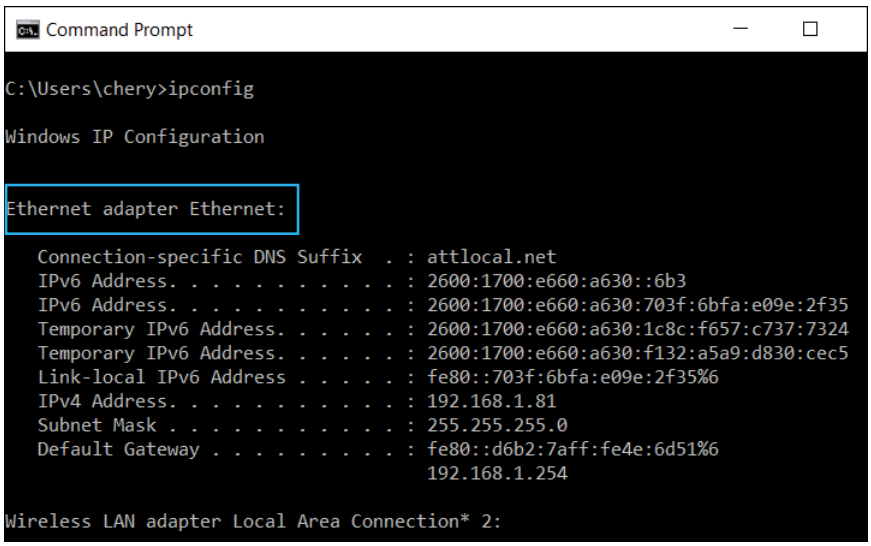


FIGURE 16.62 Verifying IP addressing information by using `ipconfig`

Windows Reboots/System Instability

Intermittent problems are some of the hardest problems to solve. When Windows reboots or shuts down unexpectedly, a lot of different things could be the cause. Spontaneous reboots could be caused by a newly installed Windows update, newly installed application, or newly updated driver. A corrupt device driver could also be the culprit, but that is hard to find. An internet search on your specific hardware device might speed up the troubleshooting process.

A spontaneous reboot can also be caused by a virus or malware. See Chapter 18 for more on those security issues. Other hardware issues could be the RAM, processor, video card, or hard drive. You can see why the cause of spontaneous reboots is one of the hardest problems to narrow down.

Spontaneous reboots are different from spontaneous shutdowns. Spontaneous shutdowns tend to be heat-related problems. Check the CPU fan and the case fans and ensure that the heatsink is properly secured to the motherboard. If the heatsink is loose, remove the existing thermal paste from the CPU and heatsink, apply new thermal paste, and then reattach the heatsink. Some BIOS/UEFI

menus have options that display internal temperatures. Start noting temperature readings. A failing CPU, overloaded power supply, or failing power supply could also cause a spontaneous shutdown.

Shutdown Problems

Windows should be shut down properly when all work is finished. Before Windows can shut down, the operating system sends a message to all devices, services, and applications. Each device or system service that is running sends back a message, saying it is okay to shut down now. Any active application saves data that has not been previously saved. If the application cannot save the data automatically, the user is given the opportunity to do so. After the data has been saved, the application sends a message back to the operating system, indicating that it is okay to shut down.

If the system has trouble shutting down, it may be due to devices, services, or applications. The most common problem is an application that does not respond. When this happens, open Task Manager. Manually stop any applications that show a status of not responding. You may also click any other applications and stop them to see if they are causing the problem. Sometimes a program does not show a status of not responding until you try to manually stop the application from within Task Manager. If a single application continually prevents Windows from shutting down, check online or contact the software manufacturer to see if there is a fix.

TECH TIP

Try the restart option instead of the shutdown option

If you cannot stop a problematic application or determine whether the problem is a service or a hardware issue, try restarting the computer instead of shutting it down. After the computer restarts, try shutting down again. As a last resort, use the computer power button to power off the computer. If even this does not work in a laptop, remove the battery (if possible).

For problems related to Windows services, boot the computer into Safe Mode and then shut down the computer. Notice whether the computer had any problems shutting down. If the process works, use the *System Configuration* > *General* tab > *Selective Startup* radio button and the *Services* tab to selectively disable services. Because there are so many services loaded, you might try the divide-and-conquer method: Disable one-half of the services to narrow the list.

Devices do not frequently cause shutdown problems, so eliminate services and applications first. Then, while working on the computer, notice what devices you are using. Common devices are video, hard drive, optical drive, keyboard, and mouse. Access the Advanced Boot Options menu in *WinRE* > *Troubleshoot* > *Advanced Options* > *Startup Settings* > *Restart*. After the computer boots, select *Enable boot logging* and the computer will restart again. When the system boots, locate the `ntbtlog.txt` file in the `Windows` folder. You may have to set folder options in File Explorer to list the file and access it. Verify that all your devices have the most up-to-date drivers loaded and that the drivers are compatible with the installed version of Windows.

Sometimes USB or IEEE 1394 FireWire ports can stop a computer from shutting down or powering off. Check the event logs to see if any device did not enter a suspend state. A feature called *USB Selective Suspend* allows the Windows hub driver to suspend a particular USB port and not affect the other USB ports. Suspending USB devices when a device is not in use conserves power. This is particularly important with laptops, netbooks, and ultrabooks because of power consumption. If USB device suspension is causing the problem, this default behavior can be modified by using the *Power Options* section of the Control Panel: Click *Change plan settings* for the active plan > *Change advanced power settings* > *USB settings* > *USB selective suspend setting* > *Disabled* > *OK*.

Summary of Troubleshooting Steps

The previous sections offer troubleshooting advice specific to a variety of topics. Use troubleshooting steps in the order listed below to minimize the impact on a system's operating system, configurations, applications, and data:

Step 1. Save and close any open applications.

Step 2. Verify hardware, OS, and application requirements. Add resources (RAM, disk space, upgraded hardware) as needed and when convenient to the user and overall operation.

Step 3. Confirm that a recent backup is available or create a new one.

Step 4. Run a system file check.

Step 5. Restart services.

Step 6. Reboot the system.

Step 7. Rebuild Windows profiles.

Step 8. Run appropriate troubleshooting wizards.

Step 9. Update, reinstall, or uninstall applications.

Step 10. Use System Restore to remove recent configuration changes and/or roll back updates in Windows Update.

Step 11. Reboot into Windows Recovery Console and run Automatic Repair.

Step 12. Reimage the entire system using a backup image or do a clean install and then apply updates.

Power Options

Windows has three customizable power plans available. You can access the Power Options Control Panel via *Control Panel* > *System and Security* > *Power Options* (see Figure 16.63). To configure a plan, click the *Change plan settings* link followed by *Change advanced power settings*. Next, expand a section, such as *Multimedia settings*, and configure its settings. These are the three main power plans:

- **Balanced:** This is the most common plan. It provides full power when you need it and saves power when the computer is not being used.
- **Power Saver:** This plan saves power by running the CPU more slowly and reducing screen brightness.
- **High performance:** This plan provides the maximum performance possible, but the computer might consume more energy.

Additional plans might be available from the computer manufacturer. Depending on the version of Windows and the manufacturer, you might need to select the *Show additional plans* link.

The *Power Options* Control Panel also includes the *Choose what the power buttons do* option. As shown in Figure 16.64, you can control how the computer responds when the power and sleep buttons are pressed. Possible selections include *Do nothing*, *Sleep* (maintain the system state in RAM in a low-power mode), *Hibernate* (save the system state to the hard drive and turn off the computer), *Shut down*, and *Turn off the display*.

When the computer enters hibernation, the contents of RAM are copied to the hiberfile (`hiberfil.sys`), and then the computer shuts down. When the computer is turned back on, `hiberfil.sys` is copied back into RAM, restoring the previous state. Note that the *Hibernate* option appears only if the motherboard supports hibernation. If the motherboard has this feature

but *Hibernate* does not appear, run the command `powercfg /hibernate on` from an elevated command prompt and then open *Power Options* again.

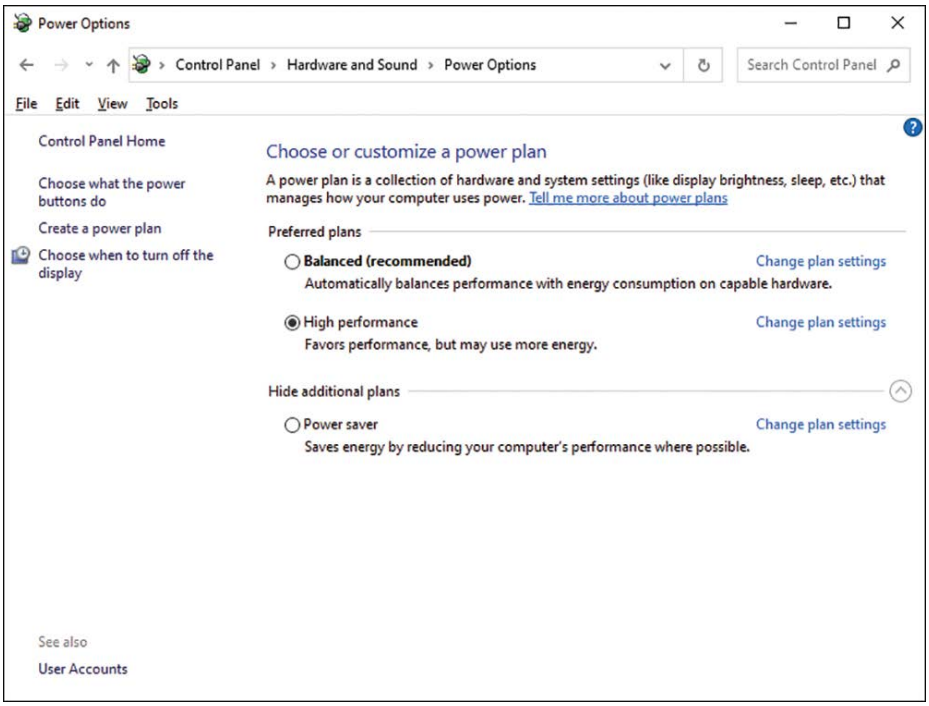


FIGURE 16.63 Power Options section of the Control Panel in Windows 10

Choose what the power buttons do > *Turn on fast startup (recommended)* can be used to speed up the boot process. It is available only if hibernation is enabled. During a normal startup, the boot loader copies sections of the Windows kernel from the hard drive into RAM and links them, and then it loads required drivers in memory. When fast startup is enabled, the system saves an image of the Windows kernel and loaded drivers to the hiberfile every time the computer is shut down. When the computer is turned back on, the kernel and drivers are loaded directly to RAM.

Laptop computers also have the option *When I close the lid* when you click *Change what the power buttons do*. For example, if an external monitor is connected to a laptop, the computer can be configured to stay on when the lid is closed. Laptops also allow for separate settings based on power source (*On battery* or *Plugged in*).

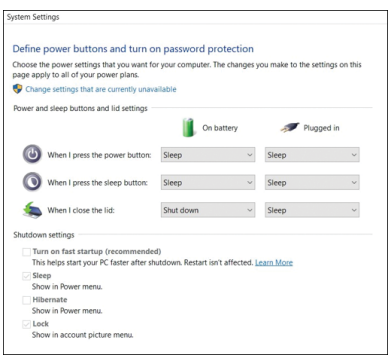


FIGURE 16.64 Define power buttons section of the Control Panel (laptop version)

Supporting Windows Computers Remotely

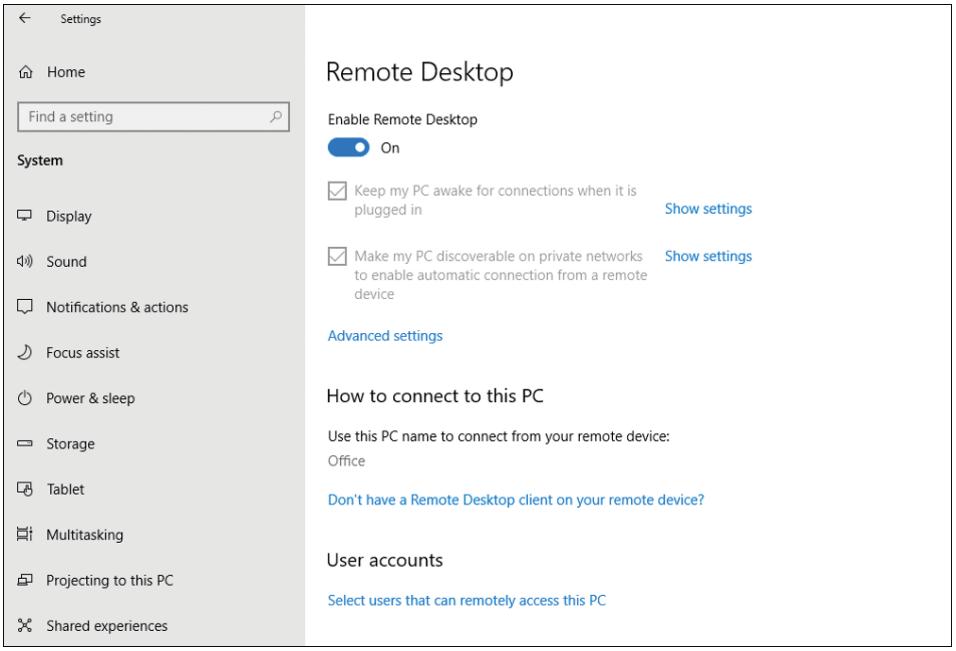
Windows provides two products for accessing a PC remotely: **Remote Desktop Connection** and **Remote Assistance**. Both of these products are useful for those working at a help desk and for technicians who must support computers in other locations. There are some key differences between these two products:

> Remote Desktop Connection allows full control of the remote desktop, whereas Remote Assistance only allows viewing of the remote desktop.
> Remote Desktop Connection requires network connectivity between the controlling computer and the remote computer (or a VPN connection through the internet).
> Remote Assistance displays a prompt at the remote computer, asking permission to allow the computer to be viewed remotely, and Remote Desktop Connection does not display this prompt.

Using Remote Desktop Connection (the `mstsc` command) requires the following elements:

> The local computer that the technician is using and the remote computer must have some type of network connectivity with each other.
> The computer used to access the remote computer must run Windows 7 Professional or higher, Windows 8/10/11 Pro or higher, or Windows Server or must have some type of terminal services running.
> Any firewalls between the two computers must allow port 3389 to be open.
> The remote PC must have the Remote Desktop Connection application installed and enabled. Remote Desktop Connection is disabled by default in Windows. To enable/configure it, open *File Explorer* and right-click *This PC* > *Properties* > *Remote Desktop* > toggle *Enable Remote Desktop* to *On* (see Figure 16.65).
> You need to know the computer name or IP address of the remote PC. For example, the local network name of the remote PC in Figure 16.65 is *Office*.
> You need to have a user account with a password on the remote PC, and that account must be permitted to use Remote Desktop Connection. By default, accounts with administrator rights are permitted to use Remote Desktop Connection. To admit additional users, use the *Select users that can remotely access this PC* link in Windows 10 or the *Remote Desktop users* option in Windows 11.

To initiate a remote connection, search for `Remote Desktop Connection`, enter the hostname or IP address of the remote computer, and then click *Connect* (see Figure 16.66). If a connection is available, you are prompted for the username and password of a valid user.



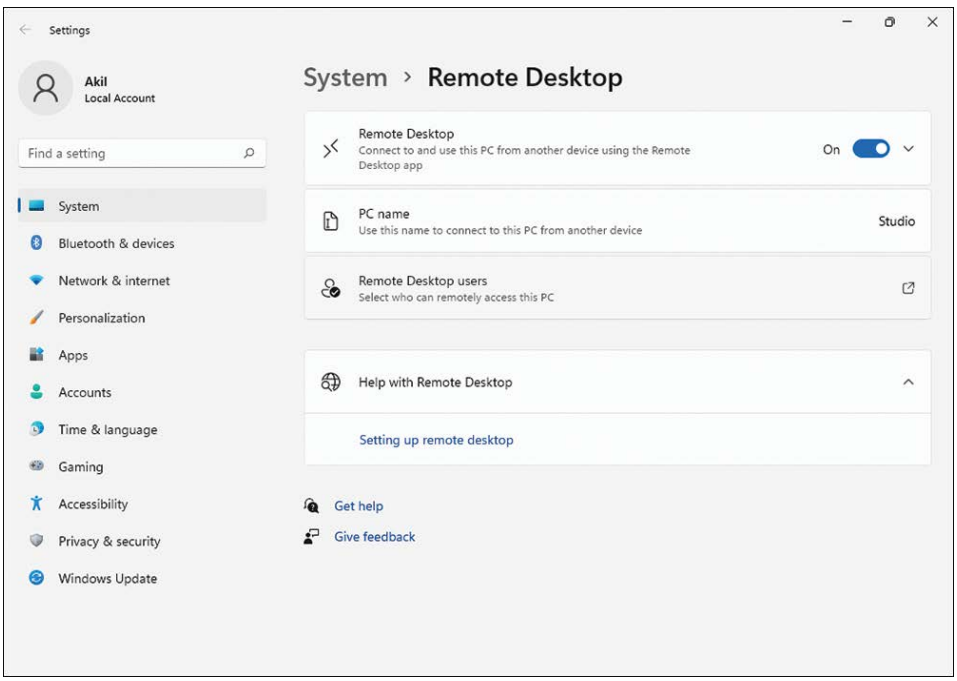


FIGURE 16.65 Windows Remote Desktop configuration for Windows 10 (top) and Windows 11 (bottom)

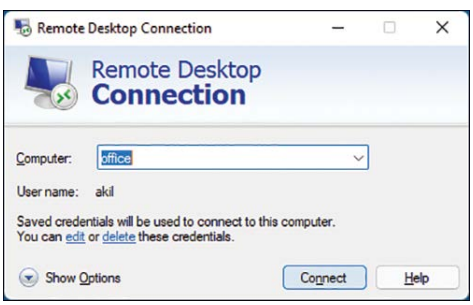


FIGURE 16.66 Windows Remote Desktop Connection login

When you are on a computer that is remotely accessing another computer via Remote Desktop Connection, there is a bar across the top of the screen that contains the remote computer's name. This is how you know that you are on another computer. The user on the remote computer is logged off and cannot see what the remote technician is doing.

With Remote Assistance, one computer user (known as the expert) views another computer user's (the novice's) desktop using a secure connection. The novice controls the computer, and the expert can only see what the novice is doing and cannot control the novice's computer.

Remote Assistance sessions can be established over the Internet without a VPN connection. On computers that use network address translation (NAT), you may have to go into the Windows Defender Firewall application and, in the left panel, select *Allow an app or feature through the Windows Defender Firewall*. Click the *Change settings* button and enable *Remote Assistance*. You must also set up a password for the guest user and manually send the password to the person invited to take over the computer.

To initiate a Remote Assistance session, follow these steps:

Step 1. Run the `msra` command or search for *Remote Assistance*.

Step 2. Choose an invitation method:

> **Save this invitation as a file:** This method creates an invitation file that the novice can send through email.

> **Use email to send an invitation:** This method starts the default email program on the novice's computer and attaches the invitation to an email message.

> **Use Easy Connect:** This option is available if Easy Connect is installed and enabled on the novice's computer. Easy Connect must also be available on the Expert's computer.

Figure 16.67 shows the available options.

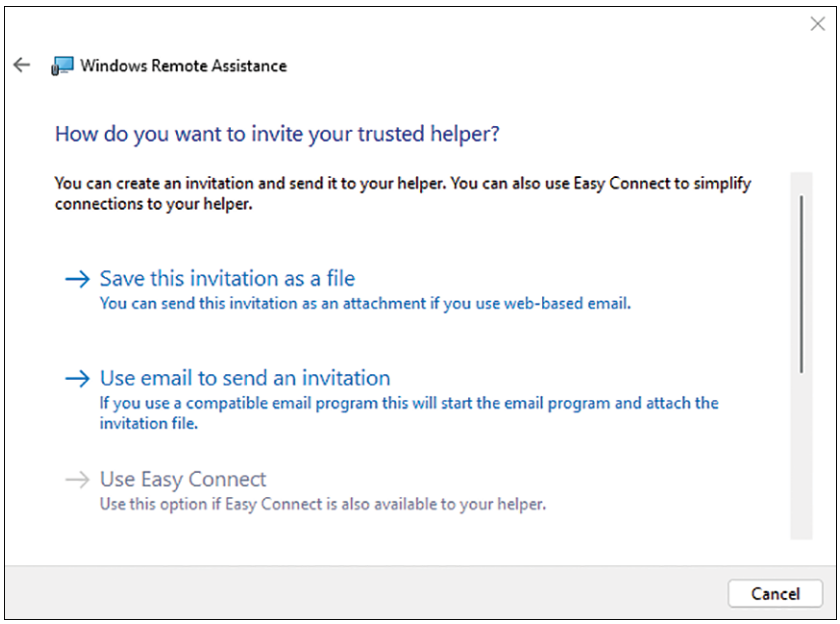


FIGURE 16.67 Windows Remote Assistance

Preventive Maintenance for Your Operating System

Your operating system is a key component of a working computer. Properly applied preventive maintenance can help avoid issues and reduce downtime. No application or hardware can work

without an operating system. It is important that you keep your operating system healthy. The following suggestions can help:

- Be sure an antivirus software program with current virus definitions is installed.
- Have a backup of your operating system. Many external hard drives include backup software.
- Make frequent data backups.
- Ensure that the System Restore utility is enabled.
- Update the operating system with service packs and **patches**.
- Use the Task Scheduler tool to automate some of the preventive maintenance tasks. You can use the `at` command to create a script file or have an application run at a specific time. Enter `at /?` at a command prompt to see the options.

Cloud-Based Productivity Tools

Productivity software helps people create things like documents for a school research project, spreadsheets for a bank account, or presentations for a new product launch. It also helps people communicate via email, video conferencing, and instant messaging.

Initially, productivity software like Microsoft Word, Apple Pages, and Mozilla Thunderbird (an email client) was client based or native, meaning it had to be installed on each workstation. The software could be preinstalled by the manufacturer, or it could be installed by the end user. The user's files could be stored on the local client or on a central server, but only one user at a time could work on a particular file. Early communication tools like Microsoft NetMeeting and Skype also required client-based applications.

With cloud-based productivity tools, multiple users can use web browsers or their client-based software to simultaneously access files that are stored on internet servers. In addition, the files can be synchronized across multiple servers, desktop devices, and mobile devices. Like their client-based counterparts, cloud-based productivity tools are useful for email, storage, and collaboration.

Email Systems

Individuals, organizations, and businesses can use cloud systems to send and receive electronic mail. The email is stored on internet servers. Users send and receive email via a web browser or a mail client application. Many devices (both desktop and mobile) have mail clients as part of their native applications. For example, Gmail is often the mail app on Android devices, and Apple Mail is the app on iOS and macOS devices. Users may also install their own mail clients, such as Microsoft Outlook or Mozilla Thunderbird.

Personal email addresses have common domain names, such as outlook.com or gmail.com. Gmail, iCloud.com, Outlook.com, and Yahoo.com are the most popular personal cloud email services. Table 16.20 describes the first steps to create an account in each service via a web browser. After completing these steps, the user will be asked for personal information such as their first and last names. They will also need to create a password for the account. In addition, they will enter a phone number (or another email address) to verify their account or to help recover a forgotten password.

TABLE 16.20 First steps to create a cloud mail account

Cloud mail service	Web client URL	To create an account
Gmail	https://mail.google.com	Select *Create account*.
iCloud Mail	https://icloud.com/mail	Select *Sign In* > *Create Apple Account*
Outlook.com	https://outlook.com	Select *Create free account*
Yahoo.com	https://yahoo.com	Select *Mail* > *Create an account*

Businesses use enterprise cloud mail systems so they can have distinctive email addresses (for example, christopher.lee@fscj.edu, cheryl.schmidt@fscj.edu). Examples of common enterprise mail server platforms include Microsoft Exchange Server, Google Workspace, and MDaemon. In large corporations, user accounts are created via automated processes after a person is configured in the company's employee database system. In smaller organizations, a system administrator manually creates each account. After the user account is created, the new email address, password, and (optionally) a URL to access the mail are given to the employee.

A web browser can be used to access both personal and enterprise cloud mail systems. In most cases, the user visits the URL for the service, selects the sign-in option, and enters their username and password. When the user accesses the service from a new device, they may be asked to confirm their identity via their phone number or an alternate email address.

Configuration of native email applications (installed on the device) varies by application and email service. For example, to use a personal Gmail account in the Microsoft Outlook app, the user enters their email address (such as chris.example.lee@gmail.com), and then Outlook automatically launches a web browser for user authentication. When the user logs in, they give permission for Outlook to access their Google email account and other required Google services associated with that email address. Outlook will also open a web browser to request the password for an enterprise account like christopher.lee@fscj.edu.

Some email servers are not configured for this streamlined authentication behavior. In these cases, the use must select *Advanced Setup* and must also get the following information from their email administrator:

- The email server's mail protocol (IMAP or POP)
- The fully qualified domain names (or IP addresses) of the outgoing and incoming email servers
- The TCP port numbers of the incoming and outgoing mail servers
- The secure connection type of the incoming and outgoing mail servers
- The username and password for the SMTP configuration

Other email clients, such as Mozilla Thunderbird and Apple Mail, have functionality and requirements like those of Microsoft Outlook.

Cloud Storage

Cloud storage is a method of saving files and data on internet servers instead of (or in addition to) using a local user device or a local server. Cloud storage offers several benefits:

- **Scalability:** The user can easily adjust storage requirements without configuring software and without installing or uninstalling hardware such as hard drives or RAM.
- **Cost-effectiveness:** Due to the vendor's economies of scale, the user's price per terabyte is significantly lower compared to the cost of local storage.
- **Universal access:** The data is available via the internet from virtually anywhere in the world.

In addition, files and data stored in the cloud are usually copied to multiple servers in different geographic locations. If an outage or corruption occurs in one location, the information can be recovered from other locations.

To use a cloud storage service, a user needs an account with a cloud storage provider. Table 16.21 lists some of the most common providers. Each service requires an email address, and most services offer several levels of service. The free tier usually has the least amount of storage space, and a user can pay for higher levels with more storage space as needed.

TABLE 16.21 Common cloud storage services

Service	URL
Dropbox	https://dropbox.com
iCloud Drive	https://icloud.com/iclouddrive
iDrive	https://idrive.com
Google Drive	https://drive.google.com
OneDrive	https://www.microsoft.com/en-us/microsoft-365/onedrive/online-cloud-storage

Cloud storage accounts can be accessed via a web browser, the provider's app, or the file manager on a device (such as Windows File Explorer or macOS Finder). In the case of a web browser, a user simply logs in to the provider's website to upload, download, delete, rename, or move files. Alternatively, the user can download the provider's dedicated app from the provider's website and install it on their desktop or mobile device. The user can also get the app from a distribution service such as Microsoft Store, Google Play, or Apple App Store.

A user's cloud storage can also be an extension of their device's file manager. For example, the iCloud Drive item in the Locations section of the macOS Finder gives a macOS user direct access to their cloud storage. Access via a file manager sometimes requires the installation of additional software. After a user downloads and installs the Dropbox app on their Windows computer, for example, a Dropbox item appears in the Navigation Pane on the left side of File Explorer. Similarly, a OneDrive item appears in the Locations section of macOS Finder after the app is installed on a Mac.

When cloud-based files are updated via a file manager, the operating system creates a local copy of the file and periodically synchronizes the file with the online version. When the device disconnects from the internet, the user can continue to work on the local copy, or the user may make updates to the online version from another device. Thus, the two files become out of sync with each other. When the device's internet connection is reestablished, the user is given the opportunity to keep one or both files. If the user keeps both, one of the files is given a different name.

Cloud storage applications can also automatically synchronize the entire contents of specific folders or data from specific applications to online storage. To select folders in Windows 11, go to *Settings* > *Account* > *Sync & Backup* > *Manage backup*. To select folders and data in macOS, go to *System Settings* > *iCloud* > *See All* > select folders and data to synchronize.

Collaboration Tools

Groups of people often use collaboration tools (such as tools for instant messaging and video conferencing) when they want to exchange information or thoughts very quickly. Tools like presentation, spreadsheet, and word processing software allow users to document and distribute their work and ideas. Cloud-based collaboration tools allow users to perform these functions over the internet on practically any device.

Table 16.22 lists some common suites of collaboration tools. All of these tools can run in a web browser, so they are independent of the device's operating system. Each online tool saves files in its vendor's online storage system. After a user creates a file in Apple iCloud, Google Workspace, or Microsoft Office 365, they can send a link to other users to access the file via a web browser. The file's owner can decide which users can view the file only and which users can also edit the file. Users can also access and update the file simultaneously. Although the tools can open similar files from other suites (for example, Excel can open a Numbers file), the tools are not 100% compatible. Files created in Google Workspace can be converted to their Microsoft counterparts.

TABLE 16.22 Common Suites of Collaboration Tools

Product suite	Online storage	Instant messaging	Presentation	Spreadsheet	Video conferencing	Word processing
Apple iCloud	iCloud Drive	Messages	Keynote	Numbers	FaceTime	Pages
Google Workspace, Google Workspace for Business	Google Drive	Chat	Slides	Sheets	Meet	Docs
Microsoft 365	OneDrive		PowerPoint	Excel	Teams	Word
Webex					Webex	
Zoom					Zoom	

There are native versions of each of these suites except for Google Workspace. They can run on Windows, macOS, Android, Linux, and iOS devices. The native versions of Apple iCloud and Microsoft 365 can also access cloud-based files, so users can have hybrid interactions with each other. For example, a user on a Windows desktop computer with the native version of PowerPoint and a macOS user running the web version of Slides can simultaneously edit the same online presentation. Likewise, an Android user can be on a Webex call with an iOS user.

Identity Synchronization

Identity synchronization refers to the process of ensuring that user accounts are consistent across different systems so users can access their resources with a single set of credentials. With cloud-only identity management, user accounts for cloud-based productivity tools are managed via the service provider's online tools. In other words, there is no on-premises user directory for managing user accounts. A personal iCloud account uses cloud-only identity management by default since the user depends on Apple's cloud resources for managing their user account.

Businesses can also use cloud-only identity management when all their accounts are cloud based. For example, a user's Microsoft Outlook email address and password give them access to OneDrive, PowerPoint, Excel, Teams, and Word. In this case, the accounts are stored online in Azure Active Directory (Azure AD). When the user or their IT department updates their password or other account information, the changes are immediately replicated throughout Microsoft's online infrastructure, so the user can use the new credentials wherever they have internet access. Businesses can use web browsers or native tools like the Microsoft 365 Admin Center or PowerShell to manage their cloud-only accounts. Google Workspace for Business administrators can manage cloud-only accounts via Google's Admin SDK for Directory API.

Businesses (especially large businesses) can also use hybrid identity management, wherein the company maintains an on-premises user account database such as Active Directory Domain Services (ADDS) and a cloud-based account database such as Azure AD. The ADDS database is authoritative (meaning accounts are created, updated, and deleted in ADDS). A server running Azure AD Connect synchronizes the ADDS data to Azure AD. ADDS authenticates on-premises users, and Azure AD authenticates remote users. Google Workspace for Business administrators can use Google's Cloud Directory Sync or their Admin SDK for Directory API to synchronize data in the on-premises database to Google's servers.

Licensing Assignment

Cloud-based tools require licenses just as native applications do. Cloud licensing assignment is the process of granting access to cloud tools within a company or organization. Companies purchase licenses based on the number of users for each product and the features required in the products. For example, a company's Webex licensing affects the number of simultaneous attendees, the availability of features like Webex AI Assistant, polling, and closed captioning.

Microsoft 365 administrators can use the Microsoft 365 Admin Center to manage the distribution and revocation of licenses for users or user groups. Administrators can see the number of licenses available for a product, the number of licenses assigned, and the number of licenses available for assignment.

Administrators use the Google Admin console to manage Google licenses. Some Google licenses, like Android, are site based, meaning every user in the organization gets a license automatically. Other services, like Google Workspace, are user based, which means a user needs to be assigned a license in order to use the service.

SOFT SKILLS: AVOIDING BURNOUT

Burnout—commonly caused by too much work and stress—is a mental state that can affect emotional and physical capabilities. Burnout affects a technician's performance as they tire of the fast pace of technology. One attraction of technology for many students is that technology is always changing; however, it is the speed of change that also provides a challenge—even to seasoned veterans. As a person matures, it seems to take more effort to stay current in the skills required for business. After being in the same job for multiple years, a technician may show signs of burnout. Technicians should monitor their own attitude and mental state constantly and watch for warning signs associated with burnout:

- Overreaction to common situations
- Constant tiredness
- Reduced productivity
- Poor attitude
- Lack of patience with customers or peers
- Feeling of a loss of control
- Use of food, drink, or drugs as coping mechanisms

It is possible to deal with or prevent burnout if you recognize the symptoms. Working too much, having too many responsibilities, and expecting too much of yourself can lead to burnout. The following list can help you recognize and cope with burnout:

- Take vacations during which you do not stay in contact with work.
- Set reachable goals, even on a daily basis.
- Take a couple breaks during the day to do something nontechnical.
- Learn something new that is not related to technology.
- Follow good eating, sleeping, and exercising routines.
- Subscribe to a positive saying or joke-of-the-day email.
- Participate in a fun or relaxing hobby or activity.

Chapter Summary

- Windows operating systems come in different editions that have various features and tools and can be 32-bit or 64-bit. The 32-bit versions are limited to a maximum of 4 GB of RAM; 32-bit operating systems or applications are sometimes referred to as x86 instead of 32-bit.
- Before installing Windows, you should complete the preinstallation steps to ensure a smooth, error-free installation.
- The installation of Windows includes three phases: determining whether to upgrade or perform a clean installation, choosing a partition system, and completing the installation.
- Corporate computer installations are more complex than other types of installations. Automated tools and disk imaging software can help with corporate computer installations.
- Many installation problems are addressed in the chapter, along with possible causes and solutions.
- Updates to Windows may be configured manually, but Windows 10/11 does automatic updates by default.

- The registry should be backed up when a computer is fully functional and immediately before any software or hardware changes are made.
- The System Configuration Utility (`msconfig`) is used to troubleshoot startup issues, set boot conditions, and access services and quick links to Windows tools.
- Tasks that a technician commonly performs to configure Windows include adding devices, removing hardware components, adding a printer, and installing or removing software.
- The Computer Management console can access three categories: System Tools (Task Scheduler, Event Viewer, Shared Folders, Local Users and Groups, Performance, and Device Manager), Storage (Disk Management), and Services and Applications.
- Managing accounts for those who use computers or computer resources from remote network computers is an important function of a technician or administrator.
- The Storage Computer Management category includes just the Disk Management tool, which is used to manage hard drives, including volumes or partitions.
- A service is an application that can be started using the Services option or configured to start when the computer boots.
- The Data Sources administrative tool can be used to select which database application is associated with a particular type of file.
- The Print Management console is used to manage printers.
- There are various methods to speed up and troubleshoot the boot process. The Windows Recovery Environment (WinRE) is accessed by booting from Windows installation media or from within Windows. WinRE includes many diagnostic and other helpful tools.
- Task Scheduler can be used to automate preventive maintenance to occur on a regular basis. Preventive maintenance can reduce downtime and includes keeping the operating system and applications patched, keeping the antivirus definitions current, keeping the hard drive defragmented, and ensuring ample space on the hard drive.
- Technicians should understand how to determine how a computer is performing by using Task Manager and comparing current performance to a baseline that was taken at a time when the computer was running optimally. Other tools, such as Performance Monitor or Resource Monitor, are also very helpful.
- Technicians may be required to access computers remotely, and this can be done using the Remote Desktop Connection or Remote Assistance products.
- Technicians can do positive things to avoid burnout, including getting good rest, avoiding drugs and alcohol, doing nontechnical things, and having good time-management skills.

A+ CERTIFICATION EXAM TIPS

- ✓ Know the minimum hardware requirements for installing 32- and 64-bit Windows 10. Know that Windows 11 can only be installed on 64-bit systems.
- ✓ Use all Windows tools before taking the certification exams. Ensure that you pay attention to the purpose of each tool and consider why (or in what situation) you would use each Windows tool.
- ✓ Review all symptoms and resolutions for a system that is running slowly or is boots slowly.
- ✓ Know the various boot methods.
- ✓ Review the various types of installations, such as an unattended installation, in-place upgrade, clean install, repair installation, remote network install, image deployment, recovery partition, and reset/restore. Review Table 16.1.
- ✓ Know the various types of partitions and what they are best used for.
- ✓ Be familiar with different user/group accounts and Credential Manager.

- ✓ Be familiar with common symptoms and troubleshooting of software problems. Common symptoms include slow performance, failure to boot, and application crashes.
- ✓ Be familiar with the following features: Computer Management, Print Management, Device Manager (which can be used to disable a device), Local Users and Groups, Performance Monitor, Services, System Configuration, Task Scheduler, Component Services, Data Sources, Windows Memory Diagnostic Tool, Task Manager, Disk Management (including knowing how to install a drive, initialize a disk, create a volume, convert a basic disk to a dynamic disk, partition a disk, select a file system, and format a partition), Upgrade Advisor, System Restore, and Windows Update.
- ✓ Interact with and use for troubleshooting the following Windows Control Panel utilities: Display/Display Settings, User Accounts, System, Power Options, Programs and Features, Print Management, Sound, and Troubleshooting.

Key Terms

account recovery options, ACL, activation clock, adding an array (Disk Management), administrator, Advanced Boot Options, application crash, application log, apply update, assigning/changing drive letter, Automatic Updates, baseline, basic disk, black screen, blue screen, boot partition, boot volume, CDFS, clean install, compatibility mode, Component Services, Computer Management, `convert`, Credential Manager, Data Sources, defragment the hard drive, device driver, Device Manager, Devices and Printers, digital signature, disable a service, disable Windows applications, Disk Cleanup, Disk Management, domain, drive partition, drive status, dynamic disk, Error Checking, Event Viewer, exFAT, ext4, extended partition, extending a partition (Disk Management), external hard drive (boot option), factory recovery partition, failure to boot, FAT32, File History, full format, GPT, graphical interface fails to load, hotfix, identity synchronization, image deployment, in-place upgrade, initializing (Disk Management), internal fixed disk (boot option), internal hard drive partition (boot option), kill task, KMS, load alternate third-party driver, Local Users and Groups, logical partition, MBR, Microsoft Management Console, `mmc`, mounting (Disk Management), `msconfig`, `mstsc`, multiboot, network boot, no OS found, Notepad, NTFS, NTLDR is Missing, optical disc (boot option), Optimize Drives, patch, performance (virtual memory), Performance Monitor, primary partition, Print Management, printing issue, Program Compatibility Troubleshooter, PXE, quick format, ReadyBoost, reboot, rebuild a Windows profile, recovery partition, refresh rate, ReFS, regedit, registry, `regsvr32.exe`, reimage, Reliability Monitor, Remote Assistance, Remote Desktop Connection, remote network installation, repair an application, repair installation, Reset This PC, resolution, Resource Monitor, restart service, restore (installation method), restore point, rights, roll back the device driver, roll back Windows update, Safe Boot, Safe Mode, service, service fails to start, service pack, Services, `services.msc`, `sfc`, Shadow Copy, share, Shared Folders, shrinking a partition (Disk Management), slow boot, slow performance, slow profile load, splitting a partition (Disk Management), Standard user, Storage Spaces, swap partition, Sync Center, Sysprep, System Configuration utility, System Control Panel, System File Checker, system file, system log, System Protection, system requirements (application), System Restore, system volume, Task Manager, Task Scheduler, UAC, unattended installation, update network settings, update the boot order, user account management, USMT, Windows Recovery Environment, Windows Update, WinRE, workgroup, WRP, zero-touch deployment

Review Questions

1. What is the maximum amount of RAM that can be recognized by any version of 32-bit Windows?

_____

2. A customer has an older 16-bit game as well as some 32- and 64-bit games. The customer is considering upgrading to 64-bit Windows 10. Will there be any issues with this? If so, what are they, and how might they be resolved?

_____

_____

3. List three steps to be taken before installing Windows.

_____

_____

_____

_____

_____

_____

4. Which tool can limit and control the number of applications used to boot a computer?

   [`taskmgr` | `regedit` | `msconfig` | `diskpart`]

5. Which Windows setting would be used to enable Windows PowerShell, Hyper-V, or Microsoft's Print to PDF option?

   [Turn Windows Features On or Off | Task Manager | System Configuration | Performance Monitor]

6. Which performance tool would a technician use first to see if a computer has enough hardware resources when a particular application executes?

   [Performance Monitor | Task Manager | Reliability Monitor | Device Manager]

7. How could you have both Windows 7 and Windows 10 operating systems installed on one computer?

_____

8. [T | F] Existing restore points are deleted if Windows is reinstalled.
9. [T | F] Device drivers are specific to a particular Windows operating system version.
10. Which System Configuration tab is used to configure a computer to boot in diagnostic startup mode?

    [Boot | Services | Startup | General | Tools]

11. What user group is allowed to perform driver rollback. (Choose all that apply.)

    [Standard User | Guest | Administrator | Backup Operators]

12. What is the purpose of the System Restore utility?

_____

_____

13. When Windows boots, nothing appears on the screen. If the display is powered on and attached, which Windows tool would be the best one to try first?

    [System Restore | Safe Mode | Command Prompt | Reset Your PC]

14. When would a technician use Event Viewer?

_____

_____

15. Describe how Task Manager can monitor computer performance?

_____

_____

16. Which disk management option would be used to create a flexible data storage option from a USB drive and an eSATA drive that is seen as one drive letter?

    [RAID 0 | RAID 1 | RAID 5 | Storage Spaces]

17. Where does Windows store passwords and login details for a particular user?

    [Storage Spaces | Credential Manager | BIOS/UEFI | `C:\Windows\System32\Configuration`]

18. Which type of Windows installation setup is used for a corporate environment?

    [workgroup | homegroup | domain | peer-to-peer]

19. Which type of Windows boot process is used in conjunction with the PXE BIOS/UEFI option?

    [in-place upgrade | multiboot | network | recovery]

20. List three things a student can do to avoid burnout in school.

    _____

    _____

Exercises

Exercise 16.1 Using Windows Tools

Objective: To determine which Windows tool to use, based on the task

Procedure: Match each scenario to the best Windows tool to use for the given situation. Note that one tool is used twice.

Tools:

a. Event Viewer
b. System Restore
c. System Repair
d. `msconfig`
e. Device Manager
f. Folder Options
g. System Properties
h. Printer & Scanners
i. Disk Management
j. Task Scheduler
k. Services
l. Performance Monitor
m. Task Manager
n. Computer Management console
o. Windows Memory Diagnostics Tool
p. Safe Mode
q. `regsvr32`
r. Safe Boot
s. Print Management

Scenarios:

____ **1.** Configure two drives in a RAID configuration.

____ **2.** Determine when a user logged in to a computer yesterday.

____ **3.** Restart the program that allows the print spooler to function.

____ **4.** You suspect that one of the DDR4 modules has an issue.

____ **5.** The quickest way to see the default printer.

____ **6.** Disable a computer vendor app that keeps running every time the computer boots, trying to get the user to buy storage space.

____ **7.** Configure a specific number of processors the computer uses to boot.

____ **8.** Run a test of hard drive reads per second and writes per second to see if the drive is causing slowdown issues.

____ **9.** Bring the system back to before a particular Windows update is installed.

____ **10.** Instruct the system to perform disk maintenance twice a week instead of just once.

____ **11.** Have the ability to access Device Manager and the Disk Management tool from one window.

____ **12.** View system files through File Explorer.

____ **13.** Testing mode with limited drivers loaded.

____ **14.** Unregister a DLL.

____ **15.** Disable a piece of hardware.

____ **16.** Adjust virtual memory.

____ **17.** View all print servers.

____ **18.** Halt a misbehaving app.

____ **19.** Control the Safe Mode boot type the next time the computer restarts.

____ **20.** Let the OS try to figure out why Windows won't boot.

Exercise 16.2 Using Task Manager Tabs

Objective: To determine which Task Manager tab to use, based on the task

Procedure: Match each scenario to the best Task Manager tab to use in Windows 10. You might want to review figures throughout the chapter. Each tab is used only once.

Tabs:

a. Processes

b. Performance

c. App History

d. Startup

e. Users

f. Details

g. Services

Scenarios:

____ **1.** See a graph of how quickly an SSD is responding to requests for information.

____ **2.** Determine what applications a person has used today and how much memory each of them has used.

____ **3.** Document how much bandwidth a particular application used on a metered network.

____ **4.** Stop and restart Wlansvc.

____ **5.** Learn which apps are considered to be actively used on the computer right now.

____ **6.** Look up the specific process ID (PID) for the `firefox.exe` application.

____ **7.** Research which applications launched automatically when the computer booted.

Exercise 16.3 Using System Configuration Tabs

Objective: To determine which System Configuration tab to use, based on the task

Procedure: Match each scenario to the best System Configuration tab to use for the given situation. You might want to review figures throughout the chapter. Each tab is used only once.

Tabs:

a. General

b. Boot

c. Services

d. Startup

e. Tools

Scenarios:

____ **1.** Determine what applications began as part of the Windows boot process.

____ **2.** Allow a technician to choose either a normal, diagnostic, or selective startup.

____ **3.** Quickly access Event Viewer.

____ **4.** Create a log file of the boot process for a computer that doesn't boot properly.

____ **5.** Select only three Windows apps that enable specific Windows features that start as part of the boot process.

Activities

Flip the CLASSROOM

Internet Discovery

Objective: To access the internet to obtain specific information regarding a computer or its associated parts

Parts: Access to the internet

Procedure: Use the internet to answer the following questions.

1. Find a website that offers Windows freeware tools. Write the name of a freeware tool and the URL where this information was found.

_____

_____

2. What is the latest update available from Microsoft for Windows 11? Write the answer and the URL where you found the answer.

_____

3. Find a website that details what to do if a Windows 11 upgrade results in a black screen. Describe what the website recommends and provide the URL where you found the recommendation.

_____

_____

_____

_____

4. Microsoft has a planned lifecycle for each of its operating systems. Find a website that provides the planned mainstream support end date for Windows 11 Enterprise (version 24H2). Write the mainstream support end date as well as the URL.

_____

_____

5. You get the error code 0x80070005 on a Windows 11 computer. Find a website that describes this error. Write at least one thing that could cause this error, one solution, and URL where the answer can be found.

_____

_____

_____

_____

6. Find a technical certification related to a Microsoft operating system. List the certification and the average salary associated with the certification. List all URLs used to find this information.

_____

_____

Soft Skills

Objective: To enhance and fine-tune a future technician's ability to listen, communicate in both written and oral forms, and professionally support people who use computers

Activities:

1. In groups of two or three students, one student inserts a problem related to Windows on a computer. The other student or students use the Remote Desktop Connection utility to find the problem and then repair it. Document each problem, along with the solution provided. Change roles so that each student practices both the repair and the documentation.

_____

2. Divide into five groups. Five questions about operating systems follow:
   - What should you do before installing an operating system?
   - What are alternatives to Windows 10 or 11 as an operating system, and what are pros and cons of these alternatives?
   - What is the difference between an active partition, a system partition, and a boot partition in regard to Windows?
   - What operating systems can be upgraded to Windows 10 or 11? What is the difference between a clean install and an upgrade, and what determines which one you do?
   - What differences can be seen for a Windows hard drive that has a FAT32 partition and one that has an NTFS partition?

   Each group is assigned one of these five questions or another question related to Windows. Each group is allowed 20 minutes (and some whiteboard space or poster-sized paper) to write their ideas. All group members help to present their findings to the class.

_____

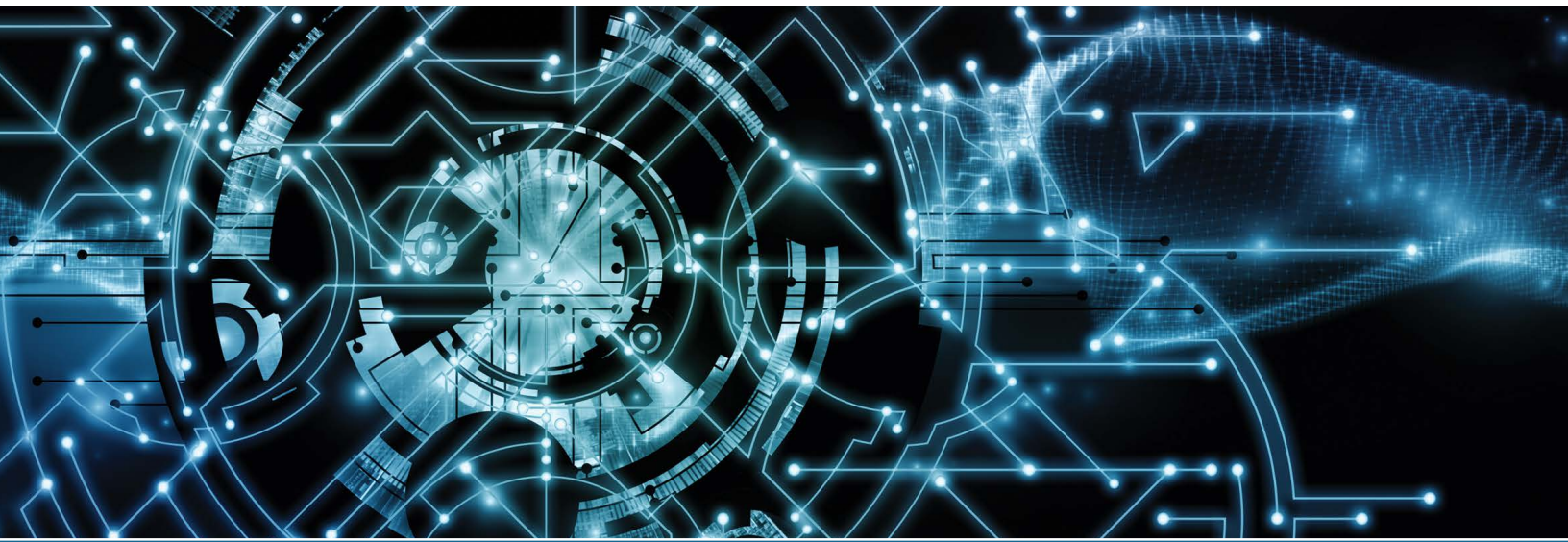
3. Find a magazine article related to a Windows solution or feature. Share your findings with the class.

_____

4. Using any research method and resource, determine the pros and cons of upgrading to Windows 11 from Windows 10. Make a list of things to check before upgrading.

_____

17 macOS and Linux Operating Systems



In this chapter you will learn:

- What operating systems are available besides Windows
- How to navigate the user interfaces of macOS and Ubuntu Linux
- How to manipulate files and folders in the graphical and command-line interfaces
- How to create system backups
- How to find Unix/Linux software
- How to work from a Linux-based command line
- Reasons to be humble in the IT field

CompTIA Exam Objectives:

- ✓ 1202-1.1 Explain common operating system (OS) types and their purposes.
- ✓ 1202-1.2 Given a scenario, perform OS installations and upgrades in a diverse environment.
- ✓ 1202-1.8 Explain common features and tools of the macOS/desktop operating system.
- ✓ 1202-1.9 Identify common features and tools of the Linux client/desktop operating system.
- ✓ 1202-2.6 Given a scenario, implement procedures for basic small office/home office (SOHO) malware removal.
- ✓ 1202-3.2 Given a scenario, troubleshoot common mobile OS and application issues.
- ✓ 1202-3.4 Given a scenario, troubleshoot common personal computer (PC) security issues.

Introduction to macOS

macOS is a Unix-based operating system that was developed by Apple, Inc., for its Macintosh (or Mac) line of computers. This Apple operating system is the second most commonly used desktop operating system (after Windows), and it is the most commonly used type of Unix/Linux-based desktop operating system.

Like most other Unix/Linux operating systems, macOS utilizes many open source projects to make up the core and functionality of the operating system, along with a touch of Apple's own customization. **Open source** software is software that is made freely available and that is open to outside contributions. Although many parts of macOS are open source, the operating system is not. macOS is unique to Apple-released hardware (see Figure 17.1) because it comes preinstalled only on Mac systems. It is not sold or distributed to run on other hardware or as virtual machines, as Windows and most other Unix/Linux distributions are.

FIGURE 17.1 Apple computer running OS X

The predecessor to macOS was **OS X**. The desktop OS X releases were named for felines, and the macOS versions are named after California landmarks. Table 17.1 lists macOS operating system distributions by release number and name. The information in this chapter is based on macOS Sequoia version 15.3.

TABLE 17.1 macOS releases since 2016 by name and number

Release number	Name	Release date
10.12	Sierra	September 2016
10.13	High Sierra	September 2017
10.14	Mojave	September 2018
10.15	Catalina	October 2019
11	Big Sur	November 2020
12	Monterey	October 2021
13	Ventura	October 2022
14	Sonoma	September 2023
15	Sequoia	September 2024

macOS is a Portable Operating System Interface (**POSIX**)-compliant operating system, which means it meets the specifications for a standardized operating system outlined by the IEEE Computer Society and contains a Bourne shell and other standard programs and services that are found in all POSIX-compliant operating systems. A **shell** is a user interface that is used to interact with an operating system. POSIX standardization makes it easier for end users, IT professionals, and developers to use different operating systems that are POSIX compliant and have familiar tools available. Because of this standardization, many skills that you learn with macOS can be applied to other operating systems.

Navigating the User Interface

macOS is renowned for its intuitive and easy-to-learn graphical user interface (GUI). There are multiple ways to interact with this GUI, including using the standard mouse and keyboard and using the more modern trackpad multitouch gestures. The macOS GUI is called Aqua. Steve Jobs, co-founder of Apple Inc., famously said, "One of the design goals was when you saw it you wanted to lick it." He was referring to the original water-like theme of the GUI, which made heavy use of translucent and reflective design elements. Now the GUI is a flatter, toned-down interface that more resembles Apple's mobile operating system iOS than earlier versions of the operating system.

There are four basic elements to the macOS GUI: Dock, Finder, menu bar, and Desktop (see Figure 17.2). The one that sticks out first on the desktop is known simply as the Dock. The **Dock** is the shortcut organizational bar used for launching, switching, and managing applications. You can easily customize the Dock by dragging and dropping applications and folder shortcuts to it. By default, the Dock is at the bottom of the screen, but its position can be changed so it is located on the side of the screen.

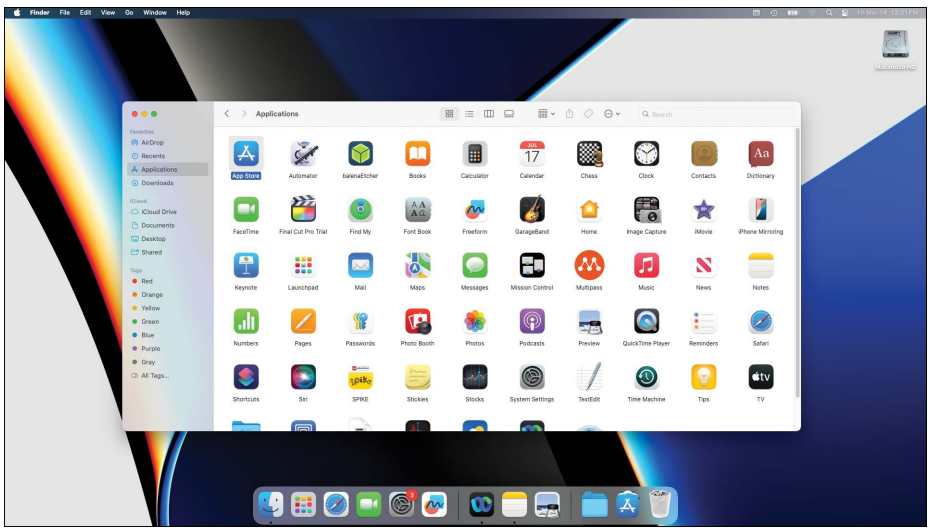


FIGURE 17.2 macOS desktop

The **Finder** is the file manager included in macOS. It is used for navigating and managing files or folders in the file system. The Finder is similar to File Explorer in Microsoft Windows. You can open the Finder by clicking the iconic Finder icon, known for its smiling face, which is always located on the Dock.

The **menu bar** is anchored to the top of the screen. It is a dynamically changing bar that presents contextual drop-down menu options on the left side, depending on what window is active. On the right side, the menu bar provides shortcuts for actions such as connecting to a Wi-Fi network or changing the volume. The menu bar is also informative, displaying information such as battery life on MacBooks, the date, and the time of day.

The Notification Center opens when the date or time is clicked on the menu bar. It displays system and app notifications. The user can also configure widgets in the Notification Center. Widgets are small applications that provide summarized information from an app or limited interaction with an app but without opening the full program. Widgets can be used for task reminders, calendar events, email alerts, weather updates, news headlines, stock market activity, and more.

Another important element of the macOS GUI is the desktop, which can hold anything the end user wants to save to it for quick access, such as documents, pictures, or mounted drives.

Notice the three colored dots on the upper-left corner of the Finder window in Figure 17.2. The red dot on the far left is used to close the window. The yellow dot, in the middle, is used to minimize the open window down to the Dock. The green dot (the rightmost one) is used to expand the window to full-screen mode. These three dots are universal across all windows in macOS. When a window is in full-screen mode, the menu bar disappears. It reappears when you move the mouse to the top of the screen. The green dot can then be used to reduce the window to its previous size.

TECH TIP

What to do if the Dock is missing

If the Dock is not present, try hovering the pointer toward the bottom or sides of the screen. Many macOS users hide the Dock to gain more screen space, so that it pops up only when the pointer is nearby.

On top of the core GUI elements are a few built-in utilities that make using the GUI easier. macOS supports multiple desktops, much as Microsoft Windows 11 does with Task View. **Mission Control** is a feature that gives an overview for managing all application windows and virtual desktops. It can be invoked by pressing the F3 key (or the F9 on older Mac keyboards), by double-clicking the Mission Control icon (located in the Applications folder), or by swiping up on a trackpad with three or four fingers at once (depending on the trackpad settings). Mission Control displays all the open windows (see Figure 17.3), their respective windows grouped together, and any extra virtual desktops. From this view, you can create, delete, or rearrange virtual desktops; switch which application windows reside on each virtual desktop; and easily explore all the open application windows.

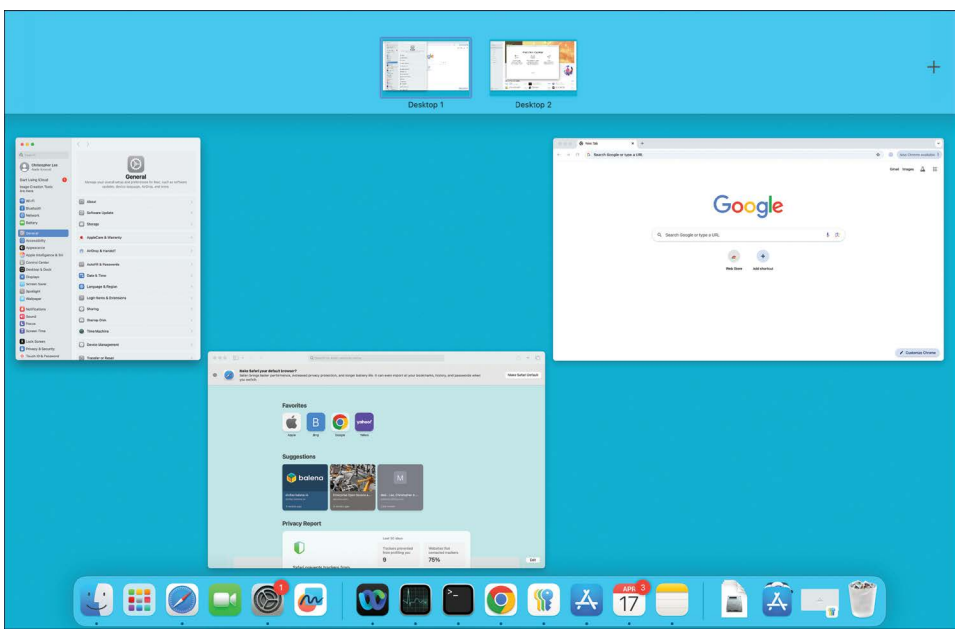


FIGURE 17.3 macOS Mission Control

Although Mission Control is great for managing applications, it cannot launch them. **Launchpad** is an application launcher shortcut. It can be invoked by clicking the Launchpad icon (available in the Applications folder or on the Dock) or by using a thumb + three-finger pinch gesture on a trackpad. This view is a grid-like display of all installed applications that you can click to launch (see Figure 17.4). You can search Launchpad with the search bar at the top of the interface. Applications can also be sorted into folders and multiple pages in this view for easy organization.

FIGURE 17.4 macOS Launchpad

Finder is used for navigating the file system, but it can be cumbersome, and it can take a long time to find something, especially if you are not sure where the item is located. You can use Spotlight to search the system. **Spotlight** is a universal search tool that can search every file and directory, as well as contacts, email, music, and even the web (see Figure 17.5). It is invoked by holding down ⌘ and pressing the Spacebar or by clicking the magnifying glass icon on the right side of the menu bar. A large search bar appears in the middle of the screen, allowing you to type in your search. The results are then presented to you underneath the search bar. You can launch applications directly from the results.

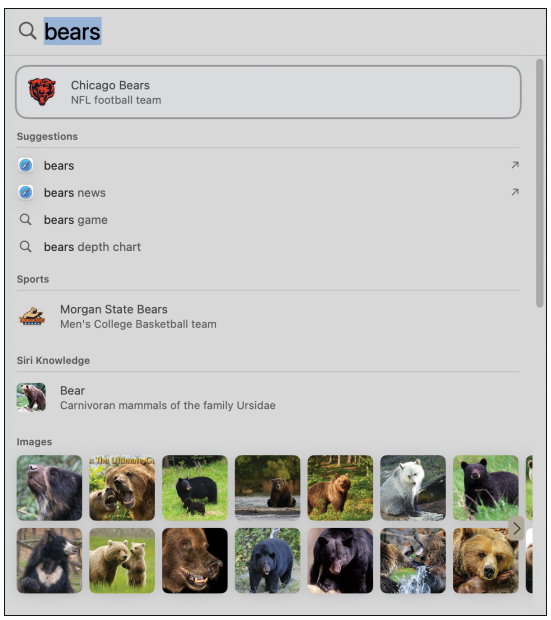


FIGURE 17.5 macOS Spotlight

You may have noticed that many of these shortcuts have their own dedicated gestures that can be triggered using a trackpad. Apple introduced the idea of finger-based **gestures** (use of fingers to make motions that provide input) in its mobile operating system, iOS. These gestures and functionality were later brought to MacBook laptops. To easily use these gestures, a user could purchase a Magic Mouse, which is a multitouch mouse sold by Apple, or a Bluetooth trackpad known as a Magic Trackpad. Table 17.2 lists the most commonly used trackpad gestures and the actions they trigger. Keep in mind that other gestures can be enabled, and many of them can be changed to have different effects, depending on the user's preference.

TABLE 17.2 Commonly used macOS gestures

Gesture	Action
Swipe left or right with two fingers	Swipe between pages
Swipe left or right with three fingers	Swipe between full-screen applications
Swipe left or right with four fingers	Swipe between desktops
Swipe up with three or four fingers	Open Mission Control
Pinch in with the thumb and three fingers	Open Launchpad
Spread apart the thumb and three fingers	Show the desktop
Pinch in or out with two fingers	Zoom in or out
Tap with two fingers at the same time	Right-click
Tap and hold down with three fingers	Take control of a window in order to drag it around the screen

Basic System Usage, Applications, Updates, and Backups

When macOS starts, you may be presented with a login screen if the user accounts have passwords enabled. You can log in with a previously created user account or, if it is enabled, you can use the guest login selection. If you log in as a guest, any changes you make or items you save will be deleted from the system when you log out. Every time you are logged in as a guest user, you are presented with a fresh desktop experience, as if it has never been used before.

macOS comes bundled with most of the software shown in the Launchpad in Figure 17.4, including applications for general use as well as system upkeep. macOS's office productivity suite, known as **iWork**, includes a word processor called Pages, a presentation application called Keynote, and a spreadsheet application called Numbers. These productivity applications are Apple's answer to the popular Microsoft Office suite. Other useful bundled applications include Mail, Safari (the default web browser), Calendar, Contacts, and Photos.

macOS also comes with **iCloud,** a cloud-based service that offers storage, application support, and syncing of contacts, photos, email, bookmarks, documents, and more between multiple OS X, macOS, iOS, and even Windows devices. You can create an iCloud account on any OS X, macOS, or iOS device. To create an account in macOS, you can use the iCloud icon in System Settings, which is located on the Dock. You need an email address to create an account. You can generate a new iCloud domain email or you can use another email address as your login. When you log in to iCloud on your machine, you can select which items you want synced among your devices. The free syncing service includes 5 GB of cloud storage, and you have the option to purchase a monthly subscription for more storage space. Using iCloud is optional, but it is worth looking into for easy syncing of devices.

iCloud offers built-in remote connectivity. If you log in to iCloud, have internet access, and enable the Screen Sharing feature in the *System Settings* > *General* > *Sharing* menu of a Mac, you can browse that Mac from another macOS device. The remote Mac appears as a shared device in Finder, and you can browse the file system. You can click the Share Screen button to start a remote desktop session.

macOS System Folders

System folders contain important files and folders that are required for an operating system to function properly. System folders and their initial contents are created during the OS installation process. The operating system and the applications constantly access and update system folders while the computer is running. Therefore, system folders should not be deleted, renamed, or moved. Except in specific cases (such as when installing an app), the user should not directly alter the contents of a system folder.

The most essential system folders in macOS are `/System`, `/Library`, `/Applications`, and `/Users`, `/Users/`*`username`*`/Library`. The `/System` folder contains the actual macOS operating system. The `/Library` folder contains resources that are used throughout macOS, such as fonts, internet plug-ins, and keyboard definitions. The `/Applications` folder contains built-in macOS apps such as Mail, Calendar, and Safari, as well as applications that the user installs.

The `/Users` folder contains a home folder for each account that logs in to the computer (such as `/Users/chrislee`). The `/Users` folder also contains the `Shared` folder, whose contents are available to anyone who uses the computer. When a user logs in to the computer, a house appears on that user's home folder. A user's home folder contains their personal folders, such as `Downloads`, `Desktops`, `Documents`, and `Pictures`. Each user also has a `Library` folder (such as `/Users/chrislee/Library`), which contains their personal settings, preferences, caches, and other application-related files.

App Store

macOS comes with a wide range of bundled software, and there is also a software marketplace, called the App Store. The **App Store** is a centralized marketplace where developers can list and sell software (see Figure 17.6). You can easily find, download, and install a wide range of software, from simple utilities to advanced 3D games. The App Store allows for easy management of purchases, which are tied to a user's Apple ID; a user can install software they have purchased on multiple systems or re-download past purchases by logging in with their account. The App Store also allows for easy application updates, enabling developers to push out updates to end users through this centralized repository. Using the App Store also provides a layer of security: Users know the applications available in the App Store have been vetted by Apple and are unlikely to include harmful or malicious code.

To uninstall an App Store app via the Launchpad, open *Launchpad* > click and hold the app's icon until it begins to jiggle > click ⊗. After the icon starts jiggling, you can also drag it to Trash on the Dock. To uninstall an app (including apps from other sources) via the Applications folder, drag the icon to Trash on the Dock or right-click the app's icon and then click *Move to Trash*.

TECH TIP

Apple ID

To use the App Store and other Apple cloud services, you need an Apple ID. This login is used for tracking software purchases through all of Apple's stores. You can create one in the App Store, through iTunes (an Apple media player, radio app, and media library), or by going to https://appleid.apple.com/account.

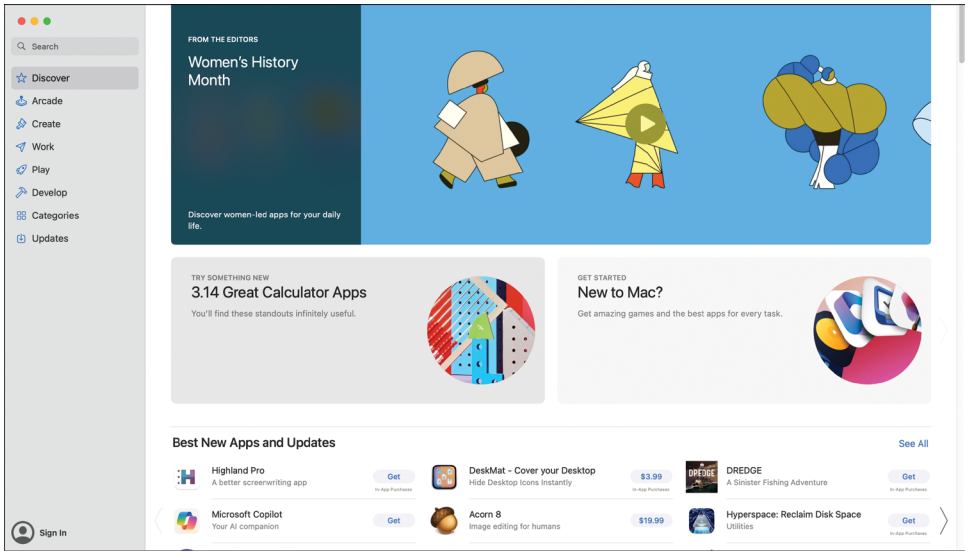


FIGURE 17.6 App Store

Installing and Uninstalling Other Applications

In addition to using the built-in applications and installing App Store applications, users can use applications from sources such as the internet. A macOS application installation file has the extension `.pkg`, `.app`, or `.dmg`. A `.pkg` or `.app` file is an application package that contains the software, folders, and other files required to install the application. To begin the application installation process, double-click the `.pkg` or `.app` file and follow the instructions.

A `.dmg` file is a disk image (similar to an `.iso` disk image file). To install an application distributed as a `.dmg` file, double-click the file to mount the disk to the computer. A new drive appears on the desktop and under *Finder* > *Locations*. The drive will open to display an application icon. Drag the application icon to the `Applications` folder to finish the installation. The application's icon will appear in the `Applications` folder when the installation is complete. To unmount the disk image, use the drive's eject button in Finder or drag the drive's icon to Trash on the Dock.

To uninstall an app via the Applications folder, drag the icon to Trash on the Dock or right-click the app's icon and then click *Move to Trash*.

Screen Sharing

If you have **screen sharing** turned on, another Mac user who is on the same network can view the display of your Apple computer and even control the computer. To view another computer's display remotely, open *Finder* > *Network*. Then double-click the Mac that you want to share and click *Share Screen*. Screen sharing is especially helpful to technicians supporting remote users.

For screen sharing using a single 4K display, the recommended bandwidth is 75 Mb/s. Also, both Mac computers must be Apple Silicon devices running macOS Sonoma 14 or later, and you might need to adjust firewall configurations.

System Updates

Apple uses the App Store to release patches and updates for macOS. It is important to check the Updates tab in the App Store from time to time to get the latest operating system and application updates. You can also have the number of updates available dynamically display on the App Store icon as a reminder that you have updates to perform.

Time Machine

It is easy to recover your previously purchased applications through the App Store, but the App Store is not a backup system. For that you need to set up Time Machine. **Time Machine** is a bundled application in macOS that enables you to do full and incremental system backups to an external hard drive. It gets its clever naming from the capability to navigate your past backups as if you were traveling through time. Notice in Figure 17.7 that the current Finder is on top. The stacked windows behind it are previous snapshots shown in time order from present to further in the past.

To use Time Machine, you need to connect an external hard drive to the system, typically through a USB or Thunderbolt connection. When an external drive is connected, you simply go to *System Settings* > *General* > *Time Machine*, select the disk you want to use, and turn it on. The *System Settings* > *Control Center* > *Time Machine* > *Show in Menu Bar* option provides a quick way to access Time Machine after it has been enabled.

Time Machine performs a full system backup after it is enabled and then continues to do a new incremental backup every hour. It retains the past 24 hours of backups, a daily backup for each day in the past month, and a weekly backup for all prior months. It deletes the oldest backups when the disk gets too full for the next backup. Following those rules, it keeps as many backups as possible. After Time Machine is set up, all the backups are done in the background, without user intervention.

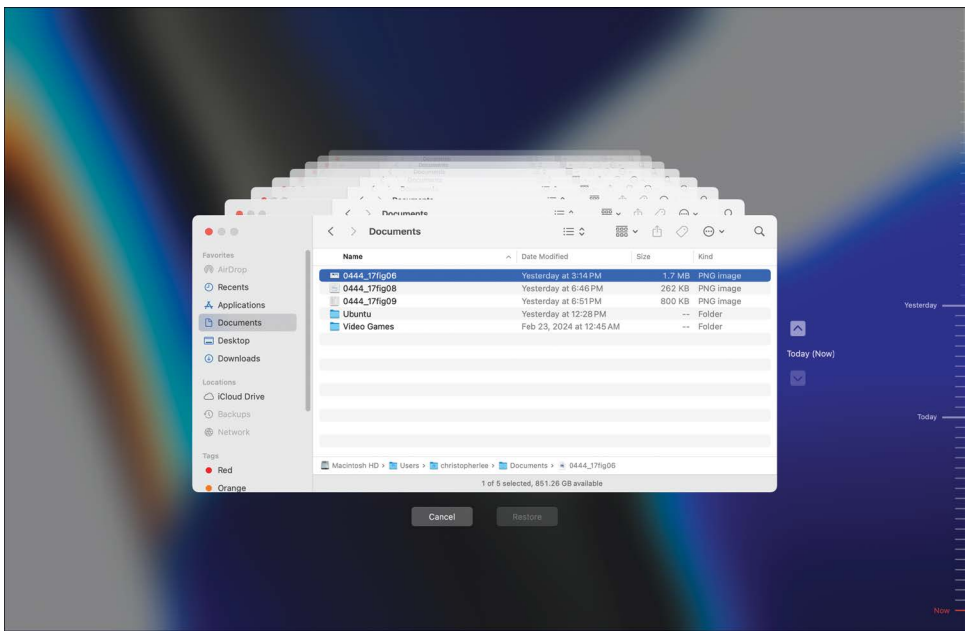


FIGURE 17.7 Time Machine

TECH TIP

Requirements for using a disk for backups

When selecting a drive to use for backups, you need to use a drive with a partition that is APFS (Case-sensitive) formatted. By default, macOS cannot write to an NTFS-partitioned drive. If you choose such a drive, the disk will be reformatted, which means all data on the disk will be erased. The number of backups possible depends on the size of the external drive. You want the drive to have at least as much disk space as your internal Mac hard drive so that you can always fit at least one full backup set on it. The larger the drive, the better. But remember: Creating a single backup is not a reliable way to back up important data. Always have multiple backup options for data that you cannot risk losing (for example, a local backup such as Time Machine as well as a remote or cloud backup).

With the Time Machine interface, you can recover deleted files or restore older versions of files, as well as applications that were deleted. You can restore an individual file or find an older version of it. Simply select the file or navigate to the location where it was saved in Finder. Then open the Time Machine application from the Finder or from the menu bar icon to bring up a timeline view of the selected file or the files that have been in the selected location. You can navigate the backups available by scrolling through the timeline presented on the right side. When you find the file or version you want to restore, select it and click the *Restore* button.

If the Time Machine external drive is not connected, local snapshots are automatically created once a day. Figure 17.7 shows tick marks at the bottom-right of the screen. Each tick mark is a backup. When you position the pointer over a tick mark, you see that tick mark light up in a particular color. For macOS Yosemite and later, a bright red tick mark indicates that the particular backup can be used to restore the system (from a local snapshot or backup drive). A less bright tick mark indicates a backup that can only be restored from the backup drive.

If a system failure occurs, you can even restore the entire backup from your Time Machine external drive onto a different Mac. You do this by booting the Mac you want to restore to into recovery mode. To enter recovery mode, make sure the computer is completely shut down. Next, press and hold the power button until *Loading startup options* appears. Click *Options* > *Continue.* Select an administrator account and enter the password. Next, click *Continue*, and the Recovery menu appears.

When recovery mode boots, you see the option *Restore from a Time Machine Backup*. Make sure the external Time Machine drive is connected, select this option, and follow the prompts to restore the backup. If you're using a networked disk for Time Machine, you have the option to connect to the remote disk for the restore process.

Force Quit

macOS is a stable operating system that rarely crashes or requires you to use backups to recover anything, but applications can still run into issues in day-to-day use. When a program stops responding or working properly, you may need to use the **Force Quit** feature. To access the Force Quit menu, either click the Apple icon on the top left of the screen and then select *Force Quit* or hold down ⌘+Option+Esc at the same time. The window that appears allows you to choose which application(s) to quit (see Figure 17.8).

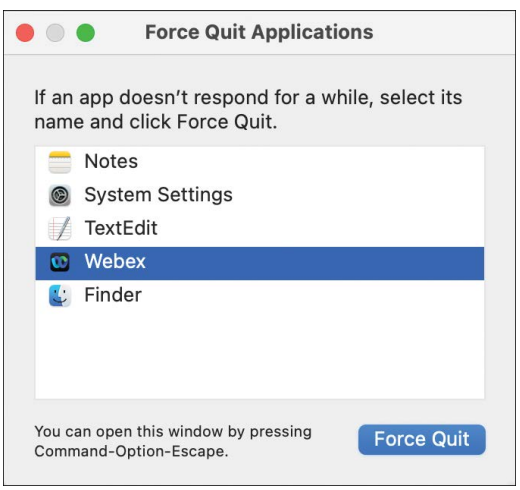


FIGURE 17.8 Force Quit Applications window

Another way of stopping an application is through the Terminal application, described later in this chapter. The Terminal program gives you access to a command prompt environment. Type

`top` to see currently running processes. Locate the process ID associated with the problematic application and press Ctrl+c to return to the command line. Next, type `kill -9 process_id` (replacing *`process_id`* with the process ID number associated with the problematic application).

Management and Troubleshooting Tools

macOS comes with a robust set of tools to keep a system running smoothly. But as with many other things in technology, they eventually break. As an IT professional, you need to understand what tools are at your disposal for fixing a system.

The most basic tool is the **System Settings** menu, which contains most of the system configuration tools, from desktop backgrounds and screen savers to more advanced settings such as user accounts and file sharing (see Figure 17.9). Third-party applications can also insert their own configuration items into the System Settings menu. Prior to macOS Ventura (version 13, released in October 2022), System Settings was known as System Preferences. Some of the tools have slightly different names in System Settings than in System Preferences. The System Settings app in macOS more closely resembles the Settings app in iOS.

By default, the System Settings shortcut is located on the Dock, and it is listed in Launchpad. It can also be opened from Finder: Select the *Applications* menu on the left sidebar and then click the *System Settings* icon. Table 17.3 lists all the default options in System Settings and provides a brief description of each one.

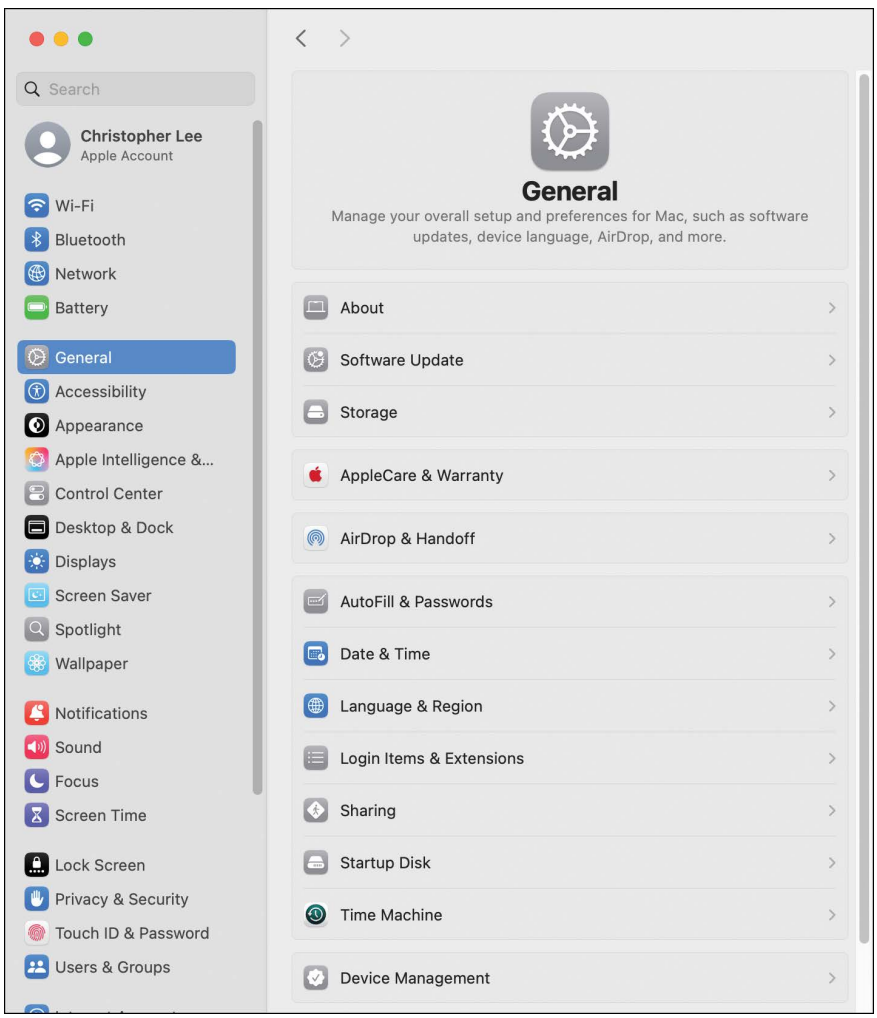


FIGURE 17.9 System Settings window

TABLE 17.3 System Settings options

Option	Description
Apple Account/ iCloud	Allows you to use your Apple ID to sign in for access to iCloud, the App Store, and other services.
Wi-Fi	Provides options to wirelessly connect to a local network and to the internet.
Bluetooth	Provides settings for toggling Bluetooth on and off and pairing devices such as Bluetooth headsets.
Network	Contains network settings for Ethernet, the macOS firewall, Thunderbolt, VPN, and so on.
Battery (Mobile)/Energy Saver (Desktop)	Provides settings to configure power options for the display and the computer. On laptops, allows users to monitor battery and power usage.
General	Enables you to manage your overall setup and preferences, including software updates, language and region, AirDrop, date and time, and sharing.
Accessibility	Provides settings for accessibility options such as colors, zoom, voiceover, captions, and more.
Appearance	Controls various visual settings, such as Light Mode vs. Dark Mode, system accent and highlight colors, wallpaper tinting, and scrollbar behaviors.
Apple Intelligence & Siri	Provides option to enable and configure Siri, a virtual personal assistant that responds to voice commands. Also provides option to enable Apple Intelligence, which uses generative artificial intelligence models to assist the user with writing, image creation, notifications, email, and other daily tasks.
Control Center	Controls which items appear in the Control Center on the menu bar.
Desktop & Dock	Provides settings for the size, location, and behavior of the dock. Also controls the appearance and behavior of Desktop windows and features like Mission Control.
Displays	Provides settings for managing the resolution, brightness, and color consistency of displays. Manages the layout when multiple displays are attached.
Screen Saver	Manages the appearance, timing, and security settings for the system screen saver.
Spotlight	Provides settings for what can and can't be searched.
Wallpaper	Manages the source of the wallpaper items that appear as the background for the Desktop.
Notifications	Provides settings for what apps can display notifications and how they are displayed.
Sound	Provides settings for the audio output/input, volume, balance of the sound between speakers, and system sounds for alerts.
Focus	Provides settings that can help minimize distractions from notifications.
Screen Time	Provides settings for managing restrictions for accounts, such as restricted websites, communication safety, time limits for computer usage, and application usage.
Lock Screen	Controls the behavior and appearance of the lock screen, which can appear after the computer has been idle.

Option	Description
Privacy & Security	Controls which apps can access your data, location, camera, and microphone. Manages other safety protections, such as FileVault, which automatically encrypts the contents of a disk.
Touch ID & Password	Provides settings to configure use of a password or your fingerprint to unlock your computer and make purchases.
Users & Groups	Provides settings for creating and deleting user accounts, as well as what groups they belong in.
Internet Accounts	Provides settings for management of email, contacts, calendars, messages, and other accounts.
Game Center	A social media gaming service that let you interact with friends, monitor achievements, and compete against other players.
Wallet & Apple Pay	Provides settings to add payment cards and use Apple Pay to make online purchases. Stores default payment details (name, address, phone number, and email address) for online purchases.
Keyboard	Provides settings for behaviors such as repeated keys, brightness, dictation, functions, shortcuts, and auto-correct.
Mouse	Provides settings for mouse speed, scroll direction, and primary mouse button side.
Trackpad	Provides settings for point and click, scroll and zoom, and multitouch gestures.
Printers & Scanners	Provides settings for adding and removing printers and scanning devices.

Safe Mode

Safe mode (sometimes called safe boot) allows a Mac computer to be booted with a slimmed-down version of the operating system. Some of the software that is normally loaded automatically is not loaded; user-installed fonts are not loaded; and font caches, kernel cache, and other system cache files are deleted. One really important function of safe mode is that the startup disk is checked and repaired, if possible, when issues are detected. Safe mode can also be used when removing malware.

TECH TIP

How to start a Mac in safe mode

Make sure the computer is completely shut down. Next, press and hold the power button until *Loading startup options* appears. Click your startup drive and then press and hold the ⇧Shift key. Then click *Continue in Safe Mode*. Release the ⇧Shift key. The computer boots into safe mode, with *Safe Boot* in red letters near the upper-right corner. Select an administrator account and enter the password.

Utilities

The tools located in the `Utilities` folder enable you to do more advanced system management, maintenance, and troubleshooting (see Figure 17.10). The path to the folder is *Finder* > *Applications* > *Utilities*.

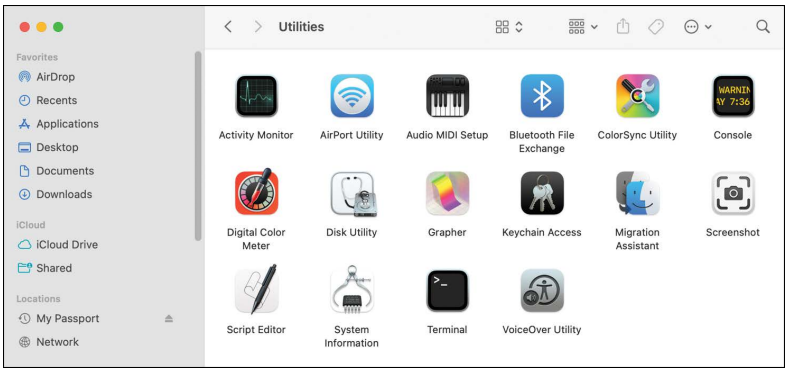


FIGURE 17.10 Utilities window

Activity Monitor

You need to be familiar with a few key utilities to properly troubleshoot a macOS system. **Activity Monitor** is a tool used to see what processes and services are running, as well as what system resources are being used. It is extremely useful in discovering why a system is running slowly (such as when an application appears to be frozen or when the system presents a constantly spinning **pinwheel**). You can look at the *CPU* tab (shown in Figure 17.11) to see what is consuming most of the CPU processing power. The *Memory* tab shows how much RAM each process is using, and the *Disk* tab provides a breakdown of how much disk read/write I/O is occurring. macOS automatically reserves some hard drive space to use as RAM. This is known as swap space. A good rule of thumb is to keep about 15% of the hard drive (and more, if possible) unused at all times. All these statistics are great tools for pinpointing poor system performance due to errant processes or lack of resources available for what the system is trying to do.

FIGURE 17.11 Activity Monitor > CPU tab

Console

The **Console** is a centralized place to find system and application logs and messages. macOS and the applications running on it constantly send activity logs to the Console. Within the Console, you can parse the logs manually or you can search for something specific. This is particularly helpful if you have an application or system service that is not behaving properly but that is not presenting an error message in the user interface. Most likely, if something has a problem, you can find a log explaining why in the Console. Figure 17.12 shows sample output in the Console.

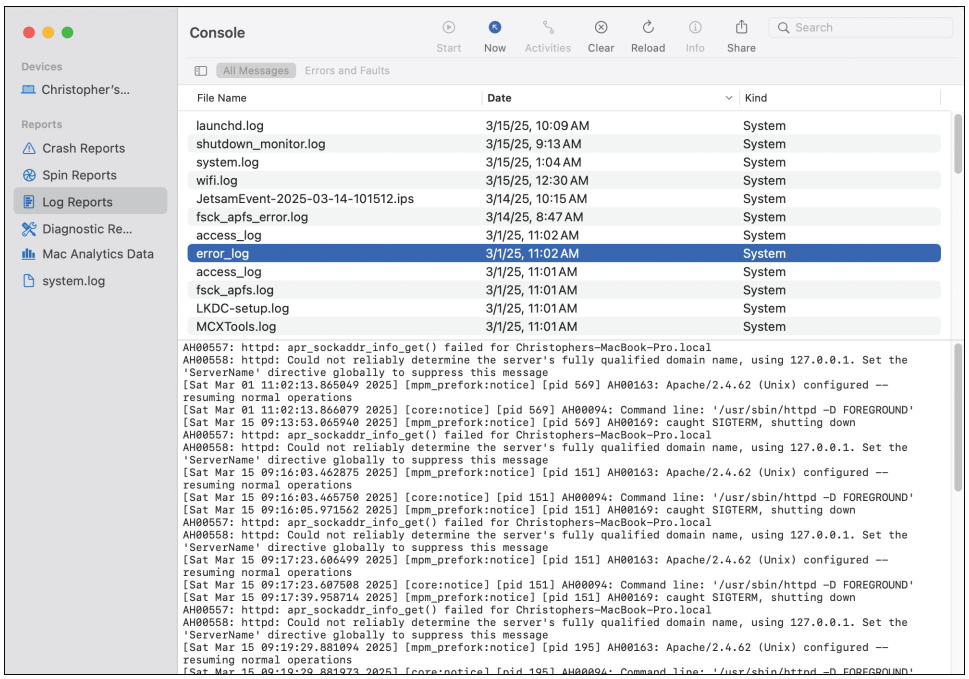


FIGURE 17.12 Console messages

Kernel Panic

The Console is good for troubleshooting **kernel panic**, which is a critical system error that the operating system cannot recover from. When this happens in macOS, the Mac reboots to return to a stable state. Trying to find the cause of kernel panic can be difficult because a wide array of issues can cause it, such as a hardware failure, an operating system failure, or a faulty application. If kernel panic happens only once, it is typically fine to ignore it. But if problems continue to occur, it is a good idea to consult the logs in the Console for help determining the cause. The kernel panic logs are saved in the `/Library/Logs/DiagnosticReports` directory, which can be viewed via the *Diagnostic Reports* option in the Console.

System Information

System Information is a utility that provides an overview of the Mac, including basic diagnostic information such as installed hardware, installed software, and network settings. If you need to find information about what is installed, such as the name of a graphics card or the firmware version used for the network card, this is the place to look. System Information can be accessed from the `Utilities` directory or by clicking the *Apple* icon in the upper-left corner on the menu bar, selecting *About This Mac* from the drop-down menu, and then selecting *System Report* at the bottom of the About window. Figure 17.13 shows sample output for hardware found through the System Information utility.

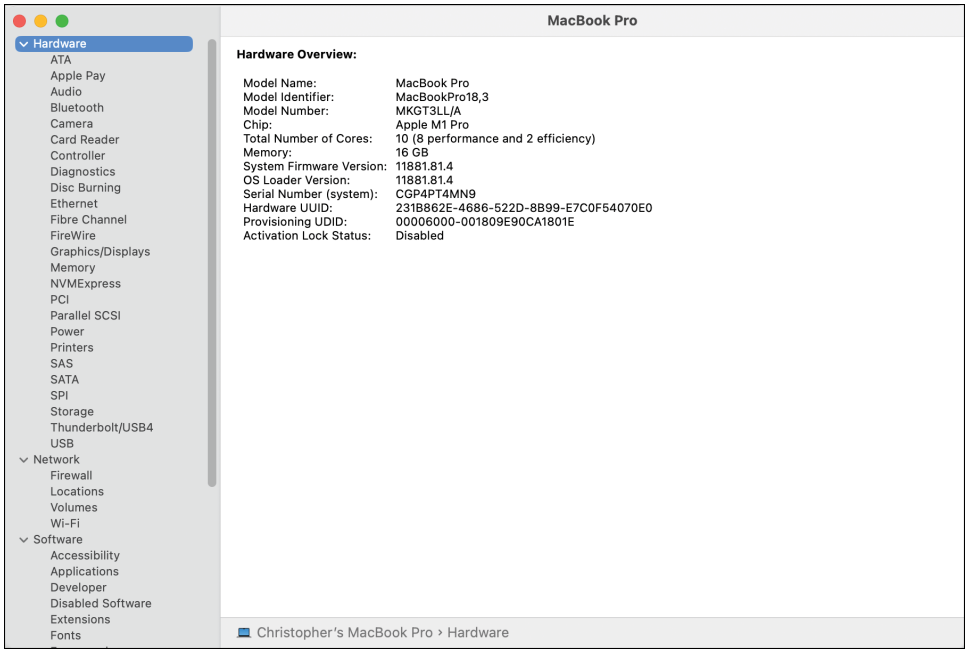


FIGURE 17.13 System Information > Hardware

Passwords App and Keychain Access

Beginning with macOS Sequoia (version 15, released in September 2024), the *Passwords* app securely stores all your passwords, passkeys (authentication using Touch ID or Face ID), and verification codes (used in two-factor verification) for applications, websites, Wi-Fi networks, and other services. When you enable *AutoFill* in *System Settings* > *General* > *AutoFill & Passwords*, your credentials are automatically saved in Passwords. The credentials are then used to automatically log you in to the same site or service when you access it again. You can use Passwords to recover a password if you forget it. If you sign in with the same Apple account on multiple devices, you can share the stored passwords across those devices. To use the Passwords sharing feature, you must enable Passwords in iCloud settings, and you must update all the devices to the latest software version.

In macOS versions prior to Sequoia, passwords are stored in Keychain Access. Like Passwords, **Keychain Access** securely manages saved passwords so users do not have to remember them. The passwords in Keychain Access are encrypted by default. A keychain file can be unlocked using the login password; however, you can set up a different password for the keychain for additional security. In macOS versions beginning with Sequoia, the Keychain Access feature only manages security certificates, which are issued by trusted organizations to validate websites, digital documents, and other web-based materials.

When you change your Mac login password, your keychain password may not automatically update, and the mismatch would cause your Mac to ask for the old keychain password. This can occur if you use a network-based account where the password was updated on a server or if you reset your password using macOS recovery mode. To fix this, open *Applications* > *Utilities* > *Keychain Access*, select the login keychain, and go to *Edit* > *Change Password* for Keychain 'login'. Enter your old password (the one before you changed it) and then enter your new login password and confirm it. The keychain password is updated to match your new login password. If you don't know your old password, you'll need to create a new keychain, but keep in mind that doing so will erase all your saved passwords.

It is easy to forget passwords. Both Passwords and Keychain Access allow you to see saved passwords. For example, if you are already connected to a Wi-Fi network and need to know the password in order to connect another device, you can open *Passwords* > *Wi-Fi* category > click the entry for the Wi-Fi network > click into the *Password* field to see the password. In the *Keychain Access* utility, select *Local Items* > double-click the entry for the Wi-Fi network > enable the *Show password* option. You are then prompted to authenticate with your keychain password. You then see the saved password, unencrypted, as shown in Figure 17.14.

FIGURE 17.14 Viewing a password in Keychain Access

TECH TIP

What to do if users cannot remember their keychain password

A user who cannot remember their old keychain password needs to start a new keychain. This is done by selecting the Keychain Access *Preferences* drop-down menu > *Reset My Default Keychain*. The user can either delete the old keychain or opt to keep it in case they later remember the password.

Disk Utility

Disk Utility allows you to manage disks and disk images in macOS (see Figure 17.15). This utility can be used to rename, reformat, erase, repair, and restore disks. It is a powerful tool and should be used with caution because it is easy to delete all the data on a system disk or on an external disk attached to the system.

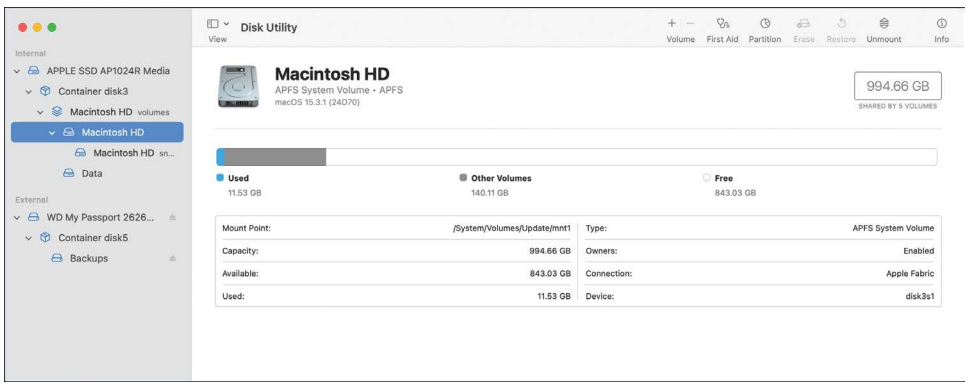


FIGURE 17.15 macOS Disk Utility

When a drive is connected to a Mac, it is mounted and shows up on the left side of the Disk Utility window. Selecting a drive gives you a handful of options: First Aid, Erase, Partition, Restore, Unmount, and Info.

The *First Aid* option is similar to `fsck` or `chkdsk` in Windows. It checks the integrity of the file system on a system and repairs any issues it finds. It is highly advisable not to run First Aid unless you have a system backup and have a reason to run it, such as when a system boots only into safe mode or into recovery mode.

The *Erase* option allows you to wipe a disk, choose the format for the disk, and name the partition. You may also perform a secure erase by going into the security options on the menu. Secure erase has a few options, all of which write 0s or random data over the previous data on the disk to make it unrecoverable. You can choose no passes of zeros to quickly wipe out the disk, one pass of zeros, three passes of various types of data for an erase that is Department of Energy (DOE) compliant, or a seven-pass erase that meets the Department of Defense (DOD) standard for safely deleting data. Keep in mind that the more passes you do, the longer it takes to erase the disk.

The *Partition* tab enables you to manage the addition and deletion of partitions on a disk. An interactive chart shows the physical partition layout. You can adjust the chart with your mouse cursor to resize existing partitions, free up space to add new partitions, or free up space to expand a partition. As with any other disk modification, you need to make sure you have backed up any data for a disk that you are repartitioning. Even if the partitioning is done properly, there is a risk of corruption and data loss.

macOS supports Hierarchical File System Plus (HFS+), also known as macOS Extended, as well as Apple File System (APFS), which supports SSDs and allows drive volumes to be reduced or increased as needed. To view the type of file system being used on a drive, select the drive in Disk Utility, and the file system type displays under the name of the disk.

Boot Camp

Boot Camp is a boot-loading utility designed to assist with partitioning, installation, and support in running Windows on a Mac. Installation requires a Mac with an Intel-based processor, a USB flash drive with at least 16 GB of space, a Windows installation ISO file or DVD installer, and a minimum of 64 GB of free space on the startup drive of the Mac. The Boot Camp application guides you through the process of repartitioning your hard drive to make a partition labeled `BOOTCAMP`. It also copies the Windows ISO or DVD installer to the USB flash drive and copies the appropriate Mac drivers to it.

After Boot Camp sets up the partition and copies everything you need to the flash drive, it reboots the system into the Windows installer, where you can complete the installation. Boot Camp can also be used to remove a Windows partition. Make sure you back up a system before doing anything involving partitioning.

Terminal

Terminal is the terminal emulator for macOS. It allows command-line interface (CLI) access to the operating system. Although the majority of things you do in macOS can be performed in the GUI, there are times when using the CLI is required. The Terminal application can be found in the `Applications` folder > `Utilities` subfolder. You need to know how to use at least a few basic commands in case you run into a situation that can be fixed only by using Terminal. Table 17.4 outlines some of the most basic and commonly used commands. (More commands are provided later in the chapter.)

TABLE 17.4 Commonly used macOS commands

Command	Description
`pwd`	Shows the current working directory path.
`cd`	Moves between directories.
`touch`	Creates a file.
`mkdir`	Creates a directory.
`cp`	Copies a file.
`mv`	Moves a file.
`rm`	Deletes a file or directory.
`ls`	Lists the contents of the current working directory.
`chown`	Changes ownership.
`chmod`	Changes file permissions.
`su`	Switch to another user account, including root.
`sudo`	Temporarily allows root privileges.
`kill`	Stops a process ID associated with a particular application.
`nano`	Opens an easy-to-use text editor.
`vi`	Opens a text editor that is used by more experienced Linux users.
`less`	Shows the contents of a file.
`grep`	Searches output for a specified search term.
`man`	When followed by another command, brings up a manual for using that command.

The basic commands in Table 17.4 are enough to navigate the file system, create and remove files and directories, and do some basic troubleshooting. Keep in mind that for all these commands, you can use a variety of flags. It is a good idea to reference the `man` page to discover what a command can do if you are unfamiliar with it. For example, the `ls` command run by itself shows the contents of the current working directory, but you can also specify a directory that is not the one where you are working so you can see its contents, as shown here:

```
testmac:~ testuser$ ls
Applications Desktop Documents Downloads Dropbox Library Movies Music
Pictures Public
testmac:~ testuser$ ls Public
Drop Box
```

As you can see here, by using `ls` and specifying another directory (in this case `Public`), the contents of the `Public` folder can be seen instead of the user's home folder. The following paragraphs provide brief examples of using the commands listed in Table 17.4.

`ls` lists the contents of a directory, including any directories located inside the current path in the file system. Here is an example:

```
testmac:~ testuser$ ls
Applications Desktop Documents Downloads Dropbox Library Movies Music
Pictures Public
```

pwd identifies the current working path, as shown in this example:

```
testmac:~ testuser$ pwd
/Users/testuser
```

cd, which is short for *change directory*, does exactly what its name indicates. Typing cd followed by a directory takes you to that directory. Notice that the working path is updated on the command line to keep track of the current location:

```
testmac:~ testuser$ cd Applications
testmac:Applications testuser$
```

touch creates a blank file with the specified name. This command is not limited to text files. For example, you could make a file with the extension html if you wanted to create a web page. Notice in the following example that the modifier -l and the filename **test.txt** are added to the ls command when showing the file created with the touch command:

```
testmac:~ testuser$ touch test.txt
testmac:~ testuser$ ls -l test.txt
-rw-r--r-- 1 testuser Editors 0 Sep 29 13:56 test.txt
```

The -l modifier is a flag for what is called *long listing*, which includes the normal output of the ls command plus add-ins. From left to right, the add-ins are as follows: file permission, number of file links, owner name, owner group, file size, time of last modification, and filename. In this example, instead of seeing all contents of the directory, you see only the file specifics.

cp is short for *copy*. The syntax of this command is cp followed by the source file and then the destination of the copy. You can also rename a file while copying it. Consider this example:

```
testmac:~ testuser$ cp test.txt testcopy.txt
testmac:~ testuser$ ls
Applications Documents Dropbox Movies Public
test.txt Desktop Downloads Library Music Pictures testcopy.txt
```

mv is short for *move*. It works similarly to cp, except it does not keep the original file in place. It actually modifies the file by moving it in the file system. During this process, you have the option to rename the file. In the following example, the testcopy.txt file was moved to testmove.txt:

```
testmac:~ testuser$ mv testcopy.txt testmove.txt
testmac:~ testuser$ ls
Applications Documents Dropbox Movies Public
test.txt Desktop Downloads Library Music Pictures testmove.txt
```

The file testcopy.txt is not listed because it is now named testmove.txt.

rm is short for *remove*. By using the rm command, you can designate which file or files to remove, as in this example:

```
testmac:~ testuser$ rm test.txt testmove.txt
testmac:~ testuser$ ls
Applications Desktop Documents Downloads Dropbox Library Movies Music Public
```

sudo is a command used to gain superuser (also known as root) privileges. In Unix/Linux, the administrator account is known as **root**. The root user has absolute power on a system, including within macOS. However, by default, this user account is disabled. It is not a good idea to log in directly using root when you don't really need to because if you were to accidentally run

something malicious, the system could be degraded or compromised. However, administrative access is occasionally needed to perform certain tasks, such as running a script or installing an application. When you need such access at the command-line level, use the `sudo` command, which invokes a temporary root session to complete the command you are running.

In the following example, the file importantdocument.txt is created:

```
testmac:~ testuser$ touch importantdocument.txt
testmac:~ testuser$ ls -l importantdocument.txt
-rw-r--r-- 1 testuser Editors 0 Sep 30 10:39 importantdocument.txt
testmac:~ testuser$ chown root importantdocument.txt
chown: importantdocument.txt: Operation not permitted
testmac:~ testuser$ sudo chown root importantdocument.txt
Password:
testmac:~ testuser$ ls -l importantdocument.txt
-rw-r--r-- 1 root Editors 0 Sep 30 10:39 importantdocument.txt
```

When you run `ls -l` for the file, you can see that you are the owner of it. Then you want to make root the owner of the file, so you attempt to use the command `chown`, which changes file ownership. When `chown` is run, the message `Operation not permitted` appears, indicating that you do not have permission to do this. To fix this, you add `sudo` to the start of the command. When prompted, you enter your account password for verification. The command runs as the root user. When you use `ls -l` again, you can see that the file owner changes from testuser to root.

To understand how to use the `chmod` command, you have to understand Unix/Linux file permissions. There are three types of permissions a user or group can have for a file: read, write, and execute. Permissions are indicated using the `-rwxrwxrwx` notation, with `r` being read, `w` being write, and `x` being execute. Notice the three sets of `rwx` entries. Starting from the left, the first set represents the owner's permissions. The second set represents the group's permissions. The last set represents everyone else (also known as others). In the following example, look at the leftmost entries:

```
testmac:~ testuser$ ls -l importantdocument.txt
-rw-rw-r-- 1 root Editors 0 Sep 30 10:39 importantdocument.txt
```

The root owner of the file can read and write to the file, as designated by the first set of letters, `rw`. The users belonging to the Editors group can also read and write to the file, as shown by the second set of letters, `rw`. Everyone else can only read the file and is not allowed to modify it in any way, as designated by the last, `r`.

To use `chmod` to change these permissions, there are various syntax options. The easiest option to visualize uses letters. For instance, to add a write permission to the `importantdocument.txt` file for those known as others, use `o+w`, as shown in the following example:

```
testmac:~ testuser$ sudo chmod o+w importantdocument.txt
Password:
testmac:~ testuser$ ls -l importantdocument.txt
-rw-rw-rw- 1 root Editors 0 Sep 30 10:39 importantdocument.txt
```

This syntax can be used with the letters `u` (user), `g` (group), `o` (other), and `a` (all). The letters `r`, `w`, and `x` are then used to signify what permissions to either add or subtract for the subject specified. Then you specify the file for which permissions are to be changed.

Another way of specifying permissions is to use numbers to represent the permissions. The syntax for this is a three-digit number string. Starting from the left, the first number represents the

owner, the second number represents the group, and the final number represents others. The numbers range from 0 to 7, and they are translated into binary numbers to represent the permissions value, but an easy thing to do is remember that read permission equals `4`, write permission equals `2`, and execute permission equals `1`. All the permissions you want to assign are added together. For example, let's assign the read (`4`), write (`2`), and execute (`1`) permissions to the root user; assign the read (`4`) permission to the group; and assign no (`0`) permissions to others. The resulting number string is `740`. You can then use the command `chmod` followed by this number and then the file that is changed. The following example shows what this looks like:

```
testmac:~ testuser$ ls -l importantdocument.txt
-rw-rw-rw- 1 root Editors 0 Sep 30 10:39 importantdocument.txt
testmac:~ testuser$ sudo chmod 740 importantdocument.txt
Password:
testmac:~ testuser$ ls -l importantdocument.txt
-rwxr----- 1 root Editors 0 Sep 30 10:39 importantdocument.txt
```

`nano` is a text editor. When using the command line, it is common to use a text editor to fix files. Instead of going through the slow process of using a graphical text editor and navigating to the file to open it, you can quickly edit a file at the command line.

There are a few command-line text editors available in macOS and Linux, including `vi`, `emacs`, and `nano`. `nano` is an easy-to-use command-line text editor. You launch it by typing `nano` followed by the name of the file you want to edit. If the file does not exist, `nano` creates it. Entering the command `q` cancels the editing session. `nano` is a powerful editor with many options, such as search and replace, line numbers, and quick navigation with page up/page down. It also has a set of quick controls displayed in its interface, which is helpful for occasional users who have not memorized all the shortcuts.

`less` is a tool you can use to quickly view the contents of a file. It presents a window of the contents that you can scroll through by using the [b] key to scroll up and [Spacebar] to scroll down; you can also page to the bottom by holding down [⇧Shift] and pressing the [b] key. `less` becomes a powerful tool when combined with a search utility known as `grep` and the | (pipe) function. The [|] key is used for passing output from one command to another. You can use `less` to see the content of a file and then pipe it to `grep` to search for something inside it. For example, you can add the following text to the `importantdocument.txt` file with which you have been working:

```
OS X 10.8 Mountain Lion
OS X 10.9 Mavericks
OS X 10.10 Yosemite
OS X 10.11 El Capitan
```

If you want to find this information somewhere within a few hundred pages, it will be difficult to find it by just reading the document. Using `nano` to search could also take a long time because you would have to run the search over and over to find all the multiple entries. A better command to use in this case is `less` to get the output of the file and send it to `grep` to search for the wanted text:

```
testmac:~ testuser$ less importantdocument.txt | grep Yosemite
OS X 10.10    Yosemite
```

You can see that `grep` works by taking the input it receives and using it as a search source. It then outputs every line of the input (`importantdocument.txt`) that contains the search term.

TECH TIP

Use the manual!

You need to know your commands and their options, but it is easy to forget the ones that you do not use often. When you cannot remember how to use a command, use the command `man` (which is short for *manual*). `man` brings up directions on how to use any command for which there is a manual page entry. The syntax is simply the command `man` followed by the command you want to know more about.

Introduction to Linux

Linux was released in 1991 by developer Linus Torvalds. It is a widely used operating system platform that is similar to trademarked UNIX, which was developed by AT&T. Linux is meant to be a free open source operating system that everyone can use, contribute to, and modify as needed. Because of this, it is widely used in many different areas of technology, such as servers, desktops, embedded systems, and smartphones. It is also mostly POSIX compliant, so some of the concepts you have already learned in this chapter about macOS also apply to most Linux systems.

The terminology of Linux can be confusing for someone who is new to it. The name *Linux* refers to an operating system kernel. A **kernel** is the heart of an operating system. It acts as the controller and interpreter for nearly everything in a system, so hardware and software can interface and work together. It controls things such as memory management, peripherals, and the allocation of other system resources to processes.

The Linux kernel is repackaged into different operating system distributions (*distros* for short). There are hundreds of different distros. Table 17.5 lists the most popular ones and where to find more information about them. Although these distros are all different from one another in some ways, they are all Linux operating systems because they all use the Linux kernel.

TABLE 17.5 Linux distros

Distro name	Website
Ubuntu	http://www.ubuntu.com
Debian	http://www.debian.org
Mint	http://linuxmint.com
SUSE	https://www.suse.com
Red Hat	http://www.redhat.com
Fedora	https://getfedora.org
CentOS	https://www.centos.org
Gentoo	https://www.gentoo.org
Arch	https://www.archlinux.org
Kali	https://www.kali.org

Anyone going into IT should explore the various Linux distros to see the differences and similarities among them. Ubuntu is the most widely used home desktop distribution, and it also has a server version. Although you probably will not find Ubuntu in an enterprise environment, you are likely to encounter it with end users, developers, and simple servers. And a lot of the skills you learn for Ubuntu are useful with other distros.

You do not have to install Ubuntu onto a computer to experiment with it. Unlike Windows or macOS, you can run Ubuntu as a live CD or DVD. That means you can boot the computer from a CD, DVD, or flash drive and then run the Ubuntu operating system from that drive as if Ubuntu were installed on the computer. This makes it much easier to try different distributions without having to dedicate a computer solely to running Linux. If you do launch Linux from a CD, DVD, or flash drive, however, you need to be careful because you can still modify the local file system on the computer and cause harm to the installed operating system.

TECH TIP

Downloading Ubuntu

Download Ubuntu's latest release from http://www.ubuntu.com/download/desktop. It will be needed to complete some of the labs.

OS Components and Common Configuration Files

Several Linux components work in conjunction with the kernel. One such component is the bootloader. The bootloader is a small program that initiates the booting process. After the BIOS/UEFI performs initial system tests, it transfers control to the bootloader. If the boot disk has multiple operating systems installed on it, the bootloader can present an interactive boot manager menu so the user can select an OS. The bootloader then locates the kernel of the operating system and loads the kernel into RAM. After the kernel is loaded, the bootloader transfers control of the computer to the kernel, which loads the rest of the operating system into RAM.

systemd, a system and service manager, is another major Linux component. It manages the boot process, starts and stops services, and handles system shutdown. After the kernel initializes the hardware, it starts the systemd process, so systemd is the first Linux process running on the computer (also known as PID1, for Process ID 1). The systemd process then starts all the other operating system processes, which can spawn their own child processes. When the computer is fully booted, systemd continues to run in the background.

Configuration files control the behavior of the operating system, as well as the functionality of applications that run in the operating system. Configuration files are usually plaintext files that can be edited with text editors like `nano`. The `/etc/passwd` file stores user account information like usernames, group IDs, and home directories. Actual passwords are stored in `/etc/shadow`, which is encrypted for security purposes. The `/etc/fstab` file specifies which file systems (disks or other directories) are mounted to the computer when it boots.

The `/etc/resolv.conf` and `/etc/hosts` files help the computer convert hostnames to IP addresses. The `/etc/resolv.conf` file contains a list of network DNS servers. If the computer is connected to a network, the computer sends a hostname to a DNS server, and the DNS server responds with the IP address associated with that hostname. Similarly, the `/etc/hosts` file contains a list of hostnames and their associated IP addresses. Before the computer sends a hostname to a DNS server, it searches for the hostname and the IP address in `/etc/hosts`. In other words, the entries in `/etc/hosts` override the network DNS associations.

Navigating the User Interface

There are many types of graphical user interfaces for Linux, such as GNOME, KDE, Xfce, and Cinnamon, each with unique interface operation and tools. GNOME is the name of the graphical

user interface in Ubuntu. It has some similarities to the user interface of macOS, but it is drastically different from the Windows user interface.

The **dash** is the shortcut bar on the left side of the screen. It is an application **launcher** with a built-in search tool. It is reminiscent of the macOS Dock, but it doesn't work completely the same. Clicking a shortcut in the dash opens its application. If you right-click or Ctrl-click the icon, a context window appears. The *Show Apps* button at the bottom reveals several other applications. When you click the *Activities* button at the top of the dash, you open the Activities Overview. The Activities Overview shows all open windows and applications, as well as a menu for a local search tool that can get results for applications, files, folders, and the internet.

The bar at the top of the screen contains an appointment calendar in the middle and a System menu on the right side. The System menu displays status icons for the network connection, sound, and other subsystems. It allows you to change the volume or screen brightness, edit your Wi-Fi connection details, check your battery status, log out or switch users, and turn off your computer.

Nautilus is the file manager for Ubuntu (see Figure 17.16). You can quickly access it by clicking the *Files* icon on the *dash*. Nautilus is the default file manager, but because Linux is so modular and customizable, it can be replaced with an alternative file manager. Like all other GUI operating systems, Linux has a standard desktop.

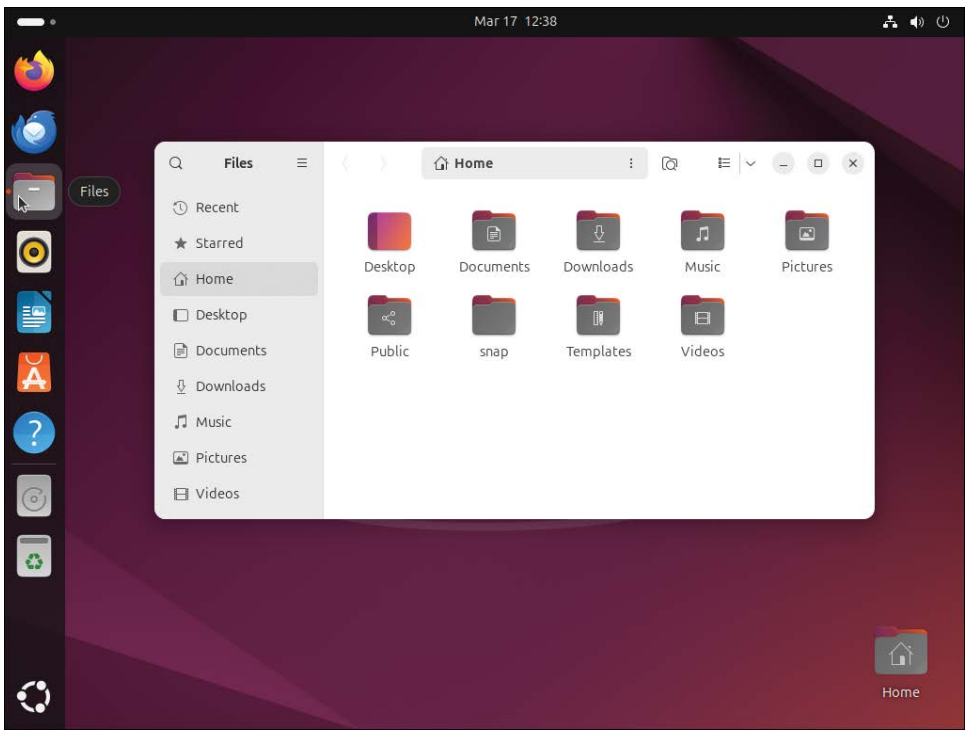


FIGURE 17.16 Nautilus file manager window

The universal search tool that is built into the Launcher searches local content, and it can be configured to search the internet as well. The search locations can be enabled or disabled in *dash* > *Show Apps* > *Settings* > *Search*. Search results appear in subcategories, called lenses, at the bottom of the search interface (see Figure 17.17).

The Ubuntu user interface is straightforward, which makes it convenient for home use. A Linux system in an enterprise environment is not accessed through the GUI. Most of the Linux systems in corporate environments do not even have a GUI installed. However, a few GUI tools should be mentioned, and they are covered in the following sections.

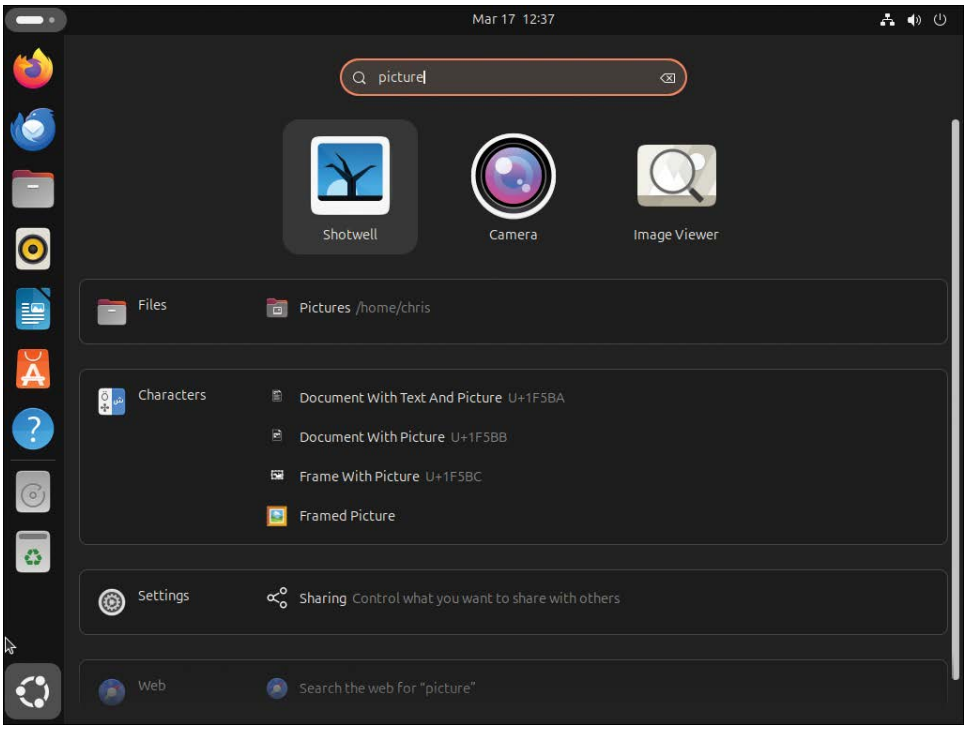


FIGURE 17.17 dash's search tool

Basic System Usage, Updates, and Backups

Numerous useful system management tools come bundled with Ubuntu. Some of them are best used through the GUI. Although everything can be done through the command-line interface, some tools are much easier to use on the desktop.

The best example of this is Disks, a disk management tool that allows for the creation, deletion, and resizing of partitions on a physical disk (see Figure 17.18). Disks has an easy-to-use drag-and-drop interface for partition management that is far easier to visualize and understand than the command line. If you experiment with Disks, be mindful that you can wipe out your system if you are unsure of the correct procedures.

Whereas Windows mostly uses NTFS, and macOS uses HFS+ or APFS, there are many more file system options to choose from with Linux. When installing Linux or partitioning with Disks, you need to be aware of these options. Table 17.6 lists and describes the most common file systems. Most distros, including Ubuntu, default to using a file system known as **ext4** (fourth extended file system), an improvement on ext3 (third extended file system), which was the most widely used file system for many years.

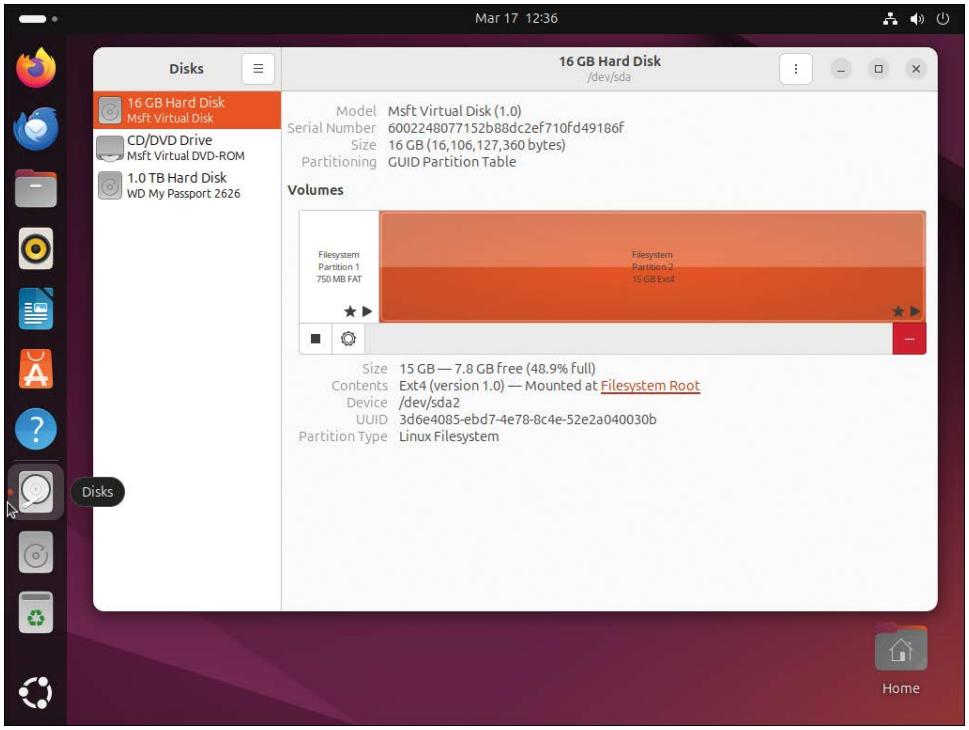


FIGURE 17.18 Disks window

TABLE 17.6 Linux file systems

File system name	Description
ext4	Fourth generation of the extended file system, which contains features such as journaling, volume support up to 1 exbibyte (EiB), and file sizes up to 16 tebibytes (TiB). It is a common file system choice.
XFS	Extended File System, created by Silicon Graphics for its IRIX operating system, which was ported to the Linux kernel with version 2.4. XFS is suitable for enterprise-level computing (such as data centers) because it efficiently handles extremely large file systems (in the petabyte range).
ZFS	File system that focuses on data integrity and that can do integrity checks on mounted disks (unlike ext4). ZFS provides built-in RAID support, including mirroring and parity, for redundancy and data protection.
Btrfs	Pronounced "butter F S," adds features absent in ext4, such as snapshots, volume spanning, live resizing of file systems, and live addition/removal of disks to live file systems. It can support volumes and file sizes up to 16 EiB.

Ubuntu comes with a fair amount of software installed, but one of the great things about using Linux is the amount of free open source software available. It isn't always easy to find software, especially if you are new to Linux and are unfamiliar with the tools that are available. *App Center* is a software manager that lets you access software from Ubuntu's repositories. The App Center launcher is in the dash. App Center was previously known as GNOME Software and as Ubuntu Software Center prior to that. With App Center (shown in Figure 17.19), you can browse, install, and manage applications from the Ubuntu Software Store (formerly known as the App Store). Many of the applications are available for free. While App Center is useful for managing software applications, you need to use the **Software Updater** tool to update the operating system.

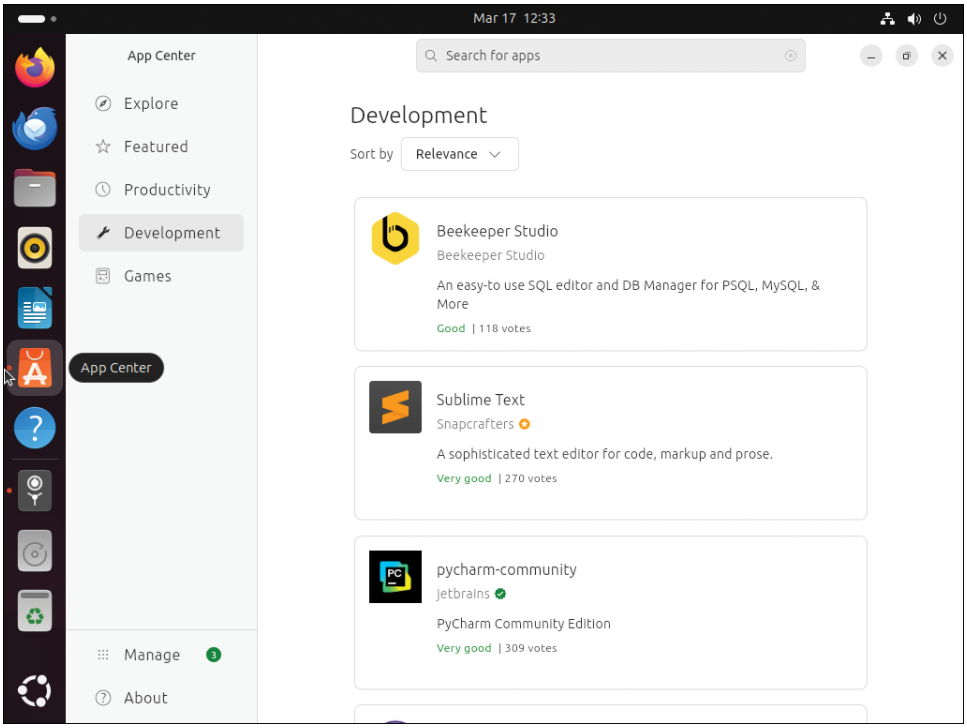


FIGURE 17.19 Ubuntu App Center

Ubuntu comes bundled with Backups, a built-in backup application (see Figure 17.20) that supports local and remote backups, encryption, and scheduling; in addition, it can run seamlessly in the background. The Backups application can be found by searching for `backups` in the GNOME search tool.

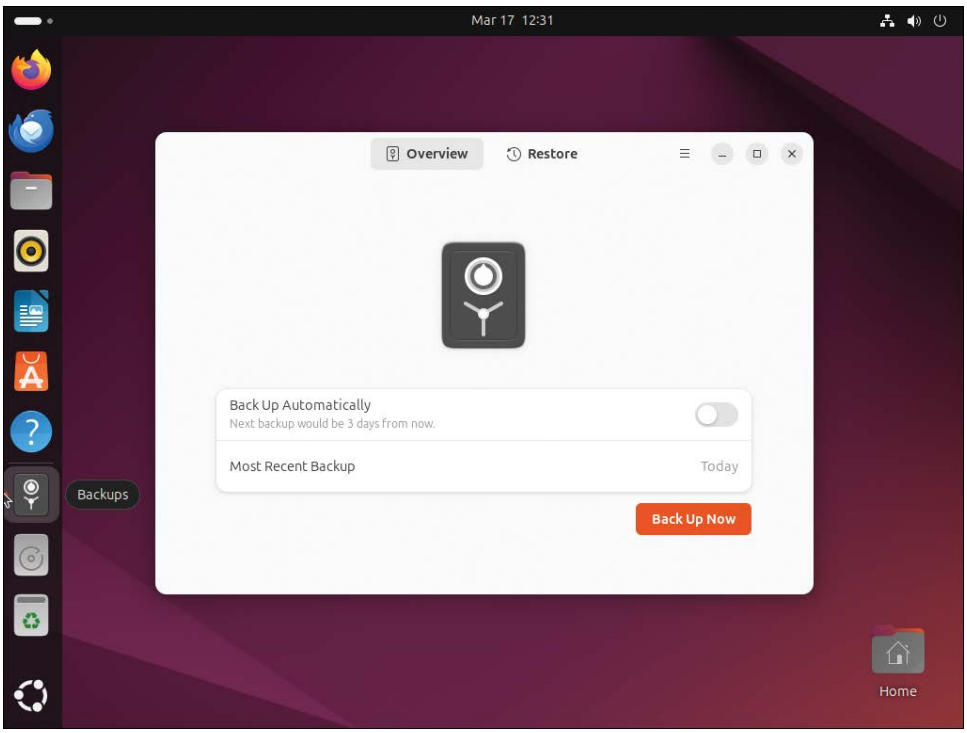


FIGURE 17.20 Ubuntu's Backups application

A wide array of other backup software is available for Linux. Many companies have their own backup procedures that use custom scripts and various utilities, such as `rsync`, to use fewer resources compared to doing a full system backup, as experienced in most Windows environments.

Command-Line Interface

Most system management for Linux and Unix systems takes place in the **command-line interface** (CLI). The CLI for most Linux systems uses a terminal language known as bash. bash is simply the command language used in the CLI, but there are a few other notable shells, such as Dash, fish, zsh, and tcsh. Since Ubuntu and most other distros use bash, we focus on bash for the rest of this chapter.

You may want to refer to Table 17.4 to review basic command-line usage in macOS. Because both macOS and Linux are based on Unix, those commands also work in Linux. There are also more advanced commands that everyone who supports Linux systems should know. Table 17.7 lists and briefly describes these commands.

TABLE 17.7 Advanced CLI commands

Command	Description
`shutdown`	Shuts down or restarts the system, depending on the options used.
`passwd`	Sets the password for a user.
`su`	Switches from one user account to another.
`ip`	Shows and configures network-related settings such as interface, IP address, and routing settings.
`iwconfig`	Shows network interface information for wireless adapters.
`apt`	Allows management of application packages.
`ps`	Shows a list of all currently running processes.
`top`	Displays real-time dynamic information about running processes and system resources.
`locate`	Searches the system for a file.
`updatedb`	Updates the file database of the system for the `locate` command.
`mount`	Adds a new file system (a disk or another directory) to the system's directory tree or displays currently mounted file systems.
`df`	Displays free disk space.
`fsck`	Checks file system consistency and interactively repairs issues.
`dd`	Copies and converts files.

To use the CLI on Ubuntu, click the *Activities* button at the top of the dash and search for *Terminal*. If a few options appear, you might want to use the one specifically labeled *Terminal*. This interface is similar to the macOS interface in that the command line shows the username and computer name.

Shutting Down the System

The `shutdown` command is straightforward: It shuts down the system. Here is an example:

```
chris@ubuntunVM-2:~$ sudo shutdown
[sudo] password for chris:
Shutdown scheduled for Mon 2025-03-17 13:00:31 EDT, use 'shutdown -c' to
cancel.
```

The `sudo` command is used before the `shutdown` command because you must have superuser permissions when you run the `shutdown` command. By default, running `shutdown` schedules a shutdown one minute into the future, which gives you an opportunity to cancel it. There are also options to schedule the shutdown for a different time, to have the shutdown happen immediately, or to restart instead of powering off. You can also have a shutdown message broadcast to warn anyone else who might be logged in to the system.

`passwd` vs. `pwd`

The `passwd` command (not to be confused with `pwd`) is used to change a user's password. Remember that the `pwd` command is used to view the current working directory. To change the logged-in user's password, just run the `passwd` command by itself. A prompt appears, where you can enter the current password and then enter the new password twice, as shown here:

```
chris@ubuntunVM-2:~$ passwd
Changing password for chris.
Current password:
New password:
Retype new password:
passwd: password updated successfully
```

If you want to change the password of a different user, enter the command followed by the username, as shown here:

```
chris@ubuntunVM-2:~$ sudo passwd test
[sudo] password for chris:
New password:
Retype new password:
passwd: password updated successfully
```

Note that you must have superuser permissions to change another user's password. To modify an account, you either need to be logged in to that account or have administrative (root) privileges.

Performing Network Configuration

The `ifconfig` command is a legacy tool used to display and configure network interfaces on Linux systems. The `ip` command is a modern replacement for `ifconfig`, and all Linux administrators and users need to be familiar with it. The basic output of the `ip` command shows the current network settings, such as IP addresses, subnet masks, interfaces used, and MAC addresses, as you can see in this example:

```
chris@ubuntu24:~$ ip link show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group
default qlen 1000
```

```
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group
default qlen 1000
    link/ether 00:15:5d:97:3f:0b brd ff:ff:ff:ff:ff:ff
    inet 192.168.32.114/24 brd 192.168.32.255 scope global dynamic
noprefixroute eth0
       valid_lft 86277sec preferred_lft 86277sec
    inet6 fe80::215:5dff:fe97:3f0b/64 scope link
       valid_lft forever preferred_lft forever
```

This output presents two different interfaces. `lo` is an abbreviation for localhost, a loopback interface that is used for testing and routing information inside the operating system. `eth0` is an abbreviation for ethernet 0, the wired Ethernet connection.

More advanced use of `ip` allows you to change interface settings. If you want to change an address for `eth0`, you can use `ip` in the following manner:

```
ubuntu@ubuntu:~$ sudo ip address add eth0 192.168.43.8/255.255.255.0
ubuntu@ubuntu:~$ ip address show eth0
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group
default qlen 1000
    link/ether 00:15:5d:97:3f:0b brd ff:ff:ff:ff:ff:ff
    inet 192.168.32.114/24 brd 192.168.32.255 scope global dynamic
noprefixroute eth0
       valid_lft 84773sec preferred_lft 84773sec
    inet 192.168.32.8/32 scope global eth0
       valid_lft forever preferred_lft forever
    inet6 fe80::215:5dff:fe97:3f0b/64 scope link
       valid_lft forever preferred_lft forever
```

Wireless network adapters require wireless-specific settings, such as the wireless network SSID, as well as any authentication settings that must be configured. The `iwlist` command can be used to get a list of available SSIDs, and `wpa_supplicant` can be used to securely connect a wireless interface to an SSID.

Viewing Processes

`ps` is another command to have in your toolbox for administering a Linux system. `ps` shows all active processes running on a system. This important information tells you what is running, how long things have been running, and how many resources are being used. Here is an example:

```
ubuntu@ubuntu:~$ ps
 PID TTY TIME CMD
 4093 pts/0 00:00:01 bash
14766 pts/0 00:00:00 ps
```

By default, ps shows only processes being run by the current user and from the current login session. Generally, you use ps along with other modifiers to get useful information. The most common version of ps is ps aux. The a modifier lists all processes from other users, u shows the user who is running the process, and x shows processes from all sessions. The ps aux command effectively shows everything that is running on the system. Here is an example:

```
ubuntu@ubuntu:~$ ps aux
USER PID %CPU %MEM VSZ RSS TTY STAT START TIME COMMAND
root 1 0.0 0.1 2148 1348 ? Ss Oct23 0:10 init [2]
root 2 0.0 0.0 0 0 ? S Oct23 0:00 [kthreadd]
root 3 0.0 0.0 0 0 ? S Oct23 0:16 [ksoftirqd/0]
root 5 0.0 0.0 0 0 ? S< Oct23 0:00 [kworker/0:0H]
root 7 0.0 0.0 0 0 ? S Oct23 1:53 [rcu_preempt]
root 8 0.0 0.0 0 0 ? S Oct23 0:00 [rcu_sched]
root 9 0.0 0.0 0 0 ? S Oct23 0:00 [rcu_bh]
```

A lesser-known option is to add the f modifier, so the command is ps faux. This shows everything from ps aux and also organizes the processes in a tree format so you can see what processes are the parent and what processes are the child. In the following example, a screen session is running for a script being run by the program supervisor. Some of the command output has been omitted here to make it easier to read:

```
root 2316 0.0 0.3 4816 2372 ? Ss Oct23 1:02 SCREEN
root 2317 0.0 0.5 5680 4088 pts/1 Ss Oct23 0:00 \_ /bin/bash
root 2325 0.0 0.3 4592 2660 pts/1 S+ Oct23 0:00 \_ sudo supervise /etc/
init.d/
```

Obtaining Software via the CLI

Earlier in this chapter, you read about using the Ubuntu App Center tool to obtain software. apt is the command-line interface tool that is the equivalent of the App Center. There is another common command-line package manager, named rpm, which is short for Red Hat Package Manager. Despite its name, it is used on more distros than just Red Hat. There is another lesser-used manager called yum, short for Yellowdog Updater Modified, that builds on rpm.

To use apt, start by refreshing the list of available software. The file /etc/apt/sources.list is on systems that use apt. This file lists the software repositories that should be checked for available software. It is common to edit this list to add different sources to get different applications. To update the list of available software from your sources list, you use the command apt followed by the modifier update. Only the first few lines of output are shown in the following example because the complete output may take up a lot of screen space, depending on the number of sources:

```
ubuntu@ubuntu:~$ sudo apt update
Get:1 http://archive.ubuntu.com vivid InRelease [218 kB]
Get:2 http://security.ubuntu.com vivid-security InRelease [64.4 kB]
```

After updating the sources, to install the software, use the apt command followed by install and then the name of the package to install. If, for example, you want to obtain software called screen, which is a tool that enables you to use multiple screens, execute the following command in the CLI:

```
apt install screen
```

It is recommended that you always simulate a software installation first by using the `-s` modifier to make sure the installation will not affect something important on the system. Here is an example:

```
chris@ubuntunVM-2:~$ sudo apt install screen -s
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Suggested packages:
  byobu | screenie | iselect ncurses-term
The following NEW packages will be installed:
  screen
0 upgraded, 1 newly installed, 0 to remove and 68 not upgraded.
Inst screen (4.9.1-1build1 Ubuntu:24.04/noble [amd64])
Conf screen (4.9.1-1build1 Ubuntu:24.04/noble [amd64])
```

This `-s` flag provides a simulation of the output that would appear during an installation without actually installing the package. Once you determine that the installation would be successful, you can rerun the command without the `-s` modifier to install the software.

TECH TIP

Always pre-download packages

When working with systems that need high uptime, it is always advisable to pre-download the packages you plan to install ahead of time to avoid downtime while waiting for a download to occur. This can be done by running the `apt install` command with the `-d` flag.

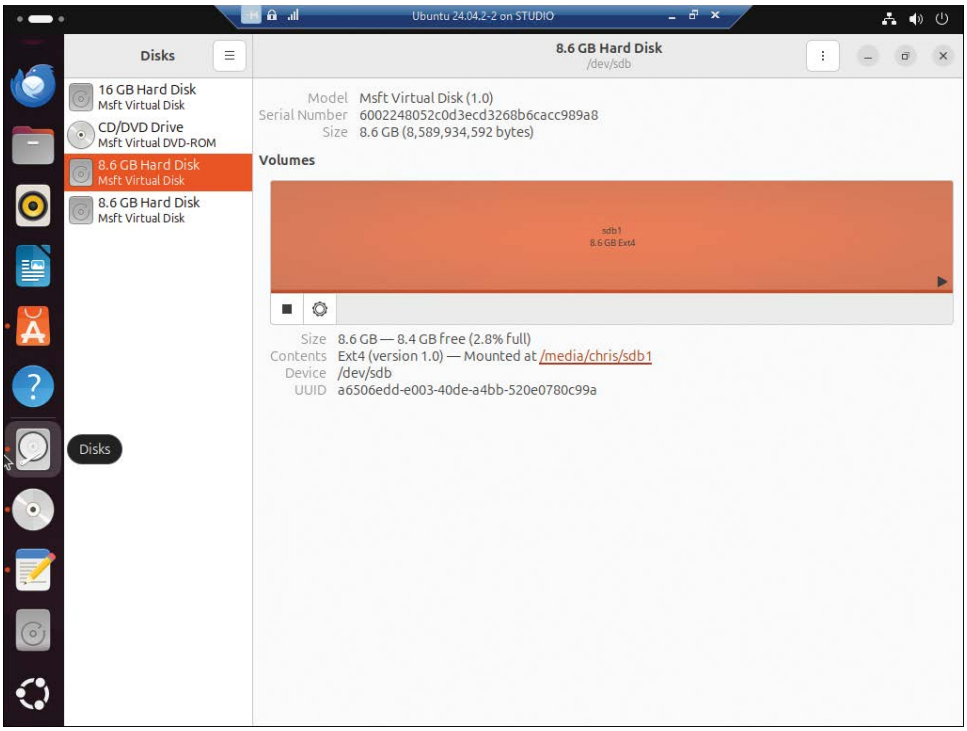
Copying Data

The command `dd` is a versatile command you can use to copy and convert data. Some common uses include copying the contents of a CD/DVD to an ISO file, cloning a partition to another one, creating a backup, erasing a disk, converting a file or its content, and benchmarking. The general syntax is the command `dd`, followed by the input file and then the output file. You can also use many other modifiers, such as `conv` for conversions, `bs` for maximum byte per read or write, and `count` for the number of blocks to copy.

We'll use Figure 17.21 to show the capabilities of `dd` in an environment with two partitions, `sdb1` and `sdb2`. The partitions were created using the application Disks. The two partitions are equal in capacity and are virtually empty. The partitions are mounted at `/media/chris/sdb1` and `/media/chris/sdb2`.

To copy the contents of a DVD onto `/dev/sdb`, the syntax is `dd` followed by the input file (the DVD) and the output file, which is `/media/chris/sdb1/test.iso`. Here is an example:

```
chris@ubuntunVM-2:/$ sudo dd if=/dev/sr0 of=/media/chris/sdb1/test.iso
6599744+0 records in
6599744+0 records out
3379068928 bytes (3.4 GB, 3.1 GiB) copied, 19.5607 s, 173 MB/s
```



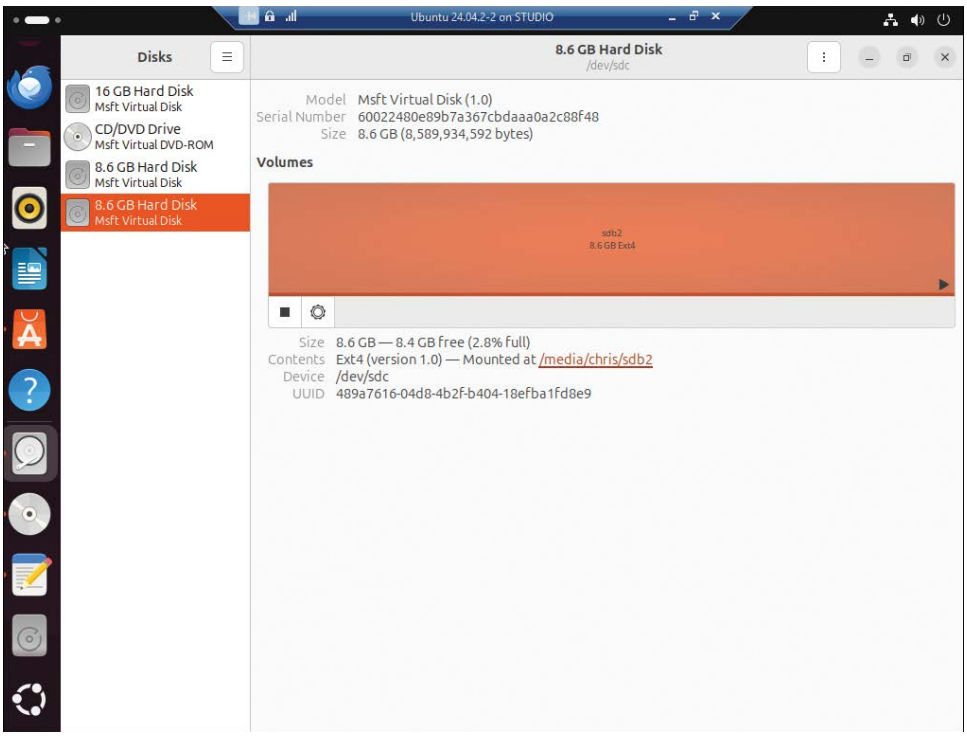


FIGURE 17.21 Disk partitions in Disks

The output in this example shows 3.4 GB of data copied (the size of the data on the DVD). It took 19.6 seconds, and it copied at 173 MB/s. As shown in Figure 17.22, the `sdb1` partition now has more space used.

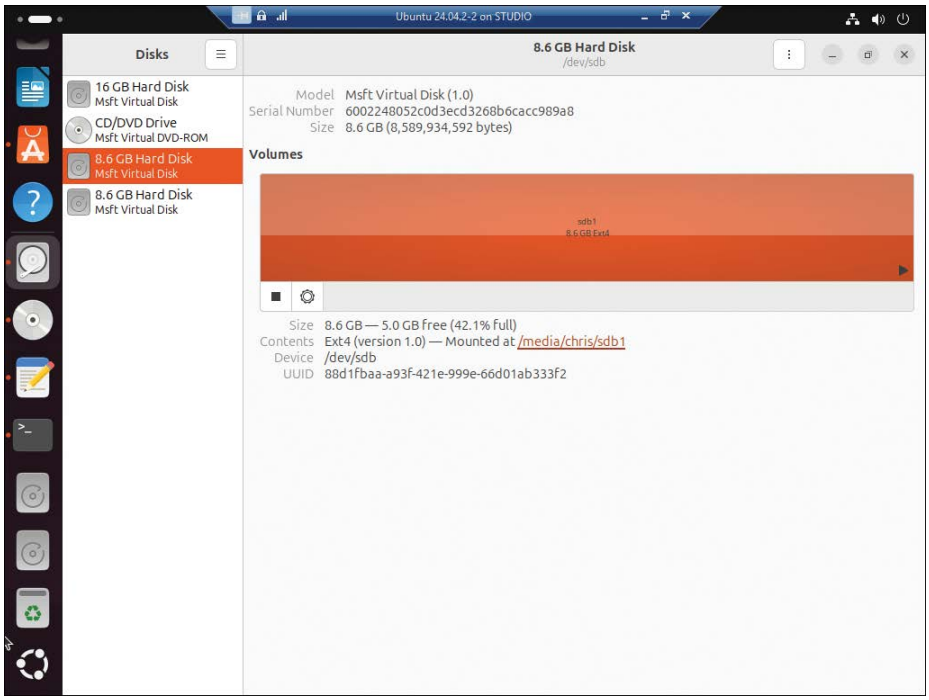


FIGURE 17.22 DVD copied onto the sdb1 partition

Now we can use `dd` to clone `sdb1` to `sdb2`. The syntax is virtually the same as before; the only difference is that when you copy one partition to another partition, you use the full device name of the partition rather than the folder to which it is mounted. The following example shows this command and its output, and Figure 17.23 shows the results in Disks:

```
chris@ubuntunVM-2:/$ sudo dd if=/dev/sdb1 of=/dev/sdb2
16777216+0 records in
16777216+0 records out
8589934592 bytes (8.6 GB, 8.0 GiB) copied, 201.014 s, 42.7 MB/s
```

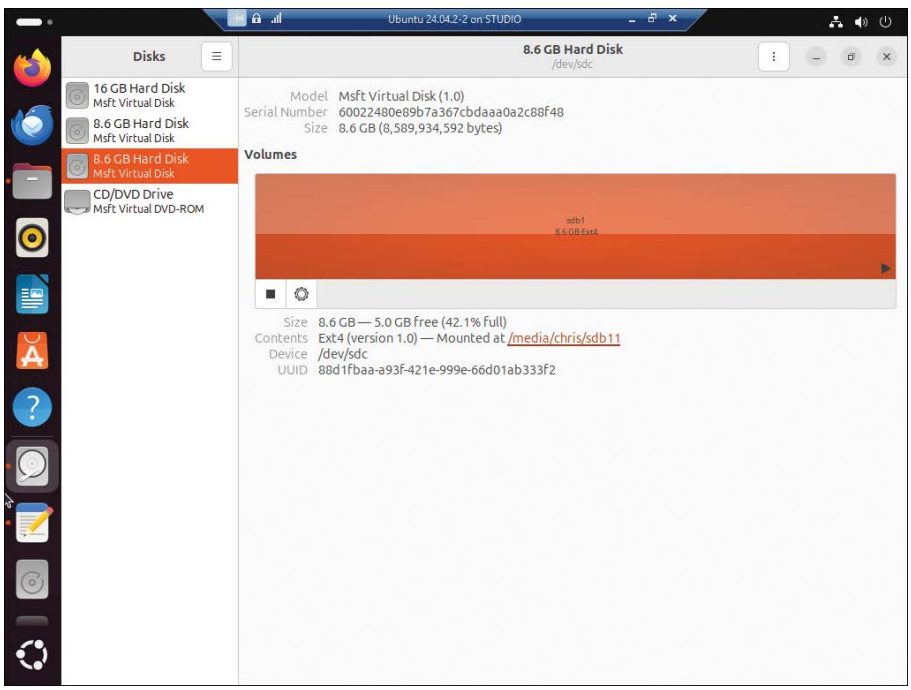


FIGURE 17.23 Cloned partition in Disks

Figure 17.23 shows that you can verify in Disks that the dd command cloned sdb1 to sdb2. They are exact clones. Comparing Figure 17.23 to Figure 17.22, notice that even the device label copied over to sdb2. Also, both partitions now use the same amount of disk space. Note that sdb2 was remounted to /media/chris/sdb11. Both mounted partitions contain the same file: the ISO previously created. The following example shows this command and its output:

```
chris@ubuntunVM-2:~$ ls -l /media/chris/sdb1
total 3299892
drwx------ 2 root root      16384 Mar 17 16:07 lost+found
-rw-r--r-- 1 root root 3379068928 Mar 17 16:08 test.iso
chris@ubuntunVM-2:~$ ls -l /media/chris/sdb11
total 3299892
drwx------ 2 root root      16384 Mar 17 16:07 lost+found
-rw-r--r-- 1 root root 3379068928 Mar 17 16:08 test.iso
```

In the next example, the dd command is used to convert a file, and the cat command is used to show the content of one or more files:

```
chris@ubuntunVM-2:/media/chris/sdb1$ cat test.txt
test
chris@ubuntunVM-2:/media/chris/sdb1$ sudo dd if=test.txt of=/media/chris/
sdb2/test.txt conv=ucase
0+1 records in
0+1 records out
8 bytes copied, 0.000114985 s, 69.6 kB/s
chris@ubuntunVM-2:/media/chris/sdb1$ cat /media/chris/sdb11/test.txt
TEST
```

A file has been created on the original sdb1 that contains only the word test in all lowercase. This example shows how to use dd to copy the file to sdb2 and the conv option to convert the contents of the file to uppercase characters.

The dd command can also be used to erase the sdb2 partition. One option is to write all zeros to the partition. You do this by using /dev/zero *device*, where *device* is a software device that is used specifically for outputting just zeros. It is used as the input file, into the output of sdb2, using block sizes of 4 kB. This process, shown in the following example, is called *zeroing out a drive*:

```
chris@ubuntunVM-2:/media/chris/sdb1$ sudo dd if=/dev/zero of=/dev/sdc bs=4k
dd: error writing '/dev/sdc': No space left on device
2097153+0 records in
2097152+0 records out
8589934592 bytes (8.6 GB, 8.0 GiB) copied, 21.3557 s, 402 MB/s
```

Zeroing out a device is a secure method of erasing data, as the whole drive is filled with zeros until it runs out of space. This makes typical data recovery methods impossible to use. In Figure 17.24, notice that the sdb2 file system is now labeled "Unknown." This is because Ubuntu cannot find a file system for the device; the partition has been rendered unusable until it is reformatted.

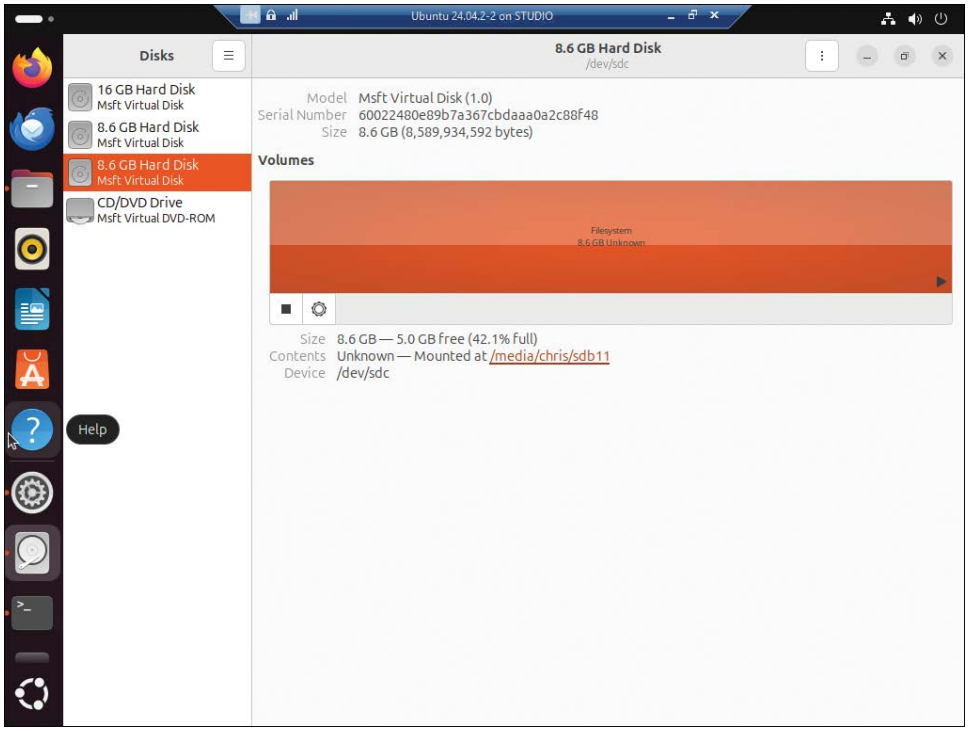


FIGURE 17.24 Unusable partition in Disks

Finding Files

Sometimes when managing a system (especially an unfamiliar system) at the command line, it is difficult to find the locations of files. This is where the commands `updatedb` and `locate` come into use. You can run `updatedb` to update a local system database that contains the full pathname of each file. You can then use the command `locate` to search for a file in this database of paths.

This is a much quicker way to search for a file than searching the system itself, but there are limitations to this search method. The database of paths has to be updated regularly to be accurate. Usually this is done via a task scheduled through the `cron` service. If you are searching for a file that was recently added, you may need to manually run the `updatedb` command to refresh the database. Because this command looks at the entire file system, you need to run it with superuser permissions to ensure that it can read all file paths. Here is an example:

```
ubuntu@ubuntu:~$ sudo updatedb
```

You can now search the system. Say that you need to retrieve an important file called `test-document.txt`, but someone else created it, and they didn't tell you where the file is located. You could use `locate` to find the path to the file, as in this example:

```
ubuntu@ubuntu:~$ locate testdocument.txt
/home/test/testdocument.txt
```

You can see from this example that `testdocument.txt` was left in the `test` user's home directory.

TECH TIP

User forums

A quick internet search is usually enough to find a command to accomplish a task, but some deeper questions might require the advice of those more familiar with using Linux. There are many Linux user forums, and the Ubuntu-specific ones are especially good places for beginners to seek help. The legacy https://ubuntuforums.org forum site has been transitioned to https://discourse.ubuntu.com.

Missing GRUB/LILO

Linux distros typically install one of two bootloaders: Grand Unified Boot Loader (GRUB) or Linux Loader (LILO). LILO is an older and more basic bootloader. It used to be the more predominant bootloader, but it has been discontinued. GRUB is now the default Linux bootloader; the current version is GRUB 2. GRUB supports more modern features, such as network boot and a command-line interface. Usually, you should keep whatever default bootloader your distro comes with unless you need a key feature that only another bootloader offers.

If you have problems booting into a Linux system, there is a chance that the bootloader has been overwritten or corrupted. This problem might happen, for example, if a PC technician decides to install a Windows operating system on the same disk that has Linux installed. The Windows installation could overwrite the Linux bootloader with its own MBR. After that, Linux cannot be loaded because the boot information created by GRUB or LILO no longer exists. To fix this issue, it is necessary to re-create the bootloader for the system by booting to an Ubuntu live CD and running a few commands.

Each missing or corrupted bootloader scenario requires its own unique fix, depending on the partition layout and the operating systems installed. It is important to read the documentation for whichever bootloader you intend to use to make sure you are using a solution that fits the problem.

macOS and Linux Best Practices

Apple macOS and any flavor of Linux, like other operating systems, should be maintained using best practices. Key best practices are as follows:

- **Perform scheduled backups:** Back up the operating system and important data on a regular basis. As an IT staff member, you should gently remind users to do this, too.
- **Schedule disk maintenance:** Mechanical drives become fragmented over time. Although fragmentation does not affect solid-state drives, they can become non-optimal due to blocks of space not being marked "available" for use even though the data in those blocks has been deleted. For best system performance, mechanical drives should be defragmented, and SSDs should be optimized on a regular basis.
- **Perform system updates:** Be sure to install the latest operating system updates to prevent security and performance problems.
- **Perform driver/firmware updates:** Ensure that the latest hardware drivers and firmware updates are installed.
- **Perform patch management:** Follow a structured patch management process to address bugs in operating systems or applications while maintaining system stability. Patch management helps with security issues, too. See Chapter 18, "Computer and Network Security," for more information.
- **Install and update antivirus/anti-malware:** Many people believe that Apple computers and Linux-based computers do not need antivirus or anti-malware software. This is not true. This software should be installed, and it needs to be updated regularly.

SOFT SKILLS: BE HUMBLE

As an IT staff member, you have to be confident that you can repair almost anything and figure things out. However, that confidence sometimes comes across to others as arrogance. Anyone who has worked in IT knows that you cannot know everything. You might know a little bit about a lot of things. You may know a lot about a specific side of IT. But no one can be an expert in it all. Show a little humility and be humble about your knowledge. Do not lord your knowledge and expertise over those you support. Showing empathy for the people you support and interact with goes a long way.

Chapter Summary

- macOS is a Unix-based operating system developed by Apple.
- Open-source software is made freely available and is open for modification.
- macOS can only run on Apple hardware, even in virtual machines.
- The macOS user interface, known as Aqua, contains the Dock, Finder, and menu bar.
- Spotlight can be used to quickly search a macOS system to find files, emails, applications, and even web search results.
- iCloud is Apple's online service that provides online storage and syncing.
- To get the most out of using macOS, end users should have an Apple ID to use with iCloud and the App Store.
- Time Machine is the tool used for automated macOS backups.
- Most system configuration items can be found and managed in the System Settings menu.
- Boot Camp, an application that comes bundled with macOS, guides you through the installation of Windows on a separate partition on a Mac.
- Basic macOS troubleshooting can be done by using the Console and Activity Monitor. The Console allows you to see detailed logs of macOS, applications, and services. Activity Monitor allows you to see what is running on the system and see the resources that the processes are using.
- Keychain Access is a utility in versions of macOS prior to Sequoia for storing passwords, and users tend not to understand it. Be prepared to show users how to update their keychain password when they update their passwords. Starting with macOS Sequoia, Keychain Access only manages security certificates.
- Beginning with macOS Sequoia, the Passwords app securely stores all passwords, passkeys, and verification codes for applications, websites, Wi-Fi networks, and other services.
- System administrators may need to use the Terminal application to access the command-line interface of macOS.
- Linux is an open operating system platform built on the principles of Unix.
- Most Linux administration happens at the command-line level, not in the graphical user interface.
- You must learn the basics of using the command line to properly administer Linux/Unix systems. Be familiar with the commands in Tables 17.4 and 17.7.
- Be prepared to spend many hours researching how to use Linux/Unix systems; it can take years to fully understand how they work and how to properly administer them. If you aren't sure about something, use online resources or ask a colleague to help you understand.

A+ CERTIFICATION EXAM TIPS

- ✓ This chapter and the objectives contained within it account for only a small percentage of the exam.
- ✓ Be familiar with the following Mac features: multiple desktops/Mission Control, Passwords, Spotlight, iCloud, gestures, Finder, the Dock, and Boot Camp.
- ✓ Know the purpose of the shell/Terminal application and review commands such as `su/sudo`, `ls`, `cd`, `shutdown`, `mv`, `cp`, `rm`, `grep`, `pwd`, `passwd`, `chmod`, `chown`, `iwconfig`, `ip`, `ps`, `vi`, `dd`, `kill`, and `apt`. Know that you need to use the `sudo` command to be able to modify settings within the operating system.
- ✓ Know macOS and Linux client best practices, including those related to scheduled backups, scheduled disk maintenance, system updates, App Store for macOS, patch management, driver and firmware updates, and antivirus/anti-malware updates.
- ✓ Be able to use (and know why you would use) the following tools in a macOS or Linux client: Time Machine backups, disk maintenance utilities, the Terminal application/shell, screen sharing, and Force Quit.
- ✓ Know that the Time Machine tool and iCloud can be used to back up/restore Mac images.
- ✓ Be familiar with the file systems associated with macOS and Linux: ext4, HFS+, and APFS.

Key Terms

Activity Monitor, App Store, `apt`, Boot Camp, `cd`, `chmod`, `chown`, command-line interface, Console, `cp`, dash, `dd`, Disk Utility, Dock, ext4, Finder, Force Quit, gestures, `grep`, iCloud, `ip`, `iwconfig`, iWork, kernel, kernel panic, Keychain Access, `kill`, launcher, Launchpad, `less`, Linux, `locate`, `ls`, macOS, `man`, menu bar, Mission Control, `mkdir`, `mv`, `nano`, Nautilus, open source, OS X, `passwd`, pinwheel, POSIX, `ps`, `pwd`, `rm`, root, safe mode (Mac), screen sharing, shell, `shutdown`, Software Updater, Spotlight, `su`, `sudo`, System Information, System Settings, Terminal, Time Machine, `touch`, `updated`, `vi`

Review Questions

1. What are the four main parts of the macOS graphical user interface? (Choose four.)

   [desktop | Finder | Time Machine | Console | Spotlight | Dock | menu bar]

2. [T | F] Ubuntu 24.04 uses the GNOME user interface.

3. In what ways could you quickly launch an application in macOS?

   _____

4. What type of account do you need to create in order to purchase software through the Apple App Store?

   _____

5. Write out the steps you would take to create a file with the Terminal application in macOS or Linux.

   _____

6. What `dd` command would you use to copy the contents of a partition named `/dev/drive1` to another partition, called `/dev/backup`?

   _____

7. What command is used to look for the word mouse in a filename?

   [`sudo` | `apt` | `grep` | `rd`]

8. The _____ command lists the contents of the current directory.

   [`apt` | `grep` | `ls` | `sudo`]

9. Which macOS tool is used to display and modify the main system configuration items?

   [Launchpad | Activity Monitor | Safari | System Settings]

10. How would you create a file from the command-line interface?

    _____

11. What steps would you take to install a new package named `lynx` using the command-line interface in Ubuntu?

    _____

    _____

    _____

    _____

12. If an application is not starting properly on macOS, what steps could you take to resolve this?

    _____

13. If a Mac is running slowly, what utility could you use to identify the cause of the slowdown?

    [Activity Monitor | dash | Launchpad | Mission Control]

14. What is the difference between `passwd` and `pwd`?

    _____

15. How large should a Time Machine backup drive be?

    _____

16. If you wanted to use `chmod` to give read, write, and execute permissions to a file's owner, what command would you use?

    _____

17. Which command grants temporary superuser permissions?

[`ls` | `less` | `root` | `sudo` | `app-get`]

18. [T | F] The `locate` command searches the Linux file system.

_____

19. How would you find out more information about a Linux command?

_____

Exercises

Exercise 17.1 macOS Tools

Objective: To become familiar with macOS tools

Procedure: Match each tool to the correct action.

Tool:	Action:
a. Time Machine	____ Stop a non-responsive application
b. Screen sharing	____ Configure file sharing
c. App Store	____ Get system updates
d. Force Quit	____ Store personal documents on internet servers
e. iCloud	____ Troubleshoot kernel panic
f. System Settings	____ View processes and used system resources
g. Activity Monitor	____ View a remote Mac
h. Console	____ Create a system backup

Exercise 17.2 macOS Commands

Objective: To become familiar with Mac/Linux commands

Procedure: Match each command to the correct action.

Command:

	Action:
a. `cd`	____ Delete a file
b. `rm`	____ Gain root privilege
c. `touch`	____ Move a file
d. `chown`	____ Move to a different directory
e. `mv`	____ Change the owner of a directory
f. `grep`	____ Get help for a particular command
g. `man`	____ Create a file
h. `sudo`	____ Search output for a specific value

Activities

Internet Discovery

Objective: Access the internet to obtain specific information regarding a computer or its associated parts

Parts: Internet access

Procedure: Complete the following procedure and answer the accompanying questions.

1. Search online to find a Linux distro besides Ubuntu. Document the website where you found it and give a brief description of the distro.

   _____

2. What are some of the common business uses of the distro you found?

   _____

3. Research why Linux servers usually do not have a graphical user interface installed. Write down the URL of the website you used to help come to your conclusion and explain your reasoning for not installing a GUI.

   _____

   _____

4. Linux is a stable platform, but it still has issues and can crash. Research to determine what Linux log files are useful for troubleshooting.

   _____

5. Find a website that describes how to troubleshoot a Linux system that will not boot. Write the URL you used and one thing you learned from the site.

   _____

   _____

Soft Skills

Objective: To enhance and fine-tune a future technician's ability to listen, communicate in oral form, work as part of a group on technical problems, and support people who use computers in a professional manner.

Activities: Complete the following questions in a group of three and share your opinions.

1. Write down two things you find confusing about using macOS or Linux and share them with your group. See which areas are the most common problems for everyone.

   _____

2. With your group, do more research on your group's list of the most common confusing items from step 1. As a group, try to come to a better understanding of each issue. For any topics that you cannot get a better grasp on, create a plan to better understand them and describe your plan.

   _____

3. Working with Unix or Linux requires the ability to do independent research to discover and understand new technologies in the field. You need to know how to properly search on the internet to effectively find information, especially when troubleshooting an issue you are unfamiliar with.

   Have everyone in the group search to find the most popular web server application run on Linux. Compare answers to see if everyone got the same results. Also compare what terms each person used to search for the answer. Some searches will be more precise at finding the answer than others. It is important to take a look at how you search to get results as quickly as possible.

   List the most common answer for the most popular web server to run on Linux, as well as the most concise search phrase or term used to find this information.

   _____

   _____

Critical Thinking Skills

Objective: To analyze and evaluate information as well as apply learned information to new or different situations

Activities:

1. You have an Ubuntu user who cannot read a file. What is the first thing you should look at to resolve this? Why?

   _____

2. Write a paragraph explaining why you think businesses prefer to use Linux rather than Windows for server environments.

   _____

3. What would be the drawbacks of using Linux rather than Windows for a server?

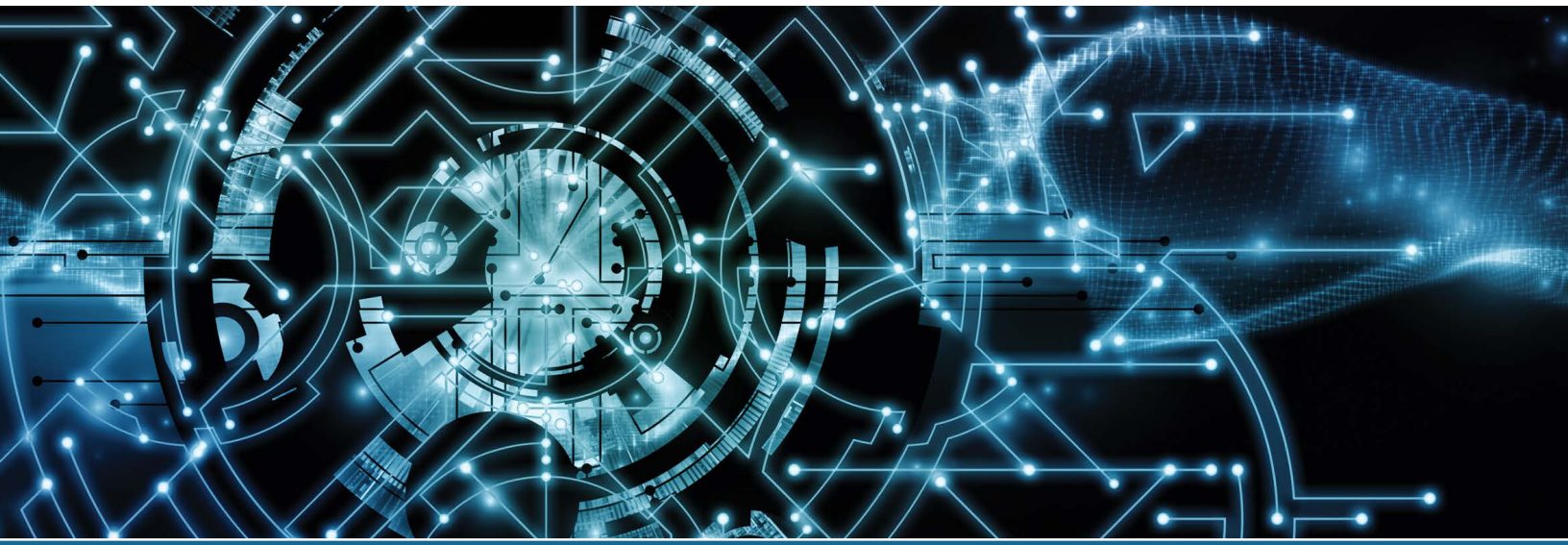
   _____

   _____

   _____

   _____

18 Computer and Network Security



In this chapter you will learn:

- What a company might put in a security policy
- How to perform operating system and data protection
- How to share and protect data
- How to optimize security for Windows
- Methods to use for data destruction and disposal
- How to configure wireless security options
- How to build customer trust

CompTIA Exam Objectives

- ✓ 1201-1.3 Given a scenario, configure basic mobile device network connectivity and application support.
- ✓ 1201-2.3 Summarize services provided by networked hosts.
- ✓ 1201-2.4 Explain common network configuration concepts.
- ✓ 1201-2.5 Compare and contrast common networking hardware devices.
- ✓ 1201-3.5 Given a scenario, install and configure motherboards, central processing units (CPUs), and add-on cards.
- ✓ 1202-1.2 Given a scenario, perform OS installations and upgrades in a diverse OS environment.
- ✓ 1202-1.3 Compare and contrast basic features of Microsoft Windows editions.
- ✓ 1202-1.4 Given a scenario, use Microsoft Windows operating system features and tools.
- ✓ 1202-1.6 Given a scenario, configure Microsoft Windows settings.
- ✓ 1202-1.7 Given a scenario, configure Microsoft Windows networking features on a client/desktop.
- ✓ 1202-2.1 Summarize various security measures and their purposes.
- ✓ 1202-2.2 Given a scenario, configure and apply basic Microsoft Windows OS security settings.
- ✓ 1202-2.3 Compare and contrast wireless security protocols and authentication methods.
- ✓ 1202-2.4 Summarize types of malware and tools/methods for detection, removal, and prevention.
- ✓ 1202-2.5 Compare and contrast common social engineering attacks, threats, and vulnerabilities.
- ✓ 1202-2.6 Given a scenario, implement procedures for basic small office/home office (SOHO) malware removal.
- ✓ 1202-2.7 Given a scenario, apply workstation security options and hardening techniques.

✓ 1202-2.8 Given a scenario, apply common methods for securing mobile devices.

✓ 1202-2.9 Compare and contrast common data destruction and disposal methods.

✓ 1202-2.10 Given a scenario, apply security settings on SOHO wireless and wired networks.

✓ 1202-2.11 Given a scenario, configure relevant security settings in a browser.

✓ 1202-3.4 Given a scenario, troubleshoot common personal computer (PC) security issues.

✓ 1202-4.1 Given a scenario, implement best practices associated with documentation and support systems information management.

✓ 1202-4.3 Given a scenario, implement workstation backup and recovery methods.

✓ 1202-4.6 Explain the importance of prohibited content/activity and privacy, licensing, and policy concepts.

✓ 1202-4.7 Given a scenario, use proper communication techniques and professionalism.

✓ 1202-4.9 Given a scenario, use remote access technologies.

Security Overview

Computer and network security relates to hardware, software, and data protection for PCs and mobile devices. Large books are devoted to this topic. This chapter focuses on issues related to a PC technician's job and the processes and terminology with which a technician should be familiar. Security should be of concern to everyone in a business or a home—including, of course, the technicians who repair and support PCs. A technician must be able to implement and explain security concepts. Another thing to consider is that some industries, such as finance, healthcare, education, and insurance, have specific IT security regulations. Every technician has the responsibility to promote security consciousness and to train users to be good stewards of equipment and data.

Security Policy

Companies struggle with information technology (IT) security as much today as when computers were first used in the corporate environment. Actually, the corporate landscape has become complicated today because people bring their own electronic devices to work. This is commonly referred to as *bring your own device*, or **BYOD**. Management must define and make clear what devices may be put on corporate wired or wireless networks and also what devices are unacceptable, along with the consequences of attaching unapproved devices.

A **security policy** is one or more documents that provide rules and guidelines related to computer and network security. Every company, no matter its size or number of employees, should have a security policy. Small businesses tend to have general operating procedures that are passed verbally from one employee to another, but it is best to have these processes documented in detail. **Non-compliant systems**, or systems that do not meet security policy guidelines, are some of the biggest threats to companies today. Some sectors, such as education, healthcare, and government, require IT security policies.

Common elements of a security policy are listed in Table 18.1.

TABLE 18.1 Security policy elements

Security policy element	Description
Physical access	Describes who is allowed into a building, to what part of the building they have access, and badge/key control. Defines who has keys to the wiring closets and server rooms as well as who is allowed in such places. Delineates what type of security log is kept when a person is allowed access to a space.
Anti-malware	States whether anti-malware software is required on every system, what product is used, how updates are obtained, and steps taken when a machine is not compliant or if a person refuses to comply.

Security policy element	Description
Acceptable use policy (AUP)	Defines who has access to, and what level of usage is appropriate for, company-provided information resources such as email and internet usage. Sometimes, an AUP defines what data can be taken from the company or data storage limitations (for example, "no personal data is to be stored on a server or workstation PC"). A security policy normally includes statements about gaming and web surfing during work hours as well as consequences for violations. The details might include defining what web browser and hardware platforms are supported. It might include the process for assigning folder and file rights and what to do if an account has been disabled.
Password policy	Spells out guidelines for protecting passwords, such as not writing them down, a timeline for changing passwords, the number and types of characters required, and processes for forgotten passwords, such as whether the new password can be given by phone or by email only.
Email usage	Defines who owns email that resides on a company server, how long email is stored, proper usage of email, and when it is backed up. Employees should be aware that their work emails may not be considered private and can be accessed or monitored by the company because the data is stored on company-owned and company-provided servers.
Regulatory compliance	Depending on the industry, a section of the security policy may be devoted to industry-related regulations concerning data, equipment, and security requirements.
Remote access	Contains statements related to who is allowed remote access, the type(s) of remote access permitted, company resources that can be accessed remotely, the process to obtain desired rights and access, and the security level required.
Emergency procedures	Details what to do when something is missing and the steps to take if a natural disaster such as a hurricane occurs. Stipulates who overrides a security policy and authorizes access to someone.

Many corporate security policies are implemented based on user profiles. Within each profile, mandatory requirements such as password length and frequency of password changes are dictated and enforced. The profile also can enforce what network resources a particular user has access to. Even though not every company has a formal security policy, specific points related to a security policy are referenced throughout this chapter. Whether written or just commonly accepted guidelines, many implementations are based on a particular company's rules for computer and network security.

To ease into the topic of security, a good place to start is security methods that might prevent a security breach from occurring in the first place. Four methods of security prevention are physical security, logical security, end-user education, and the principle of least privilege.

Physical Security

Typical physical security includes door locks, cipher locks, **keys**, security guards, **bollards** (upright posts in front of a door, such as those shown in Figure 18.1), and fences, but physical security regarding computers can mean much more. A **door lock** can be a physical lock that requires a key or an electronic one used for equipment such as servers, firewalls, switches, and data storage devices. Even in a locked room, it is important to disable unused ports on devices in case the room is compromised. Companies commonly use electronic key cards instead of keys for physical access to rooms. Electronic key cards (see Figure 18.2) are part of an access control system, which includes the key cards, door readers, and software to control and monitor the system.

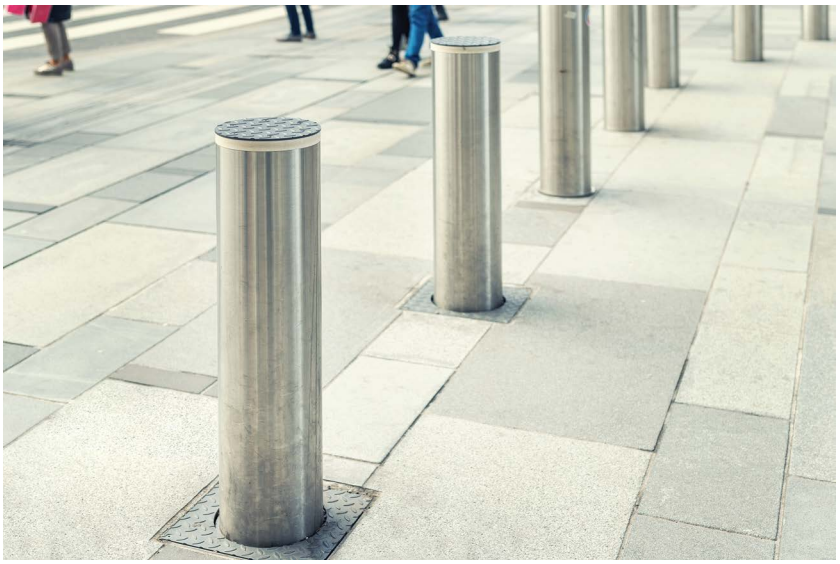


FIGURE 18.1 Bollards

FIGURE 18.2 Electronic key card system

Electronic key cards have many benefits, including the following:

> They are easy to program and issue/revoke compared to issuing a key and getting it back from an employee who quits or is dismissed.
> Data is stored in a database instead of on a checkout form.
> Access to information, such as who entered a room and at what time, can be logged and monitored more easily than with a checkout sheet.
> More layers of control can be exercised with key cards. With metal keys, the usual process is to give a key for each room, issue a key for an entire wing, or issue a key for the entire building.
> When keys are issued and one is lost, the lock must be rekeyed and new keys issued. When an electronic key card is lost, the old card is deactivated, and a new one is issued.

Other electronic devices and technologies also provide access to computers and rooms—in other words, authenticate the user. **Authentication** is the process of determining whether a network device or person has permission to access a network. Table 18.2 lists and describes security devices that help with the physical security of computers.

TABLE 18.2 Physical security devices

Device/ technology	Description
Smart card	A small ID-sized card that can store data, which can be encrypted, and that requires authorization in order to be changed. A smart card can be swiped through a card reader or may interact wirelessly with a card reader. Smart cards are used in government IDs (with information such as medical/dental records), mobile phones (as subscriber ID modules), driver's licenses, and employee badges (see Figure 18.3).
Key fob	A device used for keyless entry to a car, a building, or an interior doors, such as a fitness room in an apartment complex.
Radio frequency ID (**RFID**)	A technology that allows automatic identification of people, objects, or animals in which an RFID tag is read wirelessly by an RFID reader. RFID is used in libraries and inventory systems and is used for computers, hospital equipment, and locating lost pets or people. An RFID badge can be used to access and track access to a locked area.
Badge reader	A device that can be contactless or that may require a swipe or insertion of an identification card to allow entry into a space.
Security guard	A human who provides security by controlling access into a controlled space such as a network closet or server room.
Mobile digital key	A method of allowing physical or digital access using proximity of a mobile device such as a smartphone, tablet, or wearable device. It could also be through an app. Common usage includes cars, hotel rooms, and building access.
Security token	A device—also called an authentication token, USB token, hardware/hard token, or software/soft token—that authorizes access to something. A **hardware token** (see Figure 18.4), for example, is a physical device used to gain access to a resource such as a file or company. Examples of hardware tokens are smart cards and USB security keys.
Lighting	A well-lit area is easier to record and provide better security. Some network equipment areas have automatic lights that trigger camera recording when activated.
Trusted Platform Module (**TPM**)	A microcontroller chip on a motherboard (refer to Figure 3.29 in Chapter 3, "On the Motherboard"), smartphone, or network equipment used for hardware/software authentication. A TPM stores information such as security certificates, passwords, and encryption keys. **Encryption** is the process of converting data into an unreadable format. A TPM can also authenticate hardware devices. Applications can use TPM for file and folder encryption, local passwords, email, VPN/PKI authentication, and wireless authentication.
Hardware security module (**HSM**)	A module that is similar to a TPM except that it is specialized hardware that can be added as a USB device or a device on the network and used for digital key management, storage/protection of cryptographic keys, encryption, and authentication.
Cable lock	A physical lock used with devices in common areas such as libraries or lobby areas. Also used to secure laptops. Refer to Figure 10.64 in Chapter 10, "Mobile Devices."
Equipment lock	A physical or electronic lock on a cabinet that can provide monitoring and security for individual cabinet doors. It might also include a special cable attached to a device that cannot be removed without a specialized tool.
USB lock	A device that prevents USB storage devices from being used in USB ports in order to prevent the movement, transfer, and copying of files. A USB lock may be implemented in addition to disabling ports in BIOS/UEFI BIOS.

Device/ technology	Description
Access control vestibule	An area, also known as a mantrap or an air lock, that separates a nonsecure area from a secured area (see Figure 18.5). An access control vestibule is useful in preventing unauthorized access and **tailgating** (in which an unauthorized person enters directly behind an authorized person).
Privacy screen	A device, also called a privacy filter, that prevents **shoulder surfing**, in which someone looks over a user's shoulder to gain information by looking at the person's screen. A privacy screen allows a user to view the screen clearly only if when sitting directly in front of the monitor (see Figure 18.6).
Video surveillance	The use of wired or wireless security cameras for equipment and personnel safety as well as data in the event of a security breach.
Alarm system/ motion sensor	A system that can send out an audible or silent alarm that triggers video or calls to security, police, or fire.
Magnetometer	A device that is used to scan for firearms and weapons and that might also be used in location tracking.

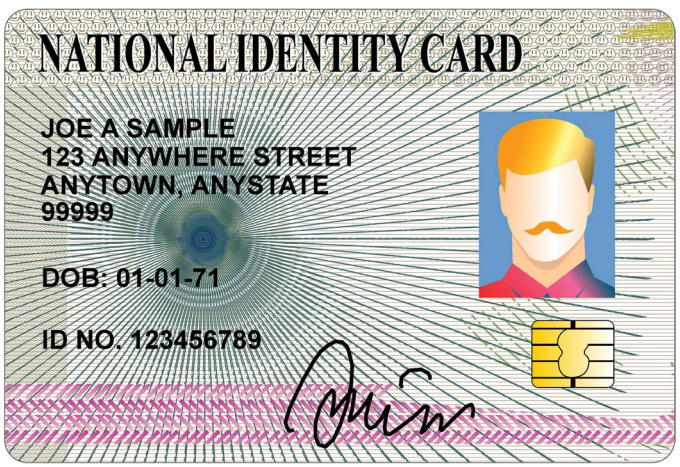


FIGURE 18.3 Smart card

FIGURE 18.4 Hardware token

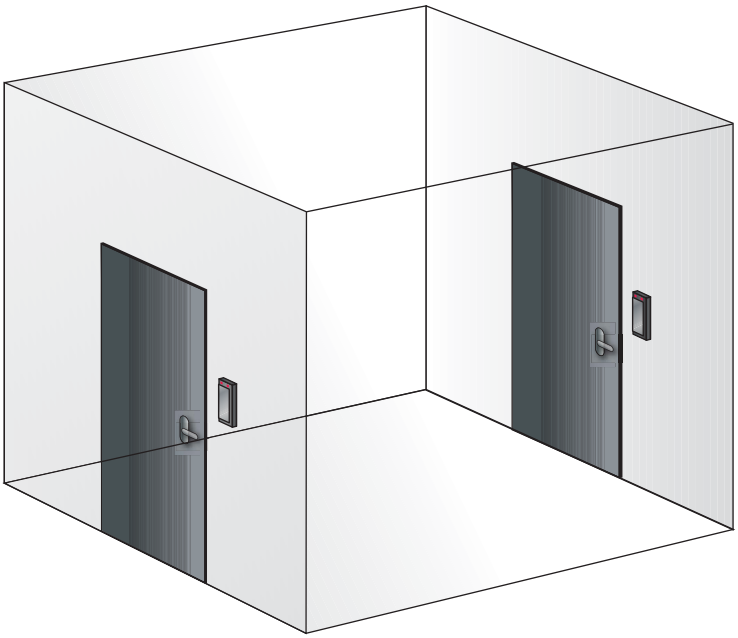


FIGURE 18.5 Access control vestibule (mantrap)

FIGURE 18.6 Shoulder surfing

Biometrics

An expanding field related to authentication that is used in multifactor authentication is **biometrics**, which is authentication based on one or more physical traits, such as a fingerprint, an eyeball (retina), or a hand. Behavioral traits, such as voice, common web surfing, or purchase habits, can also be used. Voice can actually be both physical and behavioral. A less complex system might compare voice with a stored voice print. A more complex system might compare tone and inflection, too, which are more in the behavioral realm.

Biometrics provide extra security because a biometric system is more difficult to bypass than are a user ID and password. The trait is less likely to be lost than a password. Also, biometrics require that the person being authenticated be present in order to gain access. Implementing biometrics is more expensive than implementing a user ID/password scheme.

Table 18.3 lists examples of biometric devices used to allow someone to gain access to a room, locker, or device.

TABLE 18.3 Biometric devices

Device	Description
Fingerprint scanner	Requires a finger to be placed on a reader (see Figure 18.7) and compared against a stored image. Used in laptops with some vendors having these devices already installed.
Facial recognition technology (FRT)	Commonly used with laptop webcams. Another system takes a photo and compares it with an image database (though this process is resource intensive) (see Figure 18.8).
Palm print scanner	Requires a palm of the hand to be placed against a reader and is more secure than a fingerprint reader. Higher-end systems can analyze veins in the palm.
Retinal scanner	Sometimes called an eye scanner and closely related to an iris scanner. According to LG Electronics, the iris is the most distinguishable human characteristic.
Voice recognition technology	Involves a person speaking into a microphone in order to gain access to a computer or physical space. Also called speech recognition but not the same as the software used to input data in lieu of typing.

FIGURE 18.7 Fingerprint scanner

Applications for biometric devices are not limited to computer/network security. Disney World uses biometrics to ensure that the same person uses a multiday pass. Airports use biometrics for access to employee-only areas. Police departments use biometrics to gain access to evidence and gun lockers. Biometric devices need to be installed and maintained by computer and network support staff.

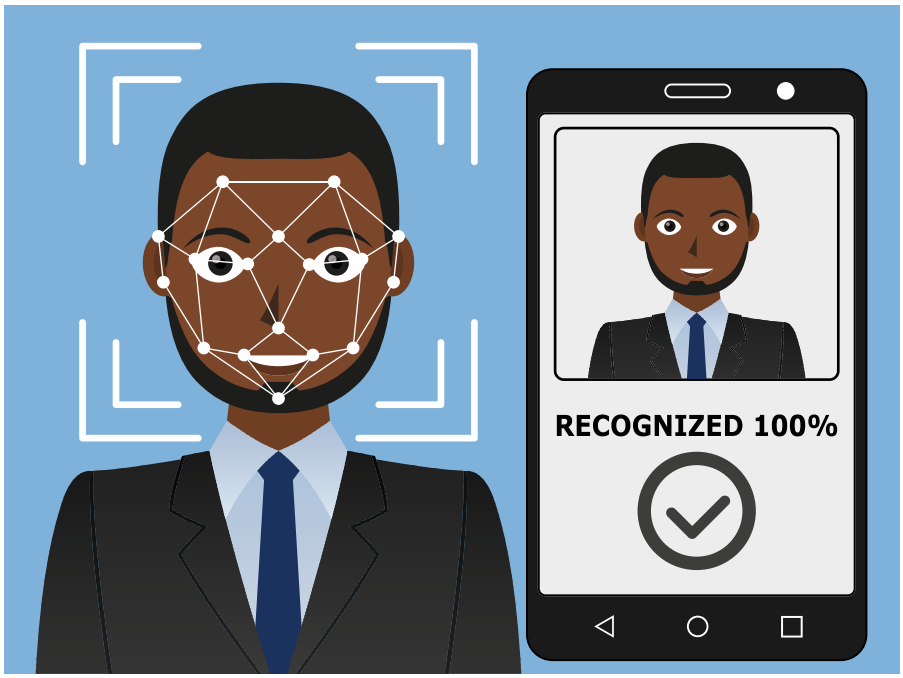


FIGURE 18.8 Facial recognition

You might be required to use the system UEFI/BIOS Setup program to activate an integrated biometric device. To use a biometric device, optionally download a driver, install it, and use a specific application that is available for download, that comes with the device or computer, or that is preinstalled on the computer.

Document Disposal/Security

Some computer data must be printed as part of normal business operations. Some of this printed material must be kept in a locked environment (such as a safe or file cabinet). When others who do not have a "need to know" are in the room, it is important to turn the printed material over or, better yet, put it inside a folder. When the material is no longer needed, it can be shredded by a shredding service or using a shredder in the office. An outside company, known as a **third-party vendor**, should provide a **certificate of destruction**, proof of **incineration** (destruction by fire), or proof of **recycling**. Recycling of corporate printouts tend to be done by professional shredding services.

Shredders are available for reasonable prices, but they are not the best option in a corporate environment because shredded paper from most models can still be reconstructed. Professional shredding services tend to use shredders that can do either cross-cut shredding (bidirectional shredding) or micro-cut shredding (with small irregular shaped cuts). For day-to-day business and personal documents, **shredding** is still a good practice to keep other people from taking documents out of trash bins (**dumpster diving**) and using the information for some malicious intent (see Figure 18.9).

Some industries have regulations regarding document disposal. For example, the Family Educational Rights and Privacy Act (FERPA) protects student records. Some states require that educational organizations shred any document that uniquely identifies a student. Medical and tax records must also be disposed of properly. The Federal Trade Commission Act (FACTA) requires businesses to have defined procedures for how documents containing consumer information are handled and disposed. There are also laws that make it illegal to destroy specific types of corporate documents and communications. No matter the area of IT you are in, it is important to know the laws regarding the industry you support.

FIGURE 18.9 Retrieving shredded documents

Logical Security

Logical security involves protection through the use of software. A number of types of devices and techniques can help in this area. The types of logical security prevention methods on the CompTIA A+ certification exam are briefly outlined here, and some of them are explained in more detail later in the chapter:

- **Antivirus/anti-malware:** **Antivirus/anti-malware** software is used to protect the operating system and applications from small programs that wreak havoc on the system, even causing it not to work at all. It is best to just have one anti-malware app installed as these programs do not work well together and cause the system to run slowly.
- **Firewall:** A **software firewall** is a tool provided with a device or an application that can be configured on a PC, a router, an access point, and so on. A **firewall** can also be a hardware device that protects an organization. A company may have more than one firewall, depending on the network design (see Figure 18.10).
- **Zero Trust model:** A **Zero Trust model** is a method of IT design that says nothing/no one is trusted by default, and everything/everyone is verified. Everything in the network, in the firewall, in data storage/access, in app access, in software-defined networking, in cloud usage, and so on is compartmentalized and protected. Policies define who or what gains access to a particular area. Imagine that each IT compartment in a company is a door. The door opens only for predetermined reasons and when the right credentials are provided. When a breach occurs, it is isolated to that one compartment.
- **Identity access management:** An **identity access management** framework focuses on identity management and access management. Identity management involves a database of user information that might include more than just a username and password, such as title, phone numbers, manager, and subordinates. Access management involves rules for determining the resources someone or some app or code is allowed to access.
- **Directory services:** **Directory services** involve a database of users, devices, apps, usernames, and passwords that are used to verify users and manage access privileges. Directory services platforms include Microsoft Active Directory, AWS Directory Service, Azure Active Directory, Open Directory, eDirectory, Google Workspace, Okta, and Free IPA.

FIGURE 18.10 Corporate firewall design

- **Principle of least privilege:** According to the **principle of least privilege**, the maximum rights given to a resource are limited to the only the rights needed to do the job.
- **Virtual private network (VPN):** A **VPN** enables secure connectivity across an unsecure network such as the internet to a remote location; an example of someone who would need to use a VPN is a mobile user who must connect to the corporate network to upload data weekly or to access corporate data stored in folders on a server. See the section "VPN Configuration," later in this chapter, for more information on how to configure a VPN.
- **Disabling unused ports:** In highly sensitive areas, ports such as Ethernet, USB, eSATA, and Thunderbolt ports may be disabled so that an external device cannot be attached to gain access to sensitive corporate or government data. It is also important to disable unused ports on routers, switches, and firewalls.
- **Access control list (ACL):** An **ACL** is a set of security rules that permit or deny the types of traffic flowing into a device, out of a device, or toward a particular network or that specify the type of traffic, such as HTTP or HTTPS packets.
- **Port security:** When people bring their own devices to work, they sometimes attach those devices to the physical network. Port security is used on a corporate switch to allow only a device with a particular MAC address to attach. Whenever someone unplugs the specified device and attaches a different one, port security settings shut down the switch or firewall port because a device with a different MAC address has been attached.
- **Trusted sources vs. untrusted sources:** Windows and mobile device users commonly have security software that tells them whether a website or a downloaded file is a **trusted source** or an **untrusted source**. Linux repositories of open source software exist. Linux users should be cautious about downloading software from unknown developers who do not make their source code public. All users, no matter the operating system, should be aware of untrusted software sources when downloading files.

Let's dive a little more deeply into some of these security items.

Authentication

Authentication involves proving who a particular person or device is by using something someone has, something a person knows, something a person is, or somewhere a person is located. For example, when you are logging into your bank account, you might have a short message service (**SMS**) text message sent to you that has a code that you enter, or you might get a voice call or an email that gives you that authentication code. This is known as **multifactor authentication (MFA)**. As shown in Figure 18.11, this type of authentication requires some combination of something you have (such as your ATM card, your current location, or a security token device), something you are (a fingerprint or another biometric reading), and something you know (such as a PIN) in order to gain access to something such as a room, a bank account, a shared folder, or data stored in the cloud. MFA is more secure than single-factor authentication, which uses only one means of authentication, such as a username and password combination. Table 18.4 lists and describes terms that are related to authentication.

FIGURE 18.11 Multifactor authentication

TABLE 18.4 Authentication concepts

Option	Description
Soft token	A code generated through software. It could be a code provided through a text message, an email, or a phone call.
Authenticator application	An application that provides a one-time password that comes from a previously configured website and is used in addition to the commonly required user ID and password.
Single sign-on (SSO)	A technology that enables a user to authenticate to multiple systems/servers, printers/copiers, and networked-based applications with a minimum of a user ID and password.
Identity synchronization	A method commonly used with corporate customer relationship management (CRM) and enterprise resource planning (ERP) platforms that allows single sign-on for access to multiple areas. It is also used when different directory systems are used, such as Microsoft Active Directory and a cloud-based platform hosted on Azure.
One-time password/passcode (OTP)	A security method in which a code that is sent via SMS text or email can be used to authenticate for access to a site or a transaction.
Time-based one-time password (TOTP)	A security measure used to provide a code to someone via text, voice call, or email that has a time limit applied.

Option	Description
Just-in-time (JIT) **access**	Part of a security process called **privileged access management** (PAM) in which a person is allowed access to a system, a device, or an app to do something specific, and then those rights are revoked. For example, a data analyst who prepares financial reports might be given access to data for a period of time so the reports can be generated.
Security Assertion Markup Language (**SAML**)	A security standard that allows someone to have access to more than one app with a single logon (such as with Microsoft Office 365).
Remote Authentication Dial-in User Service (**RADIUS**)	A network security protocol that is used to centralize authentication, authorization, and accounting (AAA). A RADIUS server can provide a way to authenticate wired and wireless users as well as devices before they are allowed to communicate on the network.
Terminal Access Controller Access-Control System (**TACACS+**)	A network security protocol that supports AAA and makes it possible to separate the pieces of AAA so you don't have to do all three on the same server. For example, you could do authentication on a different server but still support authorization and accounting on a TACACS+ server.
Kerberos	A security protocol for secure authentication. It can be used in conjunction with an authentication server or when accessing services such as SSH, POP, or SMTP.

Technicians commonly have to deal with **authentication failures** where someone cannot log in to a network. Of course, these failures can be caused by typos in the username and password, but the problem may also be related to the following:

> **Authentication server:** Check whether others can log in to the network.
> **Network path:** Check the network path from the initial device to the authentication server.
> **Misconfigured permissions/username:** If this is the first time the user is attempting a login, the user ID/password may not be configured yet or may have been entered incorrectly.

BIOS/UEFI

Most computers have BIOS/UEFI options that prevent others from altering the settings. A BIOS/UEFI password can also be assigned to require a password before the operating system loads. Table 18.5 shows some BIOS/UEFI options related to security.

TABLE 18.5 BIOS/UEFI security options

Option	Description
Supervisor/ administrator	Allows unrestricted access to all BIOS/UEFI options.
User	Enables a limited number of configuration changes, such as changes to time and boot sequence.
Trusted Platform Module (TPM)	Allows initialization and viewing of a password for the TPM motherboard chip that generates and stores cryptographic keys.
LoJack	Locates a mobile device and displays a message on the lost device.
Secure boot	Prevents an unauthorized operating system from loading.
Boot password or power-on password	Required before BIOS/UEFI looks for an operating system. This is not the Windows user password.

In a corporate environment, the supervisor password is commonly applied. Other options that may affect the corporate environment include the following:

- Enabling/disabling device options
- Enabling/disabling ports
- Encrypting a drive
- Enabling TPM
- Enabling LoJack
- Viewing/changing security levels/passwords
- Restoring security settings to the default values

Laptops, netbooks, Chromebooks, and ultrabooks sometimes have an additional password for their internal storage drive. That way, if the device is stolen, the hard drive cannot be inserted into another device and used without the hard drive password. This password is in addition to the power-on password or Windows password. If this option is available, it is configured through the BIOS/UEFI.

Login OS Security Options

Getting into any device usually requires some form of login or authentication, as already discussed. Here are some common login options used by devices today:

- With a **username and password**, a name associated with a person is stored on the local computer or on an authentication server along with a unique password used for access.
- A personal identification number (**PIN**) is a unique set of numbers defined by the user as a quick means to access a computer such as a home computer.
- A fingerprint is commonly used on a mobile device.
- Facial recognition is one of the most secure methods available.
- **Windows Hello** is a Windows 10/11 **passwordless** option that allows you to use a face, fingerprint, PIN, security key, password, or picture password to gain access.

Table 18.6 lists some guidelines for passwords.

TABLE 18.6 Computer/network password guidelines

Guideline	Description
Reminders	Do not write down passwords. Many computer users write down their passwords and keep them close to the computer. Do not put your passwords in a document stored on the same computer. Passwords can be kept digitally through an app or an encrypted file.
Number of characters/ complexity	Passwords can use uppercase letters, lowercase letters, numbers, and special characters like @, ~, !, #, %, &, (, _, and -. Many companies now require a passphrase with a large number of characters that includes special characters and numerals.
Uniqueness	A security best practice is to not reuse a password and not use a normal word. A passphrase that has letters changed to numbers or characters is the best format for a password.
Format	Do not use consecutive letters or numbers on the keyboard, such as *asd* or *123* because doing so makes it easy for someone who is watching to guess the password. Do not use passwords that are words such as *children* or *happiness* because password-cracking programs use **dictionary attacks** to hack passwords. The dictionaries used in these attacks even include foreign words and names.

Guideline	Description
Expiration	On servers, this is known as the minimum password age and the maximum password age. The minimum password age is how long a user must keep a password before changing it. Microsoft recommends 3 to 7 days. The maximum is the amount of time before the user is required to change it. Common values are 30, 60, and 90 days.
Log off when not in use	Use a screen saver or lock the computer with the ⊞+L key combination. Use the *Personalization* Settings link to configure the screen saver and require login credentials to re-access the computer. This is especially important for a private PC in a public or visible area.
Failed attempts	A common setting for the number of times a person is allowed to try a password that is wrong before being locked out is three failed attempts.
Social	People's eyes tend to stray toward movement. If someone is standing near enough to you that they could be shoulder surfing when you log in, ensure that the person's eyes are averted or wait until the person moves away before you type your password into the system. Obtain a privacy filter.

Different password requirements, user IDs, and passwords cause stress for many people. Research is ongoing into the effectiveness of requiring frequent password changes since many people write down their passwords, use weak passwords, or use passwords that are easily modified. One solution people are turning to is using a **password manager**, which is an application on a computer or a USB drive, a mobile app, or a web browser plug-in that locally or remotely stores passwords used to access accounts. When stored remotely, the passwords and associated data (site, device, and so on) should be encrypted.

Considering the End User

End-user education is a great way to prevent security events and issues. Technical staff frequently forget this step because they would rather deal with technology than the people who operate and access the devices. New hires should be presented with the acceptable use policy (AUP) during the onboarding process. Some companies present this policy, described earlier in this chapter, every time a user logs in to the network. Users should be reminded that every employee is required to follow corporate end-user policies and apply security best practices with every device used to perform business tasks. Companies also might require annual security training for all employees to update them on common threats.

Some industries or situations require an employee to sign a non-disclosure agreement (**NDA**), which stipulates that information will not be shared. An NDA might be used, for example, for new product development, with negotiations with a potential technology partner or vendor, with a corporate merger, or when customer data is involved. With a mutual non-disclosure agreement (**MNDA**), both sides sign the document.

Remind users that everyone is inconvenienced by good security practices that are time-consuming and may sometimes even seem meaningless (until a security event occurs!). People tend to take shortcuts, and humans are the weakest security link. Technicians must take care to not record users' personally identifiable information (PII) or passwords and to remind users to secure their passwords and any printed material if they leave the area. Users should be reminded that if their computer is remotely accessed by a technician, they should close windows that contain corporate or personal information prior to agreeing to a remote connection. Corporate mobile devices must be kept secure and protected. Any time a technician removes a virus or malware from

a user device, training should be part of solving the problem. Violations of security best practices are a common security threat and make a company more vulnerable to other security problems. Let's explore some of the common areas that apply to users.

Licensing

An ethical problem technicians often face is being asked to install software or other content that is not legitimate. Digital rights management (**DRM**) involves the use of the technology used to implement controls placed on digital media (software, hardware, songs, videos, and more). Users often request that technicians share with them methods to break copyright laws or work around copy protection controls. Technicians must maintain their professionalism and ethics to ensure that corporate interests are protected. Instances like these provide great opportunities to talk to users about different software sources:

- **Open source:** **Open source** software is software for which the original software code is provided.
- **Freeware:** This software doesn't cost anything but could include some harmful software.
- **Shareware:** This software might be free at first but may require later payment; it may include only part of a particular software package with the option to buy the rest.
- **Corporate use license:** With a corporate use license, software is purchased for a specific number of users and/or machines. Even when commercial licensing is obtained, there is an end-user licensing agreement (**EULA**) that specifies what can be done with a particular license.
- **Personal license:** With a personal license, software is purchased for a specific number of users and/or machines, commonly for home or small business environments. This license is covered by a EULA.
- **Valid license:** A purchased/legal license for an app or software for a specific machine.
- **Perpetual license:** A perpetual license applies to software that is still updated and supported by the originating company.

Studies have found that more than one-third of PC software does not have a legitimate license. **Piracy** (see Figure 18.12) is defined as follows:

- Copying or distribution of copyrighted software that is not authorized
- Purchasing a copy of a particular application or software and putting it on more than one computer
- Installing, sharing, selling, copying, downloading, or uploading stolen software to another site
- Installing company software on or permitting access to unauthorized devices

Software companies have different pricing structures for individual or personal licenses and corporate or enterprise licenses. An enterprise license gives a company permission to load the software on an unlimited or maximum number of devices. A personal license is more limiting (usually to one device).

People use software piracy websites to obtain illegal software. These sites are riddled with security threats that are downloaded along with the desired software. The current penalty in the United States for software piracy is $150,000 per program copied. If prosecuted for copyright infringement, fines can be up to $250,000 and/or up to five years in jail. Don't be persuaded to risk your personal life and professional future for software piracy.

FIGURE 18.12 Software pirate

Regulated Data

As ever-increasing computing power has made the mining, collection, and storage of private data more efficient and invasive, so too have the world's standards for privacy protection increased. Inadvertently disclosing regulated data embarrasses you and your employer, and it could subject you both to civil and/or criminal penalties.

Regulated data is defined by federal law or regulation according to its purpose, such as in the areas of education, healthcare, financial institutions, arms trafficking, exports administration, and online privacy of children. There are four specific types of regulated data:

- **PII:** Personally identifiable information
- **PCI:** Payment Card Industry information
- **GDPR:** Information that is subject to the European General Data Protection Regulation
- **PHI:** Protected health information

Personally identifiable information (**PII**) is information that uniquely identifies someone, such as a Social Security number, an employee ID, a patient number, a passport number, or a user ID. Any type of personal government-issued information is protected. It is important to stress to users that they should not have such information visible in the work environment except where needed. There are two broad types of PII: nonsensitive and sensitive. Nonsensitive PII is information that can be found publicly, such as a person's name, telephone number, and email address. Nonsensitive information can be transmitted unencrypted (unscrambled and with no security) without causing harm to an individual. Sensitive PII should be encrypted if it is transmitted or stored.

All members of the credit card/debit card industry, such as financial institutions, credit card companies, and merchant services must comply with standards related to Payment Card Industry (**PCI**) information. The Payment Card Industry Data Security Standard (PCI DSS) was developed to encourage and enhance the security of personally identifiable information and payment data. As a technician, you may have exposure to PII and PCI (PCI-2) data that must be kept on a separate network than other types of data. You are obligated to protect the privacy of this data.

The General Data Protection Regulation (**GDPR**) was adopted in 2016 by the European Union (EU). The GDPR unifies protection for the personal data of EU residents, including U.S. expatriates, and sets forth restrictions on processing and transferring personal data outside the EU. Any entity that offers goods or services to, or monitors the behavior of residents in the EU, must comply with the GDPR. For example, an American business selling products to an EU resident would be subject to the GDPR. Violations of GDPR provisions subject organizations to financial penalties of up to 4% of the organization's global annual turnover.

The Health Insurance Portability and Accountability Act (HIPAA) of 1996 required the U.S. Department of Health and Human Services (HHS) to develop privacy and security regulations for certain health information. HHS developed the HIPAA Privacy Rule, which defines protected health information (**PHI**) as "individually identifiable health information," including demographic data, that relates to an individual's past, present, or future physical or mental health or condition; the provision of health care to the individual; past, present, or future payment for providing health care; and the individual's identity. Common identifiers are name, Social Security number, birth date, and address. Each state in the United States has laws regarding how long medical records are to be kept, but the HIPAA rules do state that privacy-related documents like notices of privacy practice, PHI logs, and IT security reviews must be retained for at least six years.

Security Threats and Vulnerabilities

A number of types of security threats and vulnerabilities exist. Many of them fall into multiple categories because there might be multiple threats. They all do bad and weird things to devices. Malware is a good place to start.

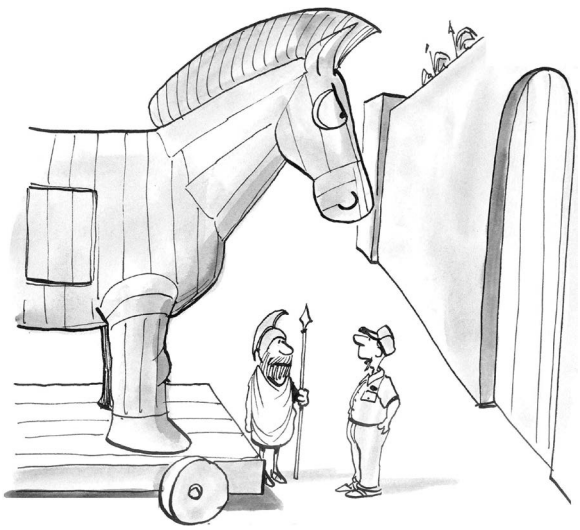
Malware

Malware is software code that is designed to damage a computer system (causing lockups, slowness, applications crashing or failing to run or running incorrectly, operating system update failures, random and frequent browser pop-ups, and so on). In most cases, allowing more users to bring their own devices to work increases the risk of introducing malware into the network. Table 18.7 lists common types of malware.

TABLE 18.7 Types of malware

Type	Description
Spyware	Collects personal information without consent through logging keystrokes, accessing saved documents, and recording internet browsing. Results in unsolicited pop-ups and identity theft.
Virus	Does something harmful to a computer (for example, displays a message, prevents the computer from booting, makes the computer run slowly, changes file or application permissions, or logs keystrokes). A virus commonly attaches to an installed program.
Boot sector virus	Installs into a storage device's boot sector code that is used to boot the computer and can spread to drives and other network devices.
Trojan	Disguises itself as a legitimate program to gain unauthorized access to a device. Also known as a Trojan horse (see Figure 18.13).
Rootkit	Gains administrator access (known as root access in Linux) to the operating system. It is important to check for unknown processes running to see if a rootkit is installed.
Ransomware	Restricts access to a device until a user pays money to regain access.

Type	Description
Keylogger	Records every keystroke entered in an attempt to collect user IDs and passwords.
Botnet	Software that spreads from hacked device to hacked device and that is under control of someone else. Bots are used to infect other computers (see Figure 18.14).
Cryptojacking	Embedded malicious code that acts as a **cryptominer**, using a computer's processing power to do cryptomining of digital currencies like bitcoin.
Stalkerware	Software used to track or monitor someone.
Fileless	Malware that is not stored on a storage device but is only in RAM, making it hard for traditional anti-malware software to detect. It is planted through the use of PowerShell or by editing the registry.



"Sure, bring her in. I've always wanted to work on one of these babies."

FIGURE 18.13 Trojan malware (disguising itself)

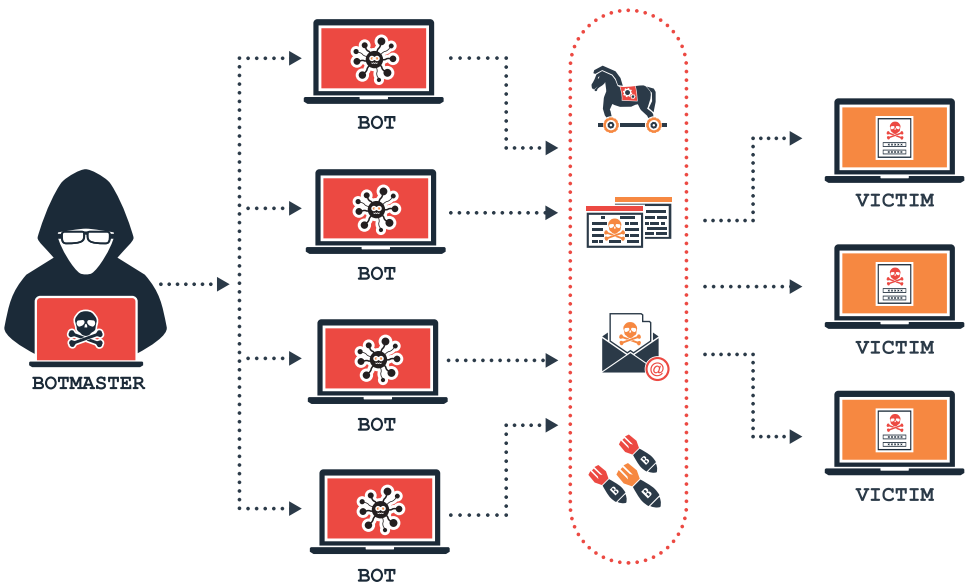


FIGURE 18.14 Bots used to infect other computers

The following are common symptoms of a virus/malware:

- Computer does not boot.
- Computer drive space is reduced.
- Applications do not load.
- An application takes longer to load or function than it used to.
- Drive activity increases (especially when no work is being done and the antivirus software is not currently scanning).
- An antivirus software message appears.
- The number of hard drive sectors marked as bad steadily increases.
- Unusual graphics or messages appear on the screen.
- Someone notices **missing files** or altered/renamed system/personal files.
- A message indicates that the drive cannot be detected or recognized.
- Strange sounds come from the computer.

Antivirus applications can be configured to run in manual mode (on demand) or as scheduled scans. When you have an infected computer, you should quarantine it. This means you should disconnect the computer from the network until the computer is virus free. Some antivirus programs can quarantine a computer automatically if the computer has a virus. Many antivirus software programs have the capability to quarantine files—files that appear to the antivirus program as possible virus-infected or suspicious files that might be dangerous. A message or **desktop alert** normally appears, with a list of files that have been quarantined, and each one must be identified as a valid file or to be left in quarantine (unusable) until a new version of the antivirus signature files has been updated and can identify the file.

Adware

Most people who are on the internet have at some point gone to a site that has material called **adware** that automatically appears and sometimes disrupts what they are doing on that site. Many times adware appears as pop-up advertisements. Adware can in many cases collect data about a user and then use that information to present more ads or direct the user to malicious websites. A user who clicks on one of these advertisements may unknowingly install a **potentially unwanted program (PUP)** that could cause problems for the computer such as changing the browser home page, slowing the browser or computer, tracking the user, or adding browser extensions/toolbars.

The following suggestions can help deal with adware:

- Avoid sites that have pop-ups.
- Implement anti-malware software.
- Ensure that the OS has all updates applied.
- Download only from reputable sites.
- Back up data or store it in the cloud.
- Review installed programs and remove any that are unfamiliar.
- Reset browser settings.
- Use anti-malware/antivirus or adware removal software to remove adware.

Social Engineering

All technicians (and employees) should be aware of social engineering. **Social engineering** involves tricking people into divulging information, including their own personal information or corporate knowledge. Social engineering does not just relate to computers but can be done over the phone, through online surveys, or through mail surveys. One technique is **impersonation**, in which someone pretends to be from a trusted bank or company, such as Microsoft.

Shoulder surfing—looking at someone's computer screen while standing behind them—is a type of social engineering. Another type is dumpster diving, where someone looks in a trash bin inside or outside the office to gather information. No auditing or network security applications and devices can help with such deviousness. Good security awareness helps prevent unintentional disclosure.

TECH TIP

Watch out for tailgating

Tailgating (also known as piggybacking) is a type of social engineering in which an unauthorized person enters a building or an area of a building behind an authorized person. Prevention of tailgating requires training and diligence by all employees.

Phishing

Closely related to social engineering is the concept of phishing. **Phishing** (pronounced "fishing") is a type of social engineering that involves attempting to get personal information by using email messages from a company that appears to be legitimate. Phishing emails target debit or credit card numbers and PINs, Social Security numbers, bank account numbers, internet banking login IDs and passwords, email addresses, and security information such as a mother's maiden name and a user's full name, home address, or phone number. Most browsers include a phishing filter, which proactively warns computer users when they go to a site that is a known phishing site or when a site contains characteristics common to phishing sites. Table 18.8 lists and describes the different variations of phishing.

TABLE 18.8 Types of phishing

Type	Description
Vishing	A phone call is used to obtain information from a target.
Smishing	Text (SMS) messages are used to tempt people into revealing information or contain malicious links.
Spear phishing	Specific information (such as an invoice, a known company, or account information) makes the recipient think an email is legit (see Figure 18.15).
Whaling	Messages sent to senior executives entice them to provide information or funds. The sender might impersonate another senior executive to make the message seem legit.
QR code phishing	Information in a QR code leads to a malicious website. Also called quishing.

FIGURE 18.15 Spear phishing

Many companies hold yearly training on security, with specific focus on phishing because it can be so damaging to the corporate network environment. Here's how to recognize phishing:

- Look closely at the address line and specifically the name after the @ symbol. Look up that domain name and see if it belongs to a legitimate company.
- Look for transposed letters in what at first glance would seem to be the name of a company you know but that is spelled incorrectly.
- Be suspicious of emails coming from an IT department or that have "IT department" (or another department that you would trust) in the subject line.
- Be suspicious of emails that use poor grammar.
- Hover your cursor over a link to see the actual URL and if the link address is suspect.
- Be suspicious of any message about a virus or computer problem that has a link. The link might redirect you to a fake antivirus application, repair application, or company. Don't click anything in the message. Use the close button and run your malware detection software to scan the system.
- Consider and review any email that seems to want to give you a sense of urgency.

Security Attacks

Security attacks can come from outside or from within a corporate network. Table 18.9 lists various types of attacks.

TABLE 18.9 Types of network attacks

Type of attack	Description
Access	A type of attack that frequently uses multiple dictionaries to gain access to accounts, databases, servers, and network devices. Types of attacks include on-path, port redirection, buffer overflow, and password attacks.
Backdoor	Also known as a trapdoor, a planted program that executes to bypass security and/or authentication.
Botnet	Software that spreads from hacked device to hacked device (called zombie computers, or zombies) and that is under control of someone else (refer to Figure 18.14).
Brute force	Repeated attempts to check all possible key combinations to gain access to a network device or stored material.
Business email compromise (BEC)	An email that appears legitimate and that makes what appear to be legitimate requests, such as an invoice that seems to be from a known vendor but with a different payment address.
Dictionary	A brute-force attack to try to determine a password or decryption key by trying different words found in a dictionary.
Denial of service (**DoS**)	A string of data sent to overload a firewall, router, switch, server, access point, etc. in an attempt to deny service to other devices.
Distributed denial of service (**DDoS**)	A group of infected computers attacking a single network device by flooding the network with traffic.
Evil twin	An attack in which the threat actor has a rogue access point and broadcasts the same SSID in order to capture packets from unsuspecting users.
Insider	An attacker who either works for the company being attacked or is using a corporate network device to carry out the attack.

Type of attack	Description
Man-in-the-middle (MITM) or **on-path**	A technique in which a hacker inserts a device between a sender and a receiver so the device can receive the intended traffic. Breaches may affect data or email communications and may change information that is being transmitted. Access points, DHCP servers, and default gateways are commonly simulated in this type of attack.
Password spraying	An attack in which the attacker uses a commonly used password on a few accounts to avoid triggering password lockout or a firewall reaction.
Rainbow table	A method of obtaining a password in a short amount of time by using a table that contains previously discovered hash values that are used to encrypt passwords.
Reconnaissance	A technique that involves attempting to gather information about a network before launching another type of attack. Tools used include port scanners, pings, and packet-sniffing programs.
Replay	A technique in which a valid network message or certificate is re-sent, usually in an attempt to obtain login information.
Smurf	A technique that involves using ICMP to send a large amount of network traffic at a specific device to deny that device network access, ping a nonexistent device to generate network traffic, or ping all network devices to generate traffic in ICMP replies.
Spoofing	A technique that involves sending an Ethernet frame with a fake source MAC address to trick other devices into sending traffic to a rogue device. Can be used in conjunction with an on-path attack.
SQL injection	An attack in which Structured Query Language (SQL) is used to access, query, and change databases as well as build data views for users. An SQL injection attack is used to acquire data, access data, cause data errors to display, or destroy data.
Supply chain/ pipeline	A hard-to-detect attack in which a trusted vendor's access is used to compromise the company.
TCP/IP hijacking	A technique in which a stolen IP address is used to gain access and/or authorization information from a network.
Vulnerability scanner	A software program used to assess network devices to identify weaknesses such as unpatched operating systems, open ports, or missing/outdated virus-scanning software.
Cross-site scripting (**XSS**)	An attack in which code is injected into a legitimate website to steal data, insert a Trojan horse program, or redirect to a rogue website.
Zero day	A type of attack that takes advantage of a vulnerability in a particular software application that is found by hackers before it is known/fixed by the software developer.
Zombie	A device that has been hacked and is controlled by someone else or that carries out malicious tasks.

Protecting Access to Local and Network Resources

Several techniques exist to protect computer access, and some of them have already been considered in this chapter as part of physical access. Companies use professional software to help with security threats, and the protection can be categorized broadly into three types:

> **Endpoint detection and response (EDR): EDR** is used to protect devices like computers, laptops, and servers.
> **Managed detection and response (MDR): MDR** provides real-time monitoring and potentially provides security recommendations.
> **Extended detection and response (XDR): XDR** includes EDR and MDR features as well as network, cloud environment, and app security coverage.

Let's look at protecting resources from the perspective of technical configuration and support and start with a couple important terms. Authentication, as we've already discussed, is used to determine what network resources can be used. **Authorization** involves the operating system or network granting access to specific resources on a computer system or network, such as files, folders, printers, video conferencing equipment, scanners, and so on.

User Management

In a corporate environment, each user has a username that is part of the domain; the user uses that username as well as a password to authenticate to a centralized server. In a home or small company, local accounts are used, and they can be either Microsoft accounts or local accounts. A local account is a traditional user account, but by using a Microsoft account, your account settings are synced across all Microsoft devices, including OneDrive, Messenger, Xbox, Outlook, and Hotmail. With a Microsoft account, if you are locked out, you are locked out of all of those accounts, and you have to take steps to reset your Microsoft account, which could take some time.

Users can be added and placed into groups for ease of management. Table 18.10 shows the default local users and groups for Windows. Note that Windows Home versions do not support local group accounts.

TABLE 18.10 Windows default users and groups

User or group	Description
Administrator (user)	Has total control of the computer; best practice is to rename the account and password protect it and create another user account that belongs to the administrator group and has a complex password.
Administrators (group)	A user account that has been created and placed in this group that has total control of the computer.
Child (user)	Part of the Microsoft Family Safety feature that allows parents to control access to apps, websites, and screen time.
Guest (user)	A member of the Guest group; disabled by default; no default user rights.
Guests (group)	Used by those who do not have an account on the computer; normally does not require a password; best practice is to disable it.
Standard Account (user)	Default type of account created when you create a common corporate staff worker; the user is required to request an administrator to make changes to software, hardware, or security settings.

User or group	Description
Backup Operators (group)	Can back up and restore files and folders, regardless of permissions assigned; cannot change security settings; can access the computer from a remote location.
Users (group)	Can perform common tasks and create local groups but cannot share folders or printers.
Remote Desktop Users (group)	Can log on to the computer from a remote location.
Offer Remote Assistance Helper (group)	Can use the Remote Assistance program to help a computer user.
Network Configuration Operators (group)	Can make TCP/IP changes and release/renew IP addresses.
Performance Log Users (group)	Can manage local or remote performance logs and alerts.

TECH TIP

Always change the default admin password

Whether it is a Windows computer, a router, or any other electronic device, always **change the default admin user account password** or create an account that has administrator access and disable the default account.

Windows 10 and 11 do not allow you to disable the Administrator account, but you can add a user who has administrator access. In Windows 10/11, access the *Accounts* Settings link. Select the *Add someone else to this computer* (Windows 10)/*Add account* (Windows 11) link > select the *I don't have this person's sign-in information* link > select the *Add a user without a Microsoft account* link. Select the newly created user and select the *Change account type* link > change the account type to *Administrator* > *OK*.

TECH TIP

Use the Lock Computer option

When away from your desk, use the *Lock Computer* option by pressing Ctrl+Alt+Del and selecting *Lock* or *Lock This Computer* or just pressing ⊞+L.

Basic Active Directory Functions

Technicians sometimes have to use a Windows server and specifically the **Active Directory** (AD) service on the server to manage users and devices on the network as part of security best practices in the corporate environment. You can use Active Directory to define domains. Remember that a domain makes it possible to organize all user accounts and devices such as computers and printers.

Within Active Directory, users can be placed in groups so that administration (for example, assigning security rights) is easier. Figure 18.16 shows a corporate structure in which one group of users is the Information Technology Services group. By expanding the group, you can see the users listed there.

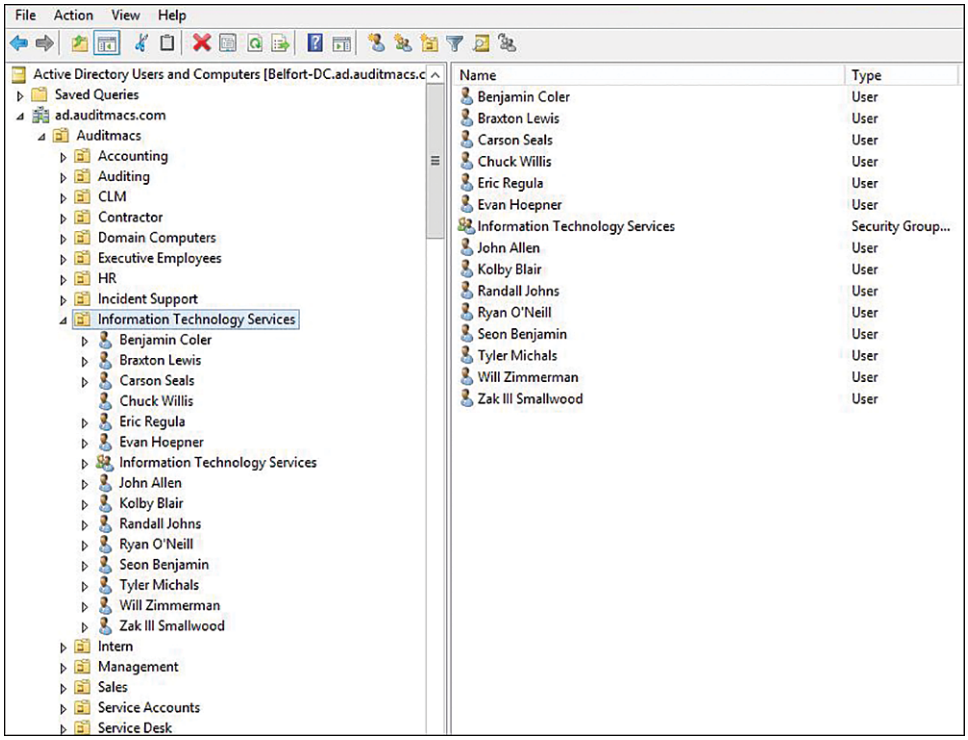


FIGURE 18.16 Active Directory Groups

You can have a computer **join a domain** by using the *System* Settings link > *Change settings* link > *Change* button > *Domain*. If you are using Azure or another vendor for corporate Active Directory management, you can use the *Accounts* Settings link to select *Access work or school* > *Connect*. Users on a domain can use single sign-on to access corporate apps and resources.

Groups can be combined into a domain group for even more centralized administration. When you create a domain group, you must choose between one of two types: security or distribution. A **security group** makes it possible to apply group policy settings or permissions to any shared resource. Distribution groups are merely email distribution lists.

Organizational units (OUs) are useful when you apply policies such as security policies or other corporate Windows rules to a part of an organization. OUs can contain groups, users, computer accounts, and even other OUs. OUs are useful when you want to delegate or let one or more administrators have control over a specific area of users, computers, and groups. Right-click on any object and select *Move* > select the target OU where you want to move it to > *OK*.

To do account creation in AD (that is, to add a user to a particular group), open the User Manager by going to the *Start* button > *Programs* > *Administrative Tools* (Windows 10)/*Windows Tools* (Windows 11) > *Active Directory Users and Computers*. Expand the domain (the section that starts with "ad.xxx") until you see the group you want; click on that group. From the menu bar, select *Action* > *New* > *User*. In the dialog box, enter the user information and click *Next*. Enter the password and select any appropriate security settings, such as *User Must Change Password at Next Logon*, as shown in Figure 18.17. Figure 18.18 shows the user account properties screen, where you click *OK*.

Users are commonly placed in groups so that they can be managed more easily. To place a user in a group, click *Start* or search for *Active Directory Users and Computers* > expand the particular group the user is currently in or just select the *Users* folder > locate the user that has been added previously and right-click on the name > *Add to a Group*. Note that you can also add a user to a group from the user's *Properties* window (refer to Figure 18.18) and select the *Member Of* tab > *Add* button. Either way, you are presented with the Select Groups window, as shown in Figure 18.19.

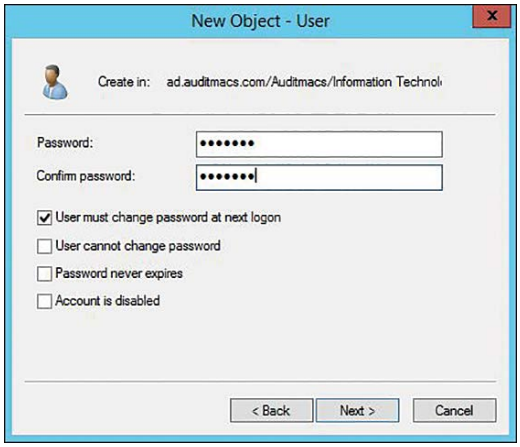


FIGURE 18.17 Setting a new user password in Active Directory

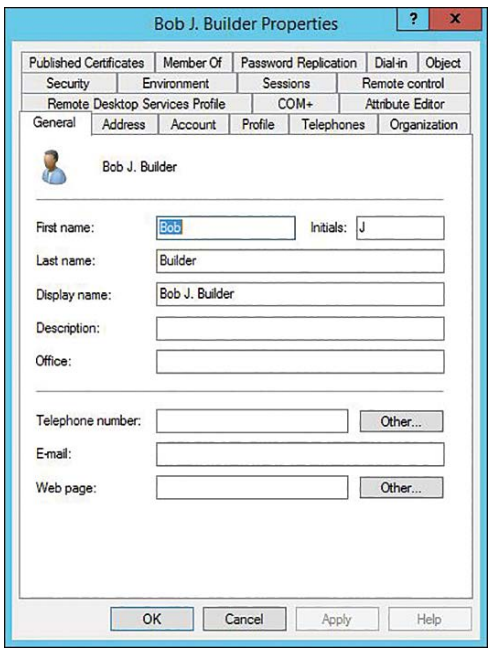


FIGURE 18.18 Viewing properties of a new user in Active Directory

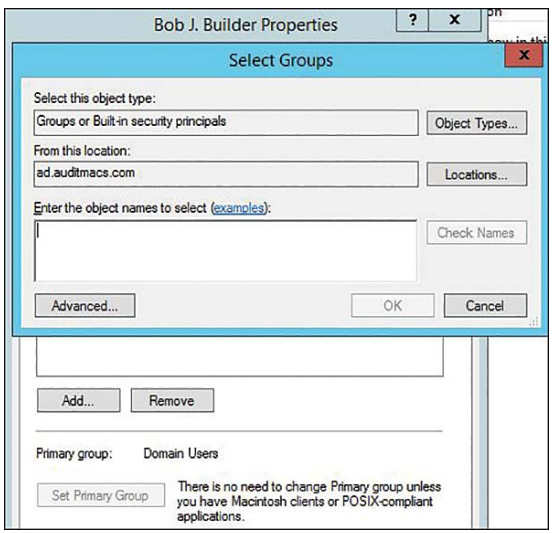


FIGURE 18.19 Adding a user to a group in Active Directory

Type the name of the group you want the user to be in. Look at the groups within the domain shown to the left of this window (refer to Figure 18.16), such as HR or Information Technology Services. You can also click on the *Advanced* button and the *Find Now* button to see a list of all the groups and then simply click on one of them. A user can be a member of multiple groups, and those groups are shown on the *Members Of* tab.

A similar window is used to add a user to one or more security groups. Use the *Security* tab within the user's properties window. Select the group(s) to add the user to > *Apply* > *OK*. Note that the user will need to log off and then log back on to the network for the resources to be available.

Other functions within the user account properties that might need to be set by a technician are the logon script, home folder, and folder redirection. A logon script (sometimes referred to as a **login script**) is a set of tasks configured in one file that run when a user logs in, such as running a specific application, performing an operating system function on the local computer, or setting system environment variables. The logon script can be defined as part of a group policy (covered in the next section) or through the *Properties* window > *Profile* tab, as shown in Figure 18.20.

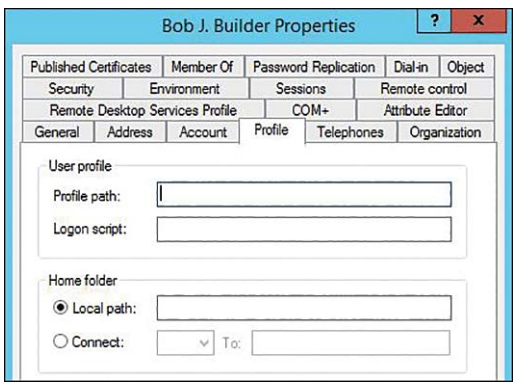


FIGURE 18.20 Using the Profile tab in Active Directory

Notice in Figure 18.20 the Home Folder section. A **home folder** is a network folder that allows users to store their files and have access to them from any device that they log onto within the same domain. Commonly the *Connect* radio button is used to assign a drive letter in the first drop-down menu, and then the network path where the files are stored is provided (for example, `\\ServerName\FolderName\%username%`).

Another technique used for user data storage is folder redirection. **Folder redirection** involves mapping a folder on the local machine to a network location such as a server. The user then has access to the files within that folder from any device on the network domain. Folder redirection is commonly implemented in conjunction with offline files and roaming user profiles. (Profiles are covered later in the chapter.) This way, data is available to the user through any device on the network, even if the network or server is down. Within the *User Configuration* section, expand *Policies* > *Windows Settings* to locate and expand the *Folder Redirection* folder. Right-click on any folder > *Properties* and input the desired network path to where you want those types of files to be stored.

A few more things you might need to do as a technician are delete or disable an account, reset a user password, and unlock a user account. There are several ways to do account deletion in AD. One way that is commonly used is to right-click on someone's name (see Figure 18.21) and select the *Delete* option > *Yes* when prompted if you are sure of the deletion. Some companies have a policy of not deleting user accounts in case users come back or in case you might for some other reason need to access accounts. Instead, some managers disable an account and put that disabled account into a group with all the other disabled accounts. Microsoft includes a Recycle Bin for

deleted Active Directory objects such as user accounts, but this feature is not enabled by default. To manually disable an account, locate and right-click on the user account and select *Disable Account*.

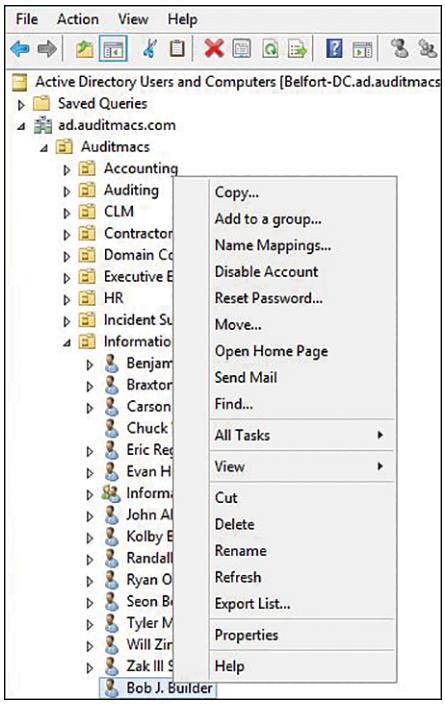


FIGURE 18.21 Right-clicking a user account in Active Directory

Local and Group Policies

Another method of controlling login passwords is through a local- or domain-based group account policy. Policies do more than just define password requirements. They can define the desktop, what applications are available to users, what options are available through the *Start* menu, whether users are allowed to save files to external media, and so on. A domain policy, or **group policy**, can be created, updated, and applied to every computer on the domain.

A **local security policy** is created on a computer, and it could be used to disable auto-playing of media such as USB drives and optical discs, prevent users from shutting down or restarting a computer, turn off personalized menus, or prevent someone from changing a browser home page. A local security policy might be implemented in a workgroup setting. A group policy is more common in a corporate environment, and a group policy can overwrite a local policy. If any computer settings on a networked computer in a corporate environment are grayed out, the settings are probably locked out due to the policy deployed throughout the domain.

TECH TIP

Accessing the local security policy and group policy

Access the Local Group Policy Editor window by typing `gpedit.msc` at a command prompt or in the *Search* textbox. Use the `gpresult` command to display group policy settings. Use the `gpupdate` command to update all domain users with a newly deployed group policy. Use the `secedit` command to configure or analyze a security policy.

The following are some best practices for securing a workstation in a corporate environment.

- **Restrict login times**. If someone works during the daytime Monday through Friday, then restrict Saturday and Sunday or evenings.
- Use the Account expires option from the Account tab if a person leaves the company. Then, if they return, it is very easy to re-enable the account. For auditing and recording purposes, avoid deleting accounts.
- Set password expiration requirements. Require a user to change their password after 60 or 90 days unless a long, complex passphrase is required. Then only require changing the password if a security breach is suspected.
- **Disable the guest account**. Use the Computer Management Console > expand *System Tools* > expand *Local Users and Groups* > double-click on the *Guest* account > select the *Account Is Disabled* checkbox.
- Enable the failed attempts lockout feature to lock out users after a specific number of failed login attempts. In the **group policy editor**, expand *Security Settings* > *Account Lockout Policy* to access how long someone is locked out and how many failed attempts are allowed.
- Configure a **timeout/screen lock** for when users are away from their workstations to automatically lock their screens after a period of nonuse.
- Restrict user permissions and apply the principle of least privilege (which is covered later in this chapter).

Through the defined policy, criteria for auditing can also be set. Auditing, sometimes called *event logging* or just *logging*, is the process of tracking events that occur on the network, such as someone logging in to the network. In a business environment, a server with special auditing software is sometimes devoted to this task because it is very important to security. Figure 18.22 shows the Local Group Policy Editor window.

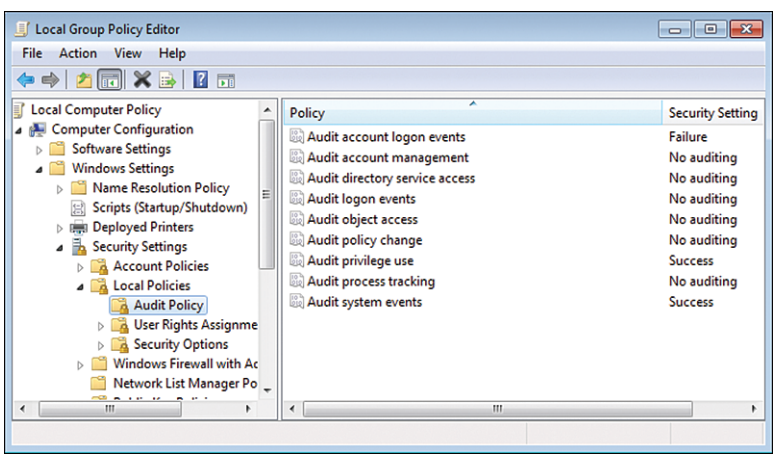


FIGURE 18.22 Local Group Policy Editor window

TECH TIP

Requiring password protection

You can enable or disable password protection through the Network and Sharing Center on a workgroup computer. If password protection is enabled, a person accessing a shared folder from a remote location must have a user account and password on the computer that holds the network share.

Permissions

It is important to monitor users and groups as well as the devices, data, and applications they have access to. Permissions control what can or cannot be done (permit or deny access) to files, folders, and devices from a remote connection. (This is similar to file attributes, covered in Chapter 15, "Introduction to Scripting.") By sharing files and folders, each computer can act as a file server. A security best practice is to restrict user permissions, but permissions can cause havoc. Network administrators and end users can set permissions on folders, and these permissions may affect another user's access to files and folders. Technicians need to be familiar with permissions.

Two types of permissions can be assigned in Windows:

> **Share permissions** provide and/or limit access to data across a network. Using share permissions is the only way to secure network resources on FAT16 or FAT32 drives.

> **NTFS permissions** provide tighter control than shared folder permissions. NTFS permissions can be used only on NTFS or ReFS drives.

TECH TIP

If file permissions change

If you ever notice that file permissions change (for example, you can no longer access an application or a file that you once could), check for a virus. Note that in the case of some viruses that change file permissions, you may need to repartition the hard drive and reinstall the operating system to remove the virus.

Share Permissions

To share a folder other than the `Public` folder, use *File Explorer* > right-click on the folder name > *Give Access To* > type the name of the person > *Add*. You can do one of the following at this point:

> If the computer is attached to a network domain, select the arrow to the right of the textbox > *Find* > type the name of the person with whom you want to share the folder > *Check Names* > *OK*.

> If the computer is on a workgroup, click the arrow to the right of the textbox, select the appropriate name, and click *Add*. If the name does not appear, click the arrow to the right of the textbox and click *Create a New User to Create the User Account*.

> An alternative method is to locate the folder using *File Explorer* > right-click or tap and briefly hold on the folder icon > *Properties* > *Sharing* tab > click the *Share* button. Figure 18.23 shows this window.

TECH TIP

Share permissions are only applicable across a network

Shared folder permissions are applicable only across a network. This type of permission does not prevent someone sitting at the computer from accessing files and folders. For best protection across a network and at the computer, use NTFS file and folder permissions.

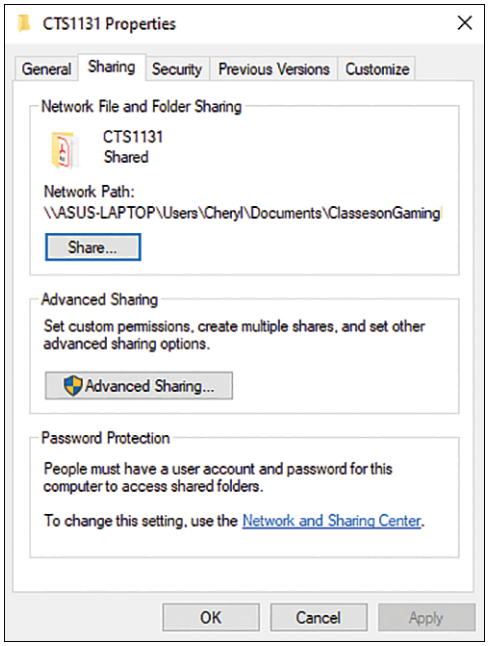


FIGURE 18.23 Using the Sharing tab to share a folder

Permissions are set by clicking the *Advanced Sharing* button (see Figure 18.24). Notice that you can limit the number of simultaneous users who can connect to this folder from a remote location. Click the *Permissions* button. Notice in Figure 18.25 that you can select the Allow or Deny checkboxes for the individual permissions.

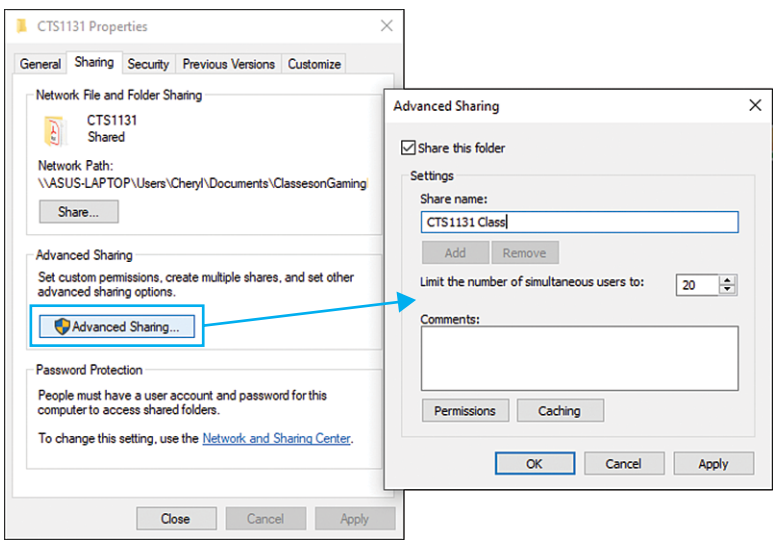


FIGURE 18.24 Folder Sharing tab > Advanced Sharing options

TECH TIP

What is the maximum number of concurrent users?

A maximum of 20 users can simultaneously use the same shared folder.

Notice in Figure 18.25 that you can select Allow or Deny for specific types of permissions (Full Control, Change, and Read). Table 18.11 shows the effects of setting each of these permissions to Allow.

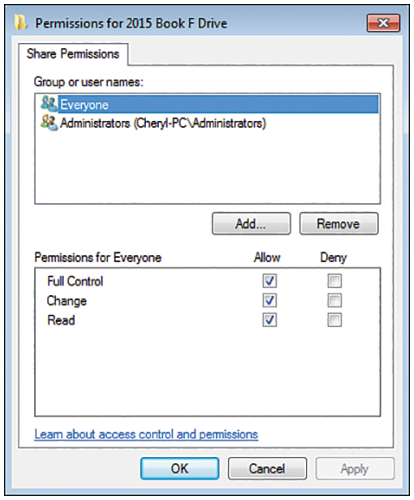


FIGURE 18.25 Folder Sharing tab > Advanced Sharing > setting Permissions

TABLE 18.11 Share permissions

Permission	Description
Full Control	Users can do everything, such as change the file permissions, take ownership of files, and perform everything that can be done with the Change permission.
Change	Users can add new subfolders, add files to a folder, change the data in a file, add data to files, change file attributes, delete folders and files, and do all the tasks that are possible with the Read permission.
Read	Users can look at file and folder names and attributes and can open files and execute scripts.

TECH TIP

Principle of least privilege

When determining access to a folder or to a server room, you should give access to only what is needed and only to the people who need access—and no more. Giving people access to an entire drive or building when they just need access to a particular folder or room puts the entire hard drive or company at risk.

File and folder security protection is a concern. A subfolder and any files created within that subfolder all inherit security permissions from the parent folder or the folder that contains the subfolder. This feature can be disabled when necessary.

Local and Administrative Shares

Files and folders can be shared in a network workgroup or a domain. A **local share** is something—a printer, folder, or media device—that is shared on a specific computer. **Administrative shares** are shares created by Microsoft for drive volumes and the folder that contains the majority of Window files. An example of an administrative share is a drive volume letter, such as `C`, followed by the dollar sign, `$`: `C$`. The `admin$` administrative share is used to provide access to the folder that contains the Windows operating system files.

Windows automatically creates administrative shares, but by default Windows prevents local accounts from accessing administrative shares through the network. A better solution is to disable a particular administrative share through a group policy.

Any local share can be made a **hidden share**, which is a share that is not visible by default throughout the network. To make a share a hidden share, add the dollar sign (`$`) to the share name. This might be beneficial for computer users who want to access something from their remote computer without making it visible to other network users.

TECH TIP

Access denied message

If a user or technician ever receives an access denied message on a shared folder or hidden share, ensure that the user login is one that has administrative privileges or check the assigned permissions on the shared folder.

Public Folder

Another way that Windows supports sharing is through using the `Public` folder. The default path for the `Public` folder is `C:\Users\Public`. You can copy or move any file to the `Public` folder. This makes it easier to share files with someone, but when files are copied into this folder, twice as much hard drive space is used because there are copies of the same material in two folders.

If sharing is enabled for the `Public` folder, anyone who has a user account and password on the computer can access the data. In addition, any user on the network can see all files and folders in the `Public` folder by selecting *Network* from File Explorer, accessing the appropriate computer, browsing to the `Users` folder, and opening the `Public` folder. You can set permissions so that this folder is inaccessible, or you can restrict anyone from changing files or creating new files. However, you cannot pick and choose what files individuals can see.

To use the `Public` folder, access the *Network and Sharing Center* Control Panel > *Change advanced sharing settings* > expand the *All Networks* section by selecting the down arrow if it is not showing any information below it > locate the *Public folder sharing* area > select the *Turn on sharing so anyone with network access can read and write files in the Public folders* radio button. Note that you must also turn on network discovery and file and print sharing to see shared files across the network.

NTFS Permissions

Additional security protection is available on an NTFS partition through Windows. To share a folder using NTFS permissions, locate the folder in File Explorer. Right-click on the folder name and select *Properties* > select the *Security* tab (see Figure 18.26). Notice that more permissions can be administered on an NTFS partition using NTFS permissions than is possible with share permissions. Table 18.12 describes these permissions.

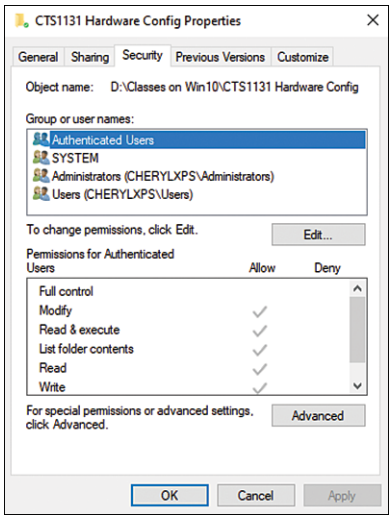


FIGURE 18.26 Windows NTFS permissions—using the Security tab

TABLE 18.12 NTFS permissions

Permission	Description
Full Control	Users can do anything in the files and folder, including delete, add, modify, and create files and folders.
Modify	Users can list items in a folder, read data, and write data, but they cannot delete subfolders and files and cannot take ownership.
Read & Execute	Users can list items in a folder and read a file, but they cannot change or delete a file or create new files. Users can execute applications contained within the folder.
List Folder Contents	Users can only look inside a folder.
Read	Users can display folder and subfolder attributes and permissions as well as look at a particular file.
Write	Users can add files or folders, change attributes for the folder, and add or append data in a file.

Inherited permissions are permissions that are propagated from what Microsoft calls a *parent object*. For example, if a folder is given the Read permission, then all files within that folder cannot be changed; they are read-only. If a subfolder is created, it inherits that permission. If the Allow or Deny checkboxes for any object are selected, the current permissions have been inherited.

There may also be issues when copying or moving is performed on objects that have NTFS permissions set. Consider these guidelines for copying and moving:

> When you copy a file/folder on the same or different NTFS drive letter, the copy inherits the destination folder's permissions.
> When you move a file/folder on the same NTFS drive letter, the original permissions of the object are retained.
> When you move a file/folder to a different NTFS drive letter, the moved object inherits the destination folder permissions.
> When you copy or move a file/folder to a drive that uses a different file system (such as FAT), the object loses all its permissions.
> If you change permissions on a folder that has content, only the new content inherits the changed permissions.

Effective permissions are the final permissions granted to a person for a particular resource. Effective permissions are important when you combine shared folder permissions given to an individual, shared folder permissions given to a group, and individual permissions. The following are some helpful tips when sharing folders and files across a network:

> Folder permissions are cumulative. When you grant folder permission to a group and then grant an individual permission to that same folder, the effective permission for that person is the combination of what the group gets and what the person gets. For example, if the group gets the Write permission and the person gets only the Read permission (and the person is a member of the group that has the Write permission), the person can both read from and write to files in the folder.
> Deny overrides any allowed permissions that have been set for a user or a group. For example, if a group is denied access to a folder, but a person is specifically allowed access to the folder, the person is not allowed to access the folder.
> When NTFS and shared folder permissions are both used, the most restrictive of the two is the effective permissions level.

Windows provides help in determining effective permissions. Right-click or tap and hold on a file or folder > *Properties* > *Security* tab > *Advanced* button > *Effective Access*. Note that what is shown is only for NTFS permissions. Share permissions are not part of the Windows calculation for this window.

Permissions-related issues are a common problem. A technician must be familiar with the results of misconfiguring permissions. If users have files that are stored in a mapped drive share and those files are moved to a different server, the mapped drive will need to be redone and point to the new server, and permissions will need to be applied on the new server.

TECH TIP

All subfolders are shared when a folder is shared

When you share a folder, all subfolders are automatically shared unless you make the subfolders private.

File and Folder Attributes

File and folder attributes are covered in Chapters 14, "Introduction to Operating Systems," and 15, "Introduction to Scripting," but need to be reviewed here as well. From the beginning, there have always been four main attributes:

> **Read-only:** Information cannot be changed.
> **Archive:** This attribute is used in backup operations to tell when a file folder has been backed up.
> **Hidden:** By default the file or folder isn't visible in File Explorer.
> **System:** By default the file or folder isn't visible in File Explorer, and it is used by the operating system.

With a drive that has been formatted with NTFS, additional attributes are available:

> **Compressed:** The file or folder has reduced storage size.
> **Encrypted:** The data within the file or folder is scrambled.
> **Indexed:** The file or folder is not included in searches by default.
> **Offline:** The file or folder is used by remote storage.

When a folder is shared across the network, the permissions given specify what a user is allowed to do with that particular folder. By default, all subfolders and files contained within a shared folder or subfolder inherit the same permissions. For example, if you select read-only as the shared folder permission, then someone can open a file but cannot modify and save it. If you right-click or tap and briefly hold on the name of a file within a shared folder that has read-only permissions assigned, you can then select *Properties* in order to access attributes, and you will see that the file has the read-only attribute already marked.

Getting the Job Done with the Correct Permissions

When working on a staff member's computer, remember that when you are logged on as that user, you may not be able to use specific utilities. Commonly used utilities or commands executed from a command prompt may not be available to you unless you operate from the administrator level (that is, **run as administrator**). Search for `command prompt`. In the resulting list, right-click or tap and briefly hold on the *Command Prompt* option > select *Run as administrator*.

Logging in with an account that has administrator access may not allow you to see the same issues the user sees. Therefore, in order to see some problems, you may need the user to be logged in. Always ensure that users log on and test whatever you fix to ensure that it works for their account and permissions.

Another adjustment that might need to be made is through User Account Control (**UAC**), which can prevent users from installing apps that might contain malware or using system tools that could cause harm to the system if used improperly. Windows 10/11 has four options to choose from:

- **Always notify:** Requires an administrator account in order to make changes.
- **Notify me only when programs/apps try to make changes to my computer:** Provides feedback if any app or program tries to make changes on the computer or install software. It will not allow any other tasks to be performed until a response is made, and it does not provide notification if any Windows settings are modified.
- **Notify me only when programs/apps try to make changes to my computer (do not dim my desktop):** Helps if the computer takes a long time to dim the desktop (the computer is slow).
- **Never notify:** Does not provide any notifications if a program tries to make changes to the computer or install software.

Folder Options

Because of quarantined files or the need to check system files, a technician is required to be familiar with File Explorer display options. Use the following directions:

- **Windows 10:** Open *File Explorer*. Access the *View* menu option > *Options* > *Change folder and search options* > *View* tab.
- **Windows 11:** Open *File Explorer*. Access the *View* menu option > point to the *Show* option.

Use the *File Explorer Options* Control Panel to configure how folders/files display and what information is included with that display.

A technician often has to work with system files and folders that are not visible by default. Table 18.13 summarizes the security-related *View* tab options. A technician must remember to set the settings to the way they were previously so that users do not see them by default. The *View* tab has a *Restore Defaults* button that resets all settings.

TABLE 18.13 View tab options

Function	Options to select
View hidden files	*Hidden files and folders* section > enable *Show hidden files, folders, and drives*
View file extensions	*Files and Folders* section > uncheck *Hide extensions for known file types*
View system files	*Files and Folders* section > uncheck *Hide protected operating system files (Recommended)*
Sharing menu/options	*Files and Folders* section > enable *Use Sharing Wizard (Recommended)*

Protecting the Operating System and Data

Several chapters have provided important security-related tips, steps, and information related to protecting the operating system and data. In this section, let's review some tips that pertain specifically to the security of the operating system and data:

- Use the NTFS file system.
- Conduct good **patch/update management**. Ensure that operating system and application service packs and updates are applied regularly. If a Windows Update fails, a message usually appears when the machine reboots. Try the update again; sometimes an update might fail when being installed with other updates. Successfully install as many as you can and then reinstall the failed updates one by one. Note that in Windows 10/11, updates come as a package, but they can be uninstalled individually by update number by using the *Update History* Windows Settings option. Note that mobile devices also need **patching/OS updates**, including updates to the phone's radio firmware.
- Ensure that the OS has not reached end-of-life (EOL) and is no longer able to be updated or receive security patches.
- Have an alternative boot source (such as an optical disc, a flash drive, another hard drive, or an operating system disc).
- Watch out for **unprotected systems**. Check for missing antivirus/anti-malware software and make sure the firewall is not disabled. Install antivirus/anti-malware software with the latest updates and enable the firewall, if necessary.
- Encrypt data that needs to be protected.
- Optionally, place operating system files and data files on separate hard drive partitions.
- Some firmware or driver versions may cause security issues. Keep the versions updated.
- Disable unused services. You can use *Security Templates* in a group policy to make company-wide changes. On a local machine, search and open *Services*. Change the *Startup Type* to *Disabled*.
- Notifications may appear from the bottom-right corner. Any **unwanted notifications** can be controlled by using the *Notifications & actions* Windows Settings link, as shown in Figure 18.27. Scroll down to see configurable actions for specific apps.
- Virtual machines need the same security software as host machines.
- If the computer you use does not need to share files or a printer with others on the network, use the *Network and Sharing Center* Control Panel and disable *File and Print Sharing*.
- To create a shared folder that is not seen by any others across the network, add a `$` (dollar sign) to end of the share name. An example of a hidden shared folder is `Book$`.

> Use the System Restore program to control restore points before installing new software or hardware. Use the *System* Settings link > *System Protection* link to access the restore points.
> Disable ports through the system BIOS/UEFI settings. Password protect the BIOS to prevent use of external devices that might be infected with viruses.

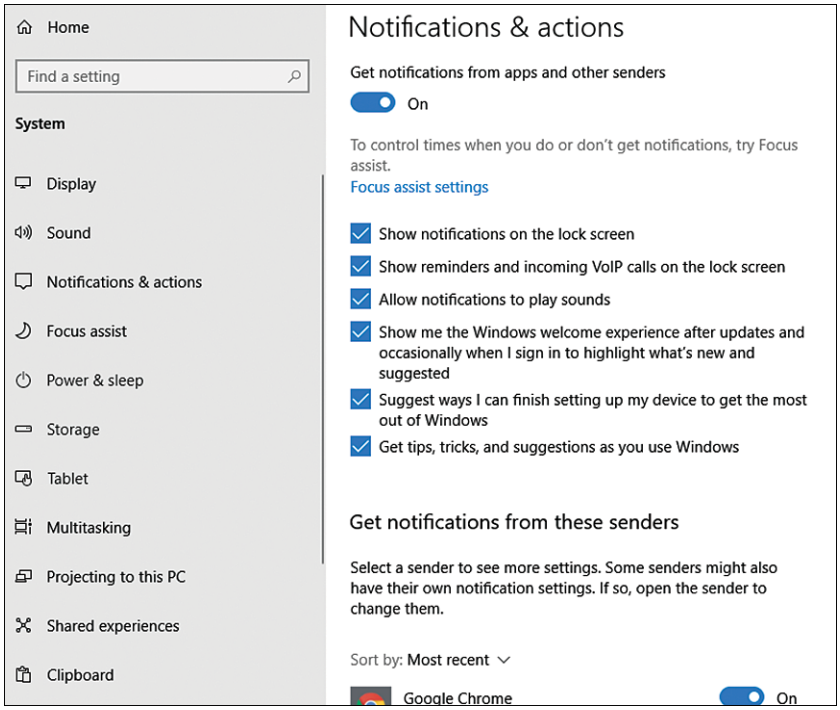


FIGURE 18.27 Windows Notifications & actions options

A larger company may have a data loss prevention (**DLP**) plan that uses specific software and processes to detect, monitor, and prevent the loss of important corporate data. The company DLP policy defines how data is named, stored, used, and secured. Whether data is being moved from one location to another, is at rest stored somewhere, or is being used by an app or a person, AI and machine learning can be used to apply the company's data security policy.

Backup/Restore

One hard drive preventive maintenance procedure that is commonly overlooked is performing a backup of the data and operating system as well as the restoration. Backup and restoration should be part of any disaster prevention plan. Most people do not realize that the most important part of any computer is the data that resides within it. Data cannot be replaced as easily as hardware can be.

Back up data routinely. Also make a backup of applications that are critical to the family or business. Have a routine maintenance plan that you recommend to users. Important data should be backed up daily or frequently, but routine data is usually backed up monthly. The sensitivity and importance of data determine how frequently backups are performed.

TECH TIP

Backup testing

Ensure that you test a backup to ensure that your method works and the time required to restore is as expected. **Backup testing** should be part of an implementation plan as well as a disaster prevention/recovery plan and should be done on a scheduled basis.

Traditionally, backups were saved to magnetic tape—quarter-inch cartridge, linear tape-open (LTO), or digital linear tape (DLT) being the most common types—but CDs, DVDs, BDs, thumb drives, and external hard drives are viable **on-site storage** alternatives today. Cloud storage (see Figure 18.28) or **off-site storage** is an important part of a backup plan.

Advantages of local storage include the ability to control the security of that data and the cost of the media used. A disadvantage is that you have to store and maintain that media. Cloud storage can be free or for a charge, but security is a concern. In addition, restoration requires connectivity to the cloud storage.

TECH TIP

A second hard drive makes an excellent backup device

Hard drives are inexpensive and easy to install. Install a second one to back up your data. Another alternative is to put your operating system and applications on an SSD and use a mechanical drive for your data for easier backups.

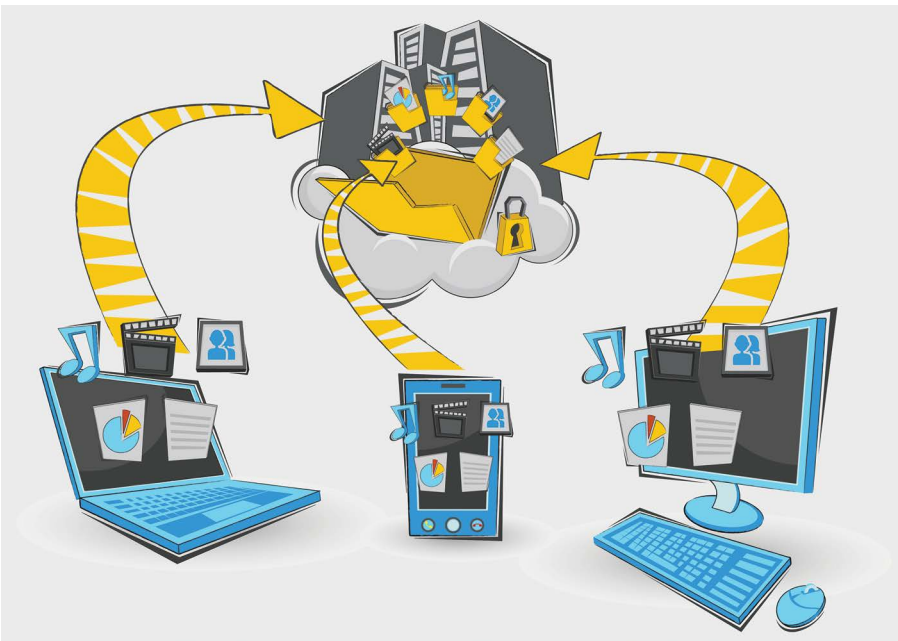


FIGURE 18.28 Cloud storage for backups

Backups use the file archive bit. A **full backup** backs up all selected files and sets the archive bit to off. An **incremental backup** backs up all files that have changed since the last backup. The files selected are the ones that have the archive bit set to on. The backup software resets those archive bits to off. In contrast, a **differential backup** backs up files that have changed since the last full backup (files that have the archive bit set to on), but the backup software does not reset the archive bit, as an incremental backup does. A **synthetic backup** makes use of a full backup and incremental backup, as shown in Figure 18.29.

All of these types of backups are known as file-level backups. Another type of backup is an image-level backup, which backs up an entire drive to one file (called an image). The drawbacks to this type of backup are the size of the image and the time involved. A company may have a computer image of an operating system and standard applications that is pushed onto the machine, and then users back up their data by using a file-level backup technique.

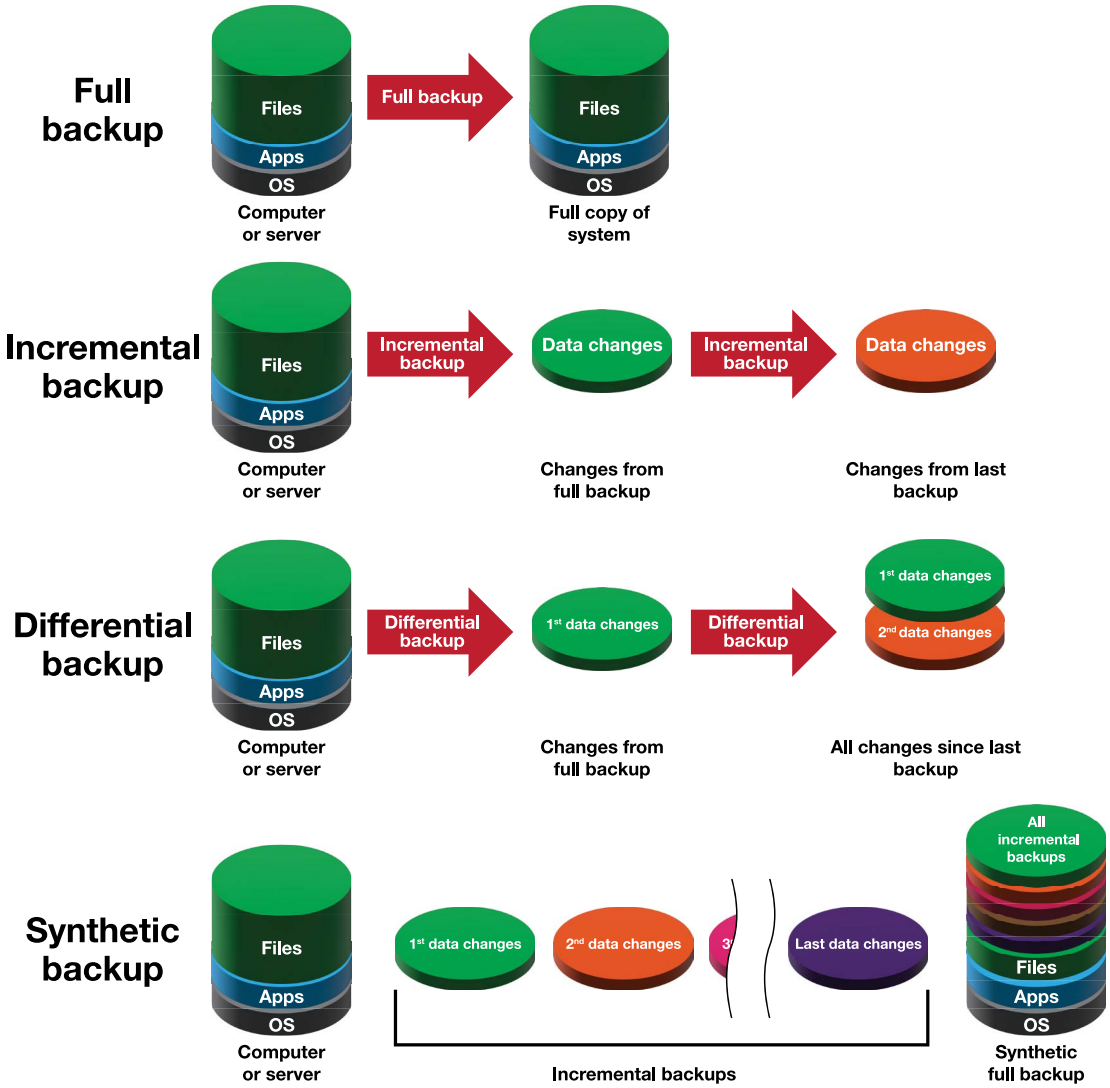


FIGURE 18.29 Backup types

There are several backup rotation techniques, but all of them should include off-site storage in case of disaster, and every company should have a plan for how often backups are done. Here are two popular ones:

> With a **grandfather-father-son** (GFS) **backup**, a full backup (a grandfather backup) is done on a schedule of perhaps once every two weeks or once a month and stored (potentially off site). Then another full backup (a father backup) is done (potentially to faster storage) more frequently, such as once a week. Then incremental backups (son backups) are performed daily until another full father backup is done.

> With a **3-2-1 backup**, three copies (one primary and two copies) of the data are made to two different media types, and one of the backups is kept off site.

Windows 10 and 11 come with a backup utility called Windows Backup, but many external hard drives come with their own software that is easier to use, has more features, and allows easy and selective data backup scheduling. Windows 10 and 11 also have the File History utility, which can also be used to automatically save file versions to OneDrive, an external drive, or a network share. Many vendors have a backup and recovery option that is part of BIOS/UEFI, part of the Windows System Recovery Options, or accessed in another manner. No matter what method of backup you use, test your backup for restoration. Install it to a different drive, if necessary.

TECH TIP

Don't use the same hard drive as a backup device

Backing up data to a different partition on a drive is not a good idea. The drive is a physical device that may have moving parts—motor, heads, and so on. Mechanical failure is always a possibility.

Probably the most commonly asked question of those with drive failures or failing/failed sectors is regarding file recovery. Windows does not have file recovery software beyond being able to locate and repair lost clusters. However, there are third-party file recovery utilities that you can use. Many times files cannot be recovered unless the file recovery utility was installed prior to the loss. Many companies also provide data recovery services.

TECH TIP

For critical data, keep backups in a different location

Off-site storage, or cloud storage, for critical data is important even for home users—to prepare for the possibility of disasters such as flooding, fire, theft, hurricane, or tornado. A company may even have redundant systems or servers located in a distant location (hot site) in case of disaster.

Even though much data is stored locally, many companies favor centralized storage, even for individual users. This protects the company's interest and also ensures that backups are done on a regular and reliable basis. Another option in business is a thin client environment, in which no hard drives are included with the systems. Storage is provided across the network to a central location. This reduces hardware and software costs and PC maintenance staffing costs, and it makes data security easier to manage as well.

All of the data recovery options covered in this section are **in-place/overwrite** solutions, which means that no matter where the backup data is stored, it is brought back and reinstalled on the problematic machine. Some companies have an **alternative location** to use when disaster strikes. The alternative location contains critical servers and other machines so that personnel could potentially work there.

Account Recovery Options

Whenever disaster occurs and backups/restores have to be done, there may also be a need to recover accounts from various vendors, including Microsoft, to aid in local account password recovery. This can be very time-consuming. Document critical information such as the following *before* disaster occurs:

- Computer/laptop/device make, model, year purchased, and warranty length
- Names, IP addresses, and backup configurations of network infrastructure devices
- Firewall rules
- Domain settings
- Account names and passwords for network infrastructure devices, network administrators, email, and internet provider settings
- BIOS passwords
- Software license keys, information, applications, versions, and purchasing agreements

BitLocker

BitLocker encrypts an entire disk volume, including the operating system, user files, page files (also known as paging files or swap files), and hibernation files. It is available on Windows 10 Pro, Enterprise, Education, Mobile, and Mobile Enterprise versions and Windows 11 Pro, Enterprise, and Education versions. BitLocker requires two NTFS or ReFS disk partitions.

BitLocker To Go is used to encrypt and password protect external drives and removable media 128 MB and larger. BitLocker can optionally TPM chips, which store security information such as encryption keys.

TECH TIP

What does it take to unlock a drive encrypted with BitLocker?

You need the BitLocker recovery key or the BitLocker password in order to unlock or decrypt a drive that has been encrypted using BitLocker.

Device Encryption

Mobile devices support **full device encryption**, which involves scrambling or encoding all user data. Once full device encryption is enabled, any new data created is automatically encrypted. A drawback to full device encryption is slower performance; in addition, disabling the option might require resetting the option back to factory defaults, which means you would lose any data and customization.

On an Android device, use the *Security* or *Lock Screen and Security* settings option. Apple iPhones have encryption enabled by default, and the option cannot be disabled.

Encryption Options

Data at rest is data that is not being used but that is stored somewhere such as on a local drive, in the cloud, or on an external drive. To protect this type of data, you can put a password on the file/folder or encrypt it using Advanced Encryption Standard (AES) or Rivest-Shamir-Adleman (RSA) (see Figure 18.30). **AES** is an encryption standard with key sizes of 128, 192, or 256 bits. AES has been used in wireless government networks for some time and is now common in almost all wireless network implementations that use WPA2 or WPA3 (covered later in the chapter). RSA is a slower algorithm and is not used as commonly as AES.

FIGURE 18.30 Encrypting data files and folders

NTFS volumes can have files, folders, and subfolders encrypted using Encrypting File System (**EFS**). The EFS algorithm originally used Data Encryption Standard (DES), which used 56- or 128-bit encryption, but now the EFS algorithm uses Advanced Encryption Standard (AES), Secure Hash Algorithm (SHA), and smart card–based encryption.

When a folder or subfolder is encrypted, all newly created files within the folder or subfolder are automatically encrypted. If any files are copied or moved into an encrypted folder or subfolder, those files are automatically encrypted. System files cannot be encrypted. EFS can use a certificate from a certificate authority (CA), such as one issued from a server, or a self-signed certificate.

TECH TIP

Can you encrypt someone else's files?

The answer is "yes" if you have the write attribute, create files/write data, and list folder/read data permissions for the file.

AutoRun and AutoPlay

Disable AutoRun to prevent software or programs that are executables from automatically starting from an optical disc, a flash drive, or an external drive. An executable may not be a safe program and may pose a security threat. In contrast, AutoPlay is a setting related to what happens when media is attached or inserted. For example, when you have AutoPlay enabled and insert a music CD, the music may automatically start playing or you may be prompted for the default action. To **disable AutoPlay** and control what happens when you insert each type of media device, use the *Devices* section of Settings > *Auto Play* link. You can also do this through the security policy. Use the following steps to disable AutoPlay and AutoRun so that the action will not occur and the user will not be prompted:

Step 1. At a command prompt or in the *Search* textbox, type `gpedit.msc` and press [Enter].

Step 2. Expand *Administrative Templates* > expand *Windows Components*.

Step 3. Select *Autoplay Policies* > double-click or double-tap *Turn off Autoplay* > select *Enabled* > select *All drives* > restart the computer.

Storage Drive Security

When donating a computer or replacing a hard drive, data on the drive needs to be removed after the data has been transferred to the new drive or is not needed any longer. Furthermore, the hard drive partitions need to be deleted and re-created. Some hard drive manufacturers offer utilities that rewrite the drive with all 1s or all 0s to prevent data remnants from being recovered. (This is sometimes called drive overwrite.) Another option is a **drive wipe**, which may use a number of techniques (not all guaranteed to be 100% effective on highly sensitive data) to remove data from the drive. A hard drive manufacturer may have a **low-level format** utility that is different from the **standard format** done through the drive installation/preparation process. You can use the SDelete utility, which can be downloaded from Microsoft (see http://technet.microsoft.com/en-us/sysinternals/bb897443.aspx).

Another option is to use the `format` and `cipher` commands. First use `format x: /p:n` (where `x:` is the drive letter and *n* is the number of passes) to format a disk volume with a 0 in every sector. Then use the `cipher /w x:` command, where `x:` is the hard drive volume letter. The `cipher` command writes all unused sectors with 0s, then 1s, and then a random number. Because this command is performed on unused sectors, it is important to remember to use the `format` command first.

A company that has extremely sensitive data stored on a hard drive should destroy the hard drive by using any of these techniques:

> Securely erasing the drive by using special software
> **Degaussing** the drive (using electromagnets to change the drive's magnetic fields, or 1s and 0s, which can be expensive and requires drive disassembly)
> Drilling through the drive platters (see Figure 18.31) and then destroying the pieces with a hammer
> Using a machine designed to destroy drives (see Figure 18.32)
> Shredding the drive by using a machine that divides the drive platters into small pieces

Specific requirements such as the HIPAA Privacy and Security Rules might need to be examined. For example, if non-sensitive protected health information (PHI) is on a drive, securely erasing the data is fine, but if sensitive information is on there, the drive has to be degaussed.

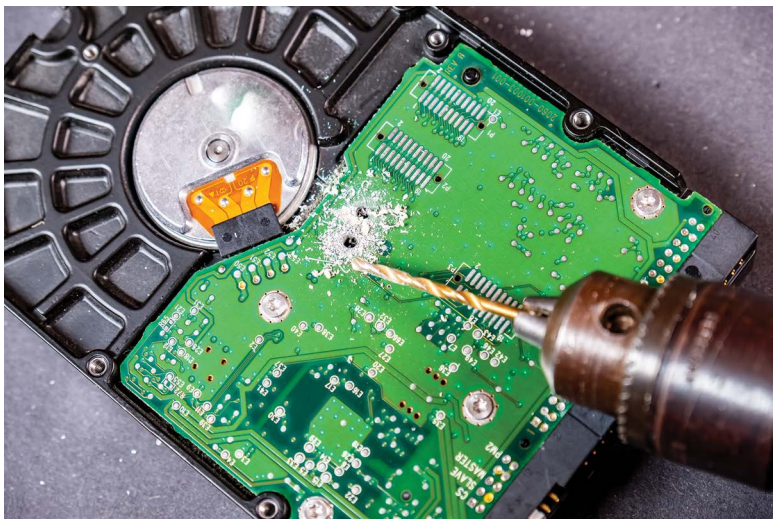


FIGURE 18.31 Drilled hard drive platter

FIGURE 18.32 Hard drive/SSD destroying machine with destroyed drive

Internet Security

Internet security basics are covered in Chapter 12, "Internet Connectivity, Virtualization, and Cloud Technologies," in the "Basic Web Browser Issues" section. This section goes into more technical detail. First, no system should connect to the internet without antivirus and anti-malware software installed. These applications are your first line of defense for internet security, but they are not foolproof.

Second, pay attention to the security alerts provided by antivirus and anti-malware software, browser applications, and the operating system! If you see a message that you haven't seen before, write it down, take a screenshot of it, and research it. Even if you have seen it before, it's a good idea to research and ensure that nothing new is the problem.

Lack of money is not an excuse for not having antivirus software. Microsoft Defender (formerly Windows Defender) is included in Windows 10/11 and has virus scanning capabilities (via **Microsoft Defender Antivirus**, which is compatible with other antivirus products), or another free antivirus program can be downloaded. To activate Microsoft Defender Antivirus, use the *Windows Security* link from within *Settings* > *Update & Security* > *Windows Security* button > *Virus & threat protection* > scroll down to the *Microsoft Defender Antivirus options* link > ensure the *Periodic scanning* option is set to *on*, as shown in Figure 18.33.

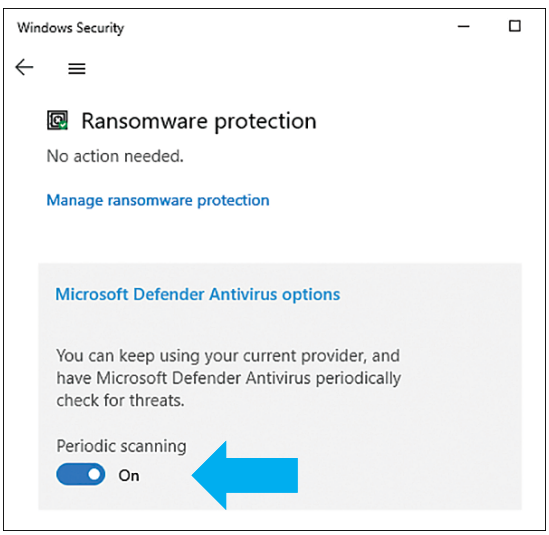


FIGURE 18.33 Microsoft Defender Antivirus activation

You can use the setting *Check for updates* to check for updated definitions. If you use a free antivirus program, ensure that you obtain it from a reputable download site. Beware of **rogue antivirus** applications that pretend to be legitimate software to help you with a computer problem but are actually viruses.

Digital Security Certificates

A digital certificate authenticates and secures information. The certificate authority (CA) is the sender (the device or person who originated the communication). A digital certificate typically contains a public key (a key used with a private key so that messages can be unencrypted), sender information, and the length of time the certificate is to be considered valid. Browsers sometimes present security warnings related to certificates. The following are sample messages:

- The security certificate presented by this website was not issued by a trusted certificate authority.
- www.hacker.com uses an invalid security certificate. The certificate is not trusted because the issuer certificate is unknown.

> The security certificate has expired or is not yet valid. The certificate for the website has expired, the time/date on the server is incorrect, or the time/date on the client computer is incorrect.

> www.watchout.com uses an invalid security certificate. The certificate is not trusted because it is self-signed.

Use the Microsoft **Certificate Manager** (`certmgr.msc`) to see details about certificates. There you can view, modify, import, export, or delete a security certificate. Use the arrows on the left to expand a category. Right-click on any specific certificate to see options, as shown in Figure 18.34.

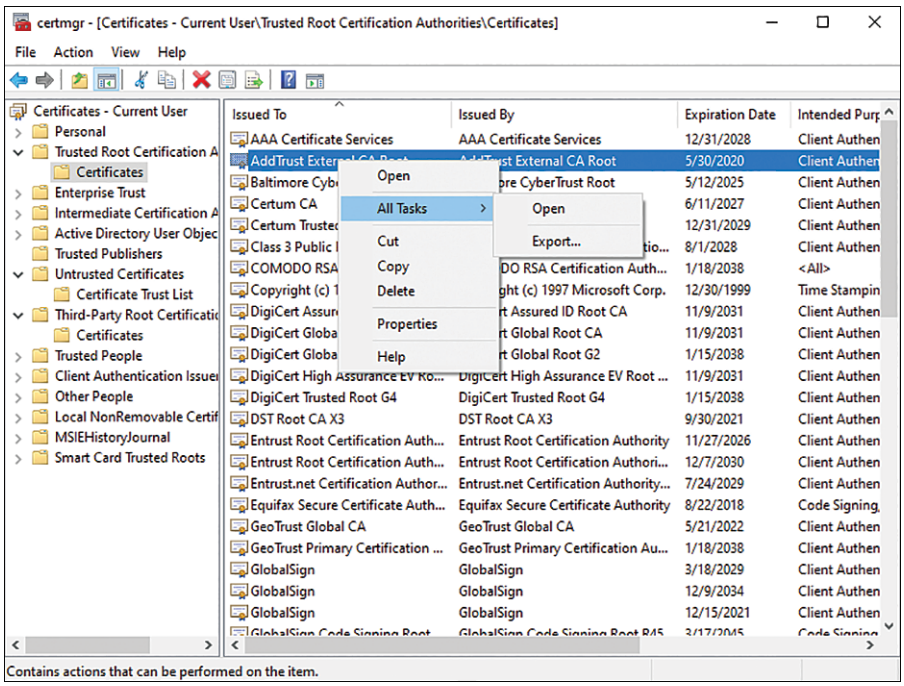


FIGURE 18.34 Microsoft Certificate Manager

If a user visited a website that should have been avoided, close the browser. Reopen the browser and use the security settings within the browser to delete a certificate that was trusted but shouldn't have been.

Malware Removal

Malware symptoms are numerous. A device may run slowly, crash, or lock; applications might behave abnormally or not at all; you might experience disappearing or missing files; you might see file attribute or file permission changes; there might be constant storage device activity or constant (greater-than-normal) network activity; your email might be hijacked (in which case you should change your password to something totally different as soon as you notice); you might get access denied messages or security messages; and you might experience removed, corrupted, or renamed system files. (Note that access denied messages are sometimes normal if a user account does not have administrative permissions to do a particular task.)

If malware has infected a system's boot sector, you may have to use the Recovery Console on older Windows computers, use Safe mode, use a boot disk to run anti-malware, or even reinstall the operating system. For anti-malware, Microsoft provides the Malicious Software Removal Tool for free. Other vendors provide free anti-malware software, too. It is easier to deal with such issues

with security software installed than without it. The following steps are best practice procedures for malware removal:

Step 1. Investigate and verify malware symptoms. Do not act based only on a customer's word that they have a virus or malware. An application could be the culprit, or something else entirely might be happening. Be sure to log all actions performed.

Step 2. Quarantine the infected system. Disconnect the system from the network or disable the wireless NIC. Do not power off the computer or reboot it.

Step 3. For Windows Home machines, disable *System Restore*.

Step 4. Remediate the infected system (see Figure 18.35). You might need to update the anti-malware software or might have to use another system to research your support options from your antivirus/anti-malware software vendor. Rescan the system for security issues using the updated software. Some antivirus software vendors have images that can be downloaded and used to create bootable antivirus discs or flash drives.

If the system still performs strangely, boot into Safe Mode and run the virus checker from there. Use the `msconfig` utility to isolate a startup application or service that might be causing the issue. If you purchased an antivirus disc, run the software from the optical disc. Boot from an alternative boot source (flash drive, external hard drive, or operating system disc).

With some worms and Trojan horse viruses, files must be manually deleted because they cannot be repaired, but the antivirus software will quarantine such files so they cannot be dangerous and affect other files. If it an executable file is quarantined, you may have to reinstall one or more apps. A hijacked web browser—which may occur, for example, when the requested web page is redirected to a different web page—may require browser configuration, different DNS settings, or a new or updated HOSTS file applied after removal. You might be required to use the `SFC /scannow` command to replace/repair operating system files after removing a virus. You also may have to reimage the computer or reinstall the OS. Finally, test all apps to ensure that they operate. Then manually delete any files that are quarantined.

Step 5. Schedule antivirus/anti-malware scans and run updates.

Step 6. For Windows Home-based computers, re-enable *System Restore*. Create a new restore point.

Step 7. Educate the user on security best practices.

FIGURE 18.35 Remediating an infected system

TECH TIP

Manually delete files, if necessary

If antivirus software or other preventive software applications state that a particular file cannot be deleted, make a note of the file and its location. File Explorer *View* options may have to be adjusted before viewing/deletion can occur.

DNS Issues

Domain Name System (DNS) is used to translate a URL to an IP address. Homes and small businesses almost always use the DNS server of the internet provider. A medium to large company may have its own DNS server, might use the internet provider's, or might pay for another company to host a DNS server. DNS is a common security target because an attacker can use it to redirect a web browser to another website that is under the control of the attacker.

If you suspect that the DNS server has been compromised because your browser is redirecting you to unusual websites, you can't access the internet, or URLs don't look quite right, you can change your DNS configuration setting to another DNS server just to see if the symptoms change. In a router, the setting is commonly found in the Setup or Basic Settings section. In Windows, use the *Network & Internet* Windows *Settings* link to access the NIC being used > *Edit* button in the *IP settings* section > ensure that the IPv4 setting is manually being set and configure *Preferred DNS* and *Alternate DNS*, as shown in Figure 18.36.

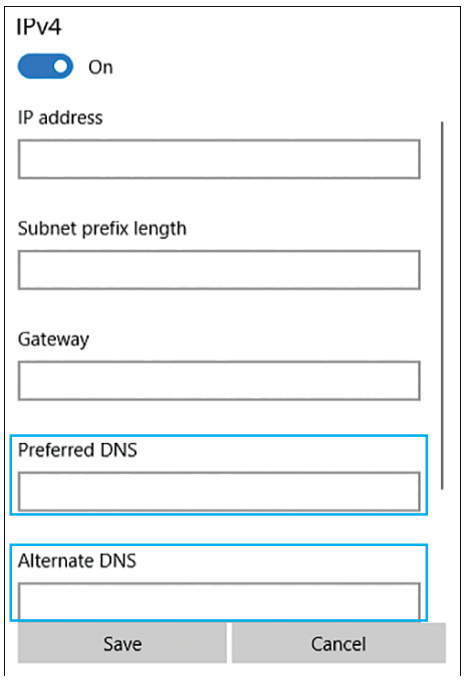


FIGURE 18.36 Manual DNS IP address configuration

OpenDNS offers free and fee-based configurations. The following IPv4 and IPv6 addresses can be used:

IPv4 OpenDNS addresses:

> 208.67.222.222
> 208.67.220.220
> 208.67.222.220
> 208.67.220.222

IPv6 OpenDNS addresses:

- 2620:119:35::35
- 2620:119:53::53

In addition, OpenDNS FamilyShield uses two addresses to automatically prevent adult websites from being accessed:

- 208.67.222.123
- 208.67.220.123

If you suspect DNS server issues, clear the browser history/cache using the directions below or by researching the browser being used:

- **Edge:** *Settings* (gear) icon > *Privacy, search, and services* > *Clear browsing data*
- **Firefox:** *Open menu* icon in top-right corner > *Settings* > *Privacy & Security* > in the *History* section > *Clear History*
- **Chrome:** *Customize* (three vertical dots in the top-right corner) > *Settings* > *Settings* menu on left > *Privacy and security* > *Clear Browsing Data* link > *Clear Data*

You should also clear the DNS cache on the computer. On a PC, access a command prompt and, as an administrator, type `ipconfig /flushdns`. On a Mac, access *Terminal* and type the following two commands:

```
sudo dscacheutil -flushcache
sudo killall -HUP mDNSResponder
```

A best practice in the corporate environment is to use **secure DNS** to protect (encrypt) DNS requests and prevent DNS cyber attacks. There are several ways to do this:

- Use a secure DNS server by enabling DNS security extensions (DNSSEC) that use security protocols to digitally sign DNS records and provide a chain of trust.
- Enable either DNS over TLS (DoT) or DNS over HTTPS (DoH) to encrypt DNS requests.
- Use a secure DNS provider.
- Use a secure DNS app.
- Implement DNS filtering to deny access from malicious websites.
- Use multiple DNS servers.

Email Issues

Email has its own section in this chapter because it is something most people deal with on a daily basis. Avoid checking email on a public computer or on an unsecure network as doing so may lead to your email account being hijacked; if this happens, you will not be able to log in using normal procedures, you may get an automated message from an unknown person as if it were an automated response to your own email, people in your contacts might send you a note about constant emails or spam from the hijacked account, or your account might have a lot of undeliverable emails. For an account that has been hijacked, perform the following steps:

Step 1. Contact the email provider to report the problem.

Step 2. Ensure that Windows, antivirus, and anti-malware updates have been applied.

Step 3. Ensure that you have an alternative email account available for when you have to register with sites, such as for online shopping.

Step 4. Try logging in to the account from a different computer to see if the email settings have been changed. (If you can get to the account, change the password.)

Step 5. Create rules in your email account to delete files from specific nontrusted sources.

Security rules can be used to process incoming email messages before putting them into specific users' email inboxes. These rules search for and remove suspicious and harmful emails, and they may potentially scan outgoing emails to ensure security or legal compliance.

Spam is unsolicited email from a previously unknown company or person. The spam folder in a user's email inbox provides evidence of such filtering. Technical staff must sometimes remind users to check the spam folder for email that was sent from an external source. Most email applications have spam filters, but they do not catch all spam. Most email applications also enable you to create a rule to block messages from particular sources or with specific subject lines. Figure 18.37 illustrates the concept of a spam filter.

A company may use a **spam gateway** to remove spam emails before they are processed by the email server. A similar approach is to use an **email security gateway** (ESG), sometimes called a security email gateway (SEG), which uses machine learning and artificial intelligence to check for spam, phishing, malware, and so on in all incoming and outgoing emails. Some ESGs can provide data loss prevention (DLP) so that particular corporate information is not sent. Having outbound filters in place also prevents a business from being blocklisted due to having a high level of spam being sent from the business.

FIGURE 18.37 Spam filtering

Email apps use **DNS TXT** messages to try to determine if a message is from a trusted domain. Spammers often use false domains to send emails. Several authentication methods can be used to authenticate email messages:

> **Domain Keys Identified Mail (DKIM):** Used by email providers like Gmail, AOL, and Yahoo to electronically sign emails so the receiving server knows that they are legitimate messages.

> **Sender Policy Framework (SPF):** Designates authorized mail servers that legitimately send email for a specific domain.

> **Domain-based Message Authentication, Reporting, and Conformance (DMARC):** Used if an email message does not pass SPF or DKIM to ensure that the sender of the email matches and determine what to do with messages from unknown or unauthorized senders.

Another email problem is email messages sent in clear text. If such a message is intercepted, it is easy to read. Pretty Good Privacy (PGP) and Secure Multipurpose Internet Mail Extensions (S/MIME) are frequently used to provide encryption and authentication for email messages.

Proxy Servers

A company may use a **proxy server** to protect its network. This server acts as an agent (a go-between) between an application such as a web browser and a remote server. A proxy server can also cache frequently accessed web pages and provide them when requested from a client instead of accessing the web server. A proxy server is commonly located with other network servers in a corporate network design, as shown in Figure 18.38.

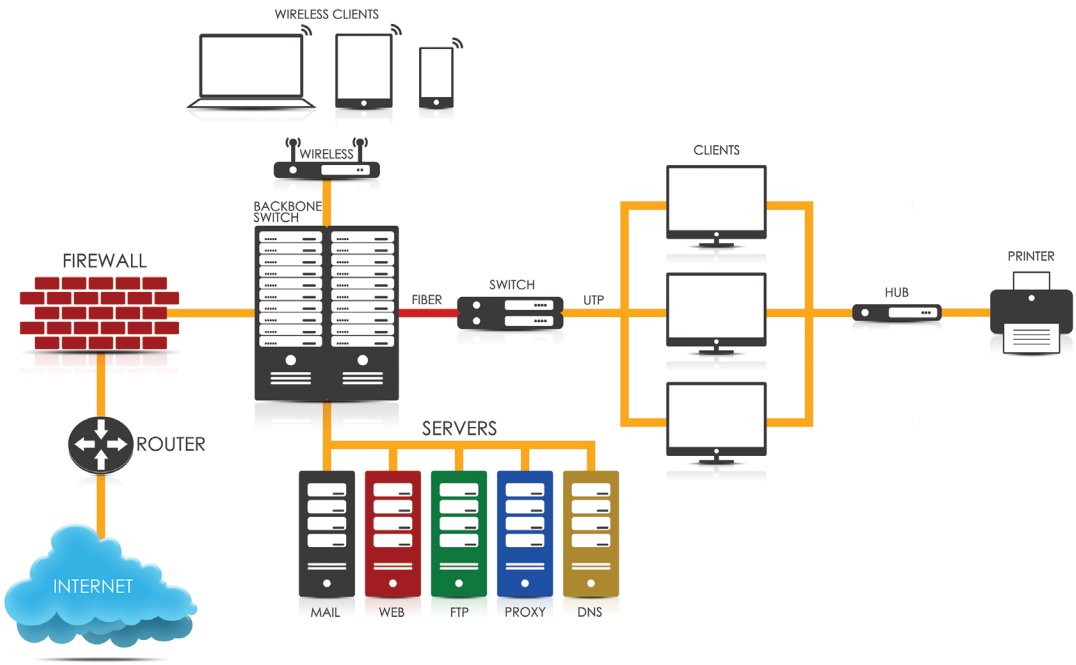


FIGURE 18.38 Proxy server

All traffic from corporate wired and wireless devices that is being sent to the internet will be directed to the proxy server. The proxy server will then change the source IP address to its own address and send that traffic to the internet. When the traffic returns from the internet, the traffic will be sent to the proxy server (not the original device); the proxy server then forwards the traffic to the original network device.

To configure any device or application to use a proxy server, obtain the following information from the company's network administrator or through the Web Proxy Auto-Discovery protocol:

> IP address of the proxy server
> Port number of the proxy server
> Optionally a username and password (although some organizations use server-based authentication)

Use the *Network & Internet* Windows *Settings* link > *Proxy* and locate the *Manual proxy setup* section. Improperly configured proxy settings may cause a computer to be redirected to an invalid website with no internet connectivity.

Firewalls

If a computer connects to the internet, it should be connected behind a firewall. No computer should be unprotected and missing a firewall as this is software that comes with the operating system. A firewall protects one or more computers from outside attacks and is used to implement security policies. The concept of a firewall is similar to the concept of a moat with a drawbridge protecting a castle. The castle is the inside network, the moat with the drawbridge is the firewall, and everyone outside the castle is an "attacker." The drawbridge controls access to and from the castle.

TECH TIP

Antivirus and anti-malware applications are needed even when a firewall is installed

A computer protected by a firewall still needs antivirus and anti-malware applications for protection. Having a firewall on each computer as well as on a router or modem that connects to the internet (or a device dedicated to providing firewall services) is common in both home and business environments.

A firewall can be either a software application or hardware, and it should be implemented for any computer that connects to another network, especially a computer that connects to the internet. A firewall keeps hackers from accessing a computer that connects to the internet. A software firewall is a Windows tool or software application that is a good security solution for individual computers. A hardware firewall is a good solution for home and business networks. Hardware and software firewalls can be used concurrently. With any firewall, any ports that are not used should be disabled.

Allow Lists and Deny Lists

A security concept related to firewalls is allow lists and deny lists. Security measures are commonly implemented based on one of these two methods. An allow list implementation is based on a list of who is allowed in through the firewall to use a VPN, use an application, enter a secured network closet, and so on. An easy way to remember the allow list method is to think of your front door at home. Anyone who has a key to the door is allowed in; each person with a key is on the allow list.

On the other hand, a deny list details what users or websites are not allowed. Anyone or any site that is not on the deny list is allowed in. To remember the deny list method, think of a college's list of people not allowed on campus or the list of blocked calls on your cell phone.

DMZ

In a corporate environment, a firewall, router, or wireless router can be used to create an area called a demilitarized zone (**DMZ**), also known as a screened subnet, that might be in a home or in a small office/home office (SOHO) router configuration. Servers such as web servers or application servers can reside in the DMZ (see Figure 18.39). Customers can use a server within the DMZ without having to be let into the part of the network where the sensitive corporate data resides. A DMZ might also be used to separate Internet of Things (IoT) devices from the rest of the network.

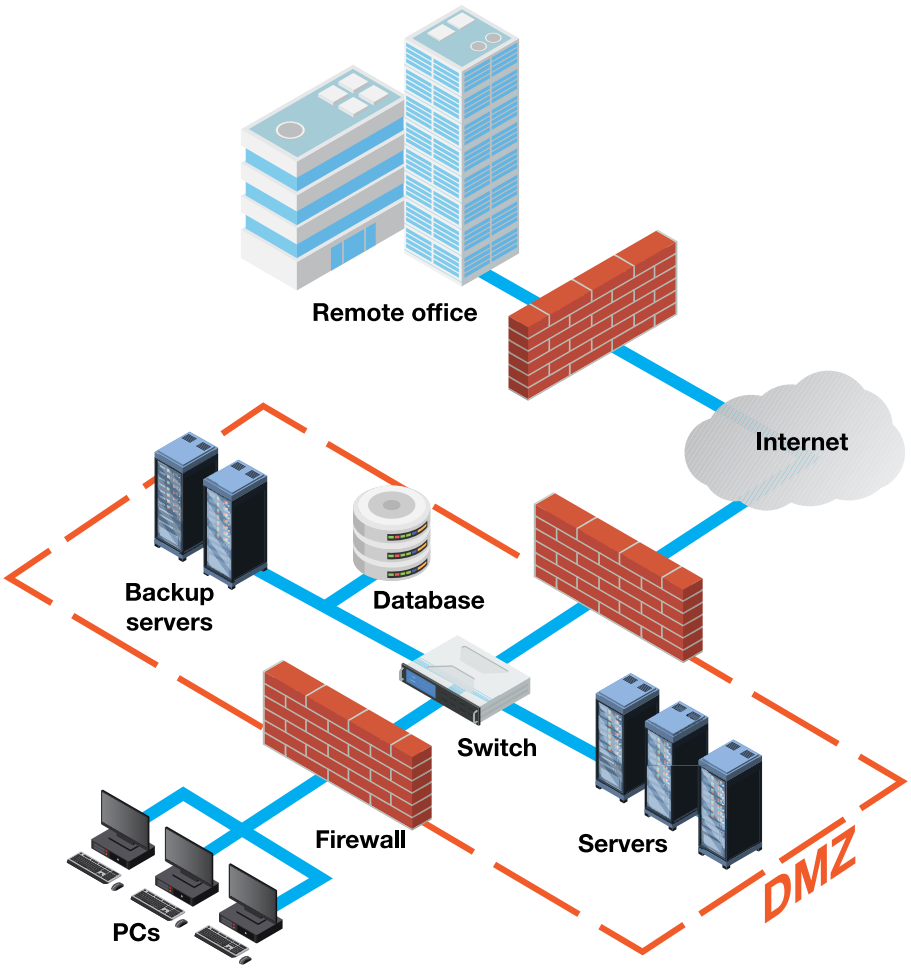


FIGURE 18.39 DMZ

Universal Plug and Play

Universal plug and play (**UPnP**) is used to set up a network with very little configuration, such as a home network. Devices such as a home router, printers, PCs, and mobile devices can all be configured for UPnP, and the devices discover each other. Note that this setting is commonly found in an Administration or Advanced tab or section and might be enabled by default. On a Windows computer, when you enable *Turn on Network Discovery* in the *Network and Sharing Center* Control Panel > *Change Advanced Sharing Settings* option, you are enabling UPnP.

Windows Firewall and Advanced Security

Windows displays messages and warnings related to security and maintenance. To control the types of messages that appear, access *Settings* > *System* > *Notifications & actions* > *Get notifications from these senders* section and ensure that the *Security and Maintenance* option is set to *On*.

Part of the Windows Security app is **Windows Defender Firewall**, which is a local or host-based firewall that is just for the one system. The firewall allows or blocks inbound/outbound traffic based on rules that have been configured automatically for the network profile (domain, public, or private) being used currently by the system and viewable using the *Update & Security* Settings link > *Windows Security* app > *Firewall & network protection* Windows Security app link. For example, if a corporate laptop connects to the organization domain through a wired Ethernet connection, the domain security settings might be less restrictive than if the laptop wireless is being

used at an airport and the public security settings are in effect and are more restrictive. These are the types of profiles you see in Windows:

> The *Private (Home or Work)* profile turns on file sharing and network discovery through the firewall, so communication will be easier at work or in a private home network.
> The *Guest* profile or *Public* profile configures settings in the firewall to help protect a computer when on a public network such as when you are in an airport.
> With the *Domain* profile, the computer participates in a Windows Active Directory domain environment.
> The *All Networks* profile includes private folder sharing, media streaming, file sharing, and password-protected sharing options that can apply to all types of network connections.

Settings can also be accessed/configured through the *Windows Defender Firewall* Control Panel. Figure 18.40 shows the expanded network profiles.

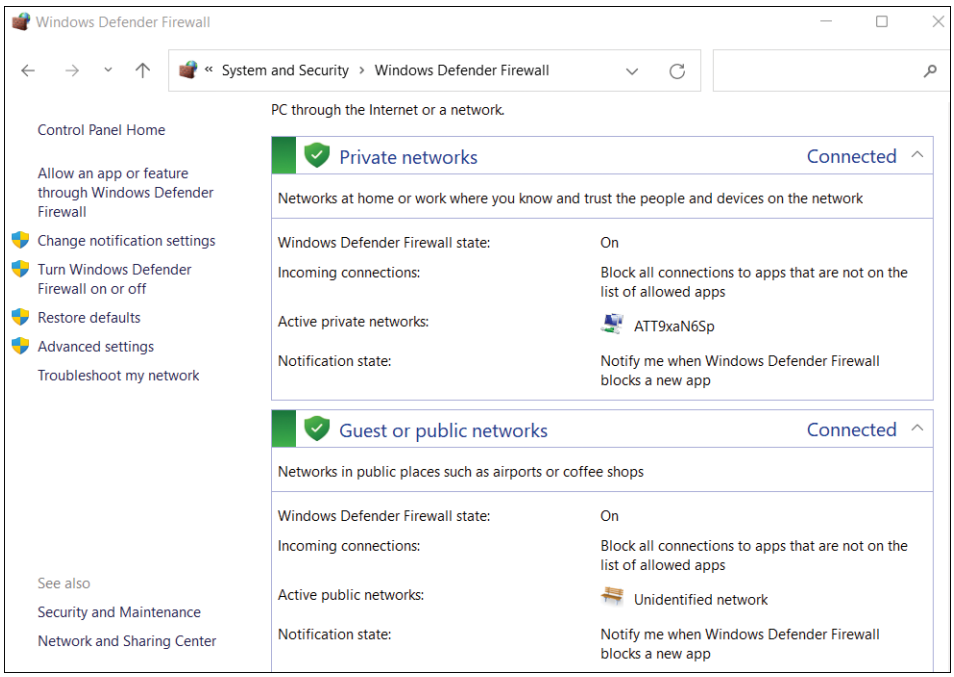


FIGURE 18.40 Windows Defender Firewall profile settings

Notice how each of the profiles shown in Figure 18.40 appears with a green checkmark. This means the firewall is activated or active. A red background with an X over it indicates that the firewall is deactivated. Use the *Turn Windows Defender Firewall on or off* link on the left to change the state.

TECH TIP

Be sure you work with the correct profile

If you cannot access devices and resources that are normally available through the wireless NIC, ensure that the correct location profile is used. Access the *Change advanced sharing settings* link from the *Network and Sharing Center* Control Panel. The profile used will have the following words after the profile name: *(current profile)*.

When Windows Defender Firewall is installed and enabled on a Windows computer and another computer or application tries to connect, Windows Defender Firewall blocks the connection and prompts with a security alert to allow a choice of *Allow access* if an app is trusted or Cancel *to keep it blocked*.

TECH TIP

Allowing an application through Windows Defender Firewall

Open the *Windows Defender Firewall* section of the Control Panel > select the *Allow an app or feature through Windows Defender Firewall* > *Change Settings* > enable the checkbox beside the app you want to allow and select the network types this applies to > *OK*.

Port forwarding is a term used for a packet allowed through a firewall based on a particular port number/protocol. Port triggering is a similar concept. Port triggering allows data into a computer temporarily, based on a configured situation. To configure Windows Defender Firewall to allow inbound traffic for a specific TCP/UDP port number (that is, to configure **port security**), use the *Advanced settings* link > *Inbound Rules* > in the *Action* column select *New Rule* (see Figure 18.41) > select the *Port* radio button. The *Outbound Rules* link can be used in the same manner for a specific port.

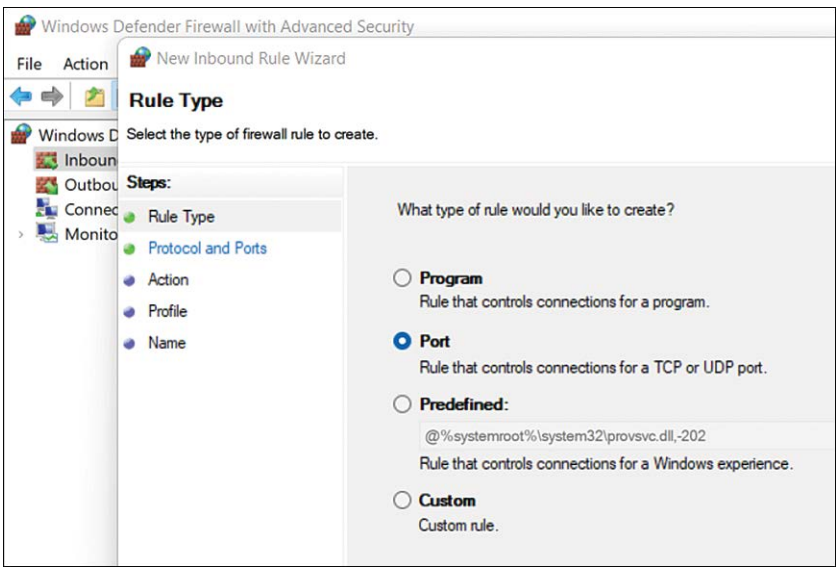


FIGURE 18.41 Configuring Windows Defender Firewall rule for a specific port number

Table 18.14 shows Windows Defender Firewall issues and solutions to help with troubleshooting.

TABLE 18.14 Windows Defender Firewall and advanced security troubleshooting

Windows Defender Firewall issue	Resolutions
The firewall is blocking all connections.	Access Windows Defender Firewall and disable the *Block All Incoming Connections* checkbox.
The firewall is blocking a specific application.	If a dialog box appears, select the *Unblock* option to allow it through. If the dialog box does not appear, access Windows Defender Firewall and use the *Exceptions* tab to create a rule that allows the application through the firewall.
No one can ping a Windows computer.	Ensure that *File and Print Sharing* is enabled through the *Network and Sharing Center* Control Panel. Access the *Administrative Tools/ Windows Tools* link and select *Windows Defender Firewall with advanced security*. Select *Inbound Rules* in the left pane. Select *New Rule* in the *Actions* column. Select the *Custom* radio button and *Next*. Select the *All programs* radio button and click *Next*. Select *ICMPv4* from the *Protocol Type* drop-down box. Select the IP addresses to which this rule will apply and name the rule.

Windows Defender Firewall issue	Resolutions
Windows Firewall is turned off every time the computer restarts.	Another security firewall is installed.
No one can access local files and/or a shared printer.	File and Print Sharing has not been enabled.

Freeware programs are available, as are full security suites (such as the ones from McAfee or Symantec) that include software firewalls and components to prevent malicious software applications from executing.

NAT/PAT

Companies use private IP addresses (192.168.x.x, 172.16.x.x through 172.31.x.x, 10.x.x.x) on devices inside the company, but these addresses cannot be routed on the internet. A network device such as a router or firewall performs network address translation (**NAT**), which means it translates private IP addresses to public addresses that can be routed over the internet. If NAT/PAT is not working, internet access is unavailable.

With port mapping, one public address can be used for multiple internal company connections. **Port mapping** allows the combination of one public address and a specific port number to represent one internal company host. The same public address and a different port number represent a second internal company host. Some people also call this concept, which is illustrated in Figure 18.42, port forwarding or port address translation (PAT).

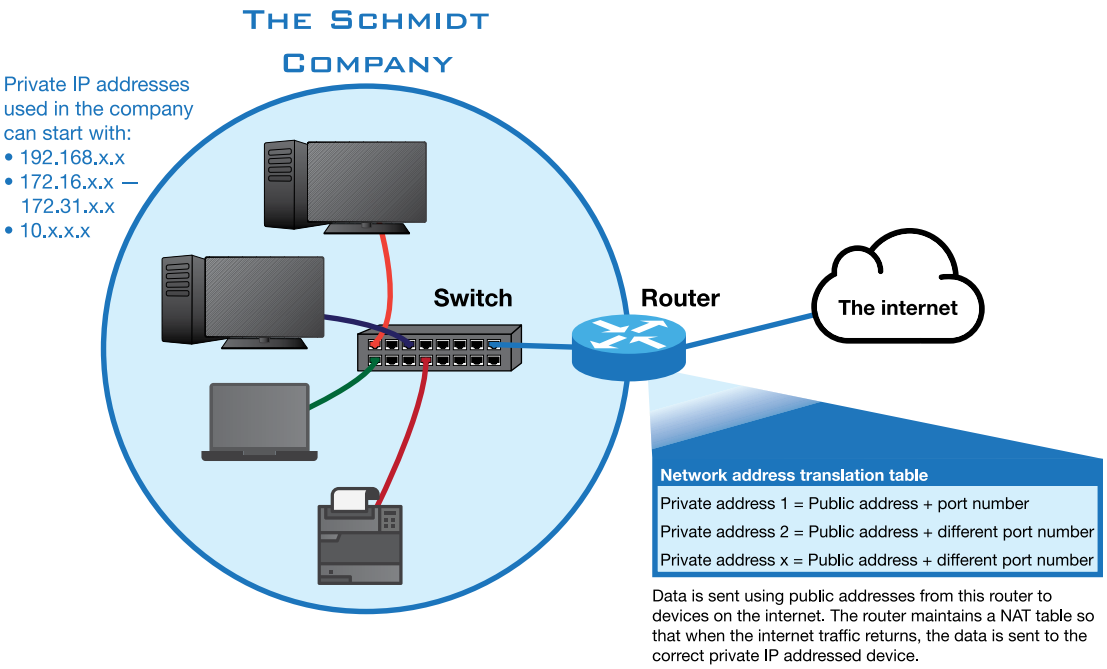


FIGURE 18.42 Network/port address translation

Remote Access to Network Devices

Corporate users commonly work from home or travel and need to access printers, servers, and other devices within the company. Technicians commonly use remote desktop or third-party tools in order to perform troubleshooting and repairs. Let's explore the protocols used to do remote access, the methods used, and how security is handled.

Remote Access Techniques

Several techniques, protocols, and apps are used to remotely access devices. With any technology used to remotely access a network device, there are risks in that someone may pose as a legitimate company or department and gain access or even convince users to provide specific company files. Most companies limit the ability to remotely access devices on the corporate network. Remote access technologies are described in Table 18.15, along with security concerns.

TABLE 18.15 Remote access technologies and security concerns

Remote access technology	Description	General or security concerns
Quick Assist	Allows a user to view or remotely control another computer; may need to enable this app in *Apps > Optional features*	This app requires an internet connection. The invitation could be from a threat actor and include a modified invitation file that infiltrates the target computer, if accepted.
RDP (Remote Desktop Protocol)	Creates a peer-to-peer remote desktop connection from one computer to a remote computer. You might have to enable port forwarding (see Chapter 13, "Networking") and allow port 3389 in order to connect to the remote device.	Reported security issues should be taken into consideration before using RDP.
SSH (Secure Shell)	Uses port 22 to securely log in to a remote network device. Is better than using Telnet.	There are security vulnerabilities with version 1. Use SSH version 2.
Telnet	Uses port 23 to access a remote device on the network, such as a router, a server, an access point, or a switch.	Telnet uses clear text to send data and passwords. Telnet should not be used unless the network device supports no other remote access protocol.
VNC (virtual network computing)	Uses one computer as a "server" and another computer as a "viewer" to access the other computer.	The viewer and server software must be downloaded. Some versions cost money. It is important to ensure that the firewall is configured to allow this connection through.
SPICE (Simple Protocol for Independent Computer Environments)	Used to remotely access and control VMs	This open source protocol requires a guest agent to be running on the VM. It supports TLS encryption as well as authentication mechanisms between the server and a client.
WinRM (Windows Remote Management)	Allows remote Windows computer management. Requires the service to be running on the destination computer.	The firewall must be configured to allow the connection through. It supports encryption and authentication.

Remote access technology	Description	General or security concerns
VPN (virtual private network)	Enables a special type of secure connection from one network device to another. Can be provided as a service.	A VPN can slow internet access. You can also be infected with malware from a provider. Because VPNs support multiple authentication and encryption protocols, choosing a weak protocol could be a risk. (See the next section, "VPN Configuration.")

Because of the security shortcomings of remote access technologies, companies use third-party remote monitoring and management (**RMM**) tools to share a screen with a user in order to troubleshoot a specific problem or transfer files. Specific file transfer software may also be used. A technician may also use videoconferencing software like Cisco Webex, Google Meet, or Microsoft Teams to be able to talk to the user as they are working on the computer. Examples of remote access software include LogMeIn Rescue, TeamViewer, Zoho Assist, AnyViwer, Splashtop, Radmin, RealVNC, and Highfive. Furthermore, a company may use a specific desktop management software/server that makes supporting and controlling corporate PCs easier in terms of remote imaging/reimaging, OS/app updating, inventory control, and security.

VPN Configuration

VPNs can be used in a variety of ways. One example is a home PC that connects to a corporate server and has access to company resources that cannot otherwise be accessed except by being on a computer on the inside network. The VPN connection makes it appear as if the home computer is on the inside corporate network. Another example is a branch office network device connecting to a corporate server, VPN concentrator, firewall, or other network device. When connected, the branch office network device connects as if it were directly connected to the network. Figure 18.43 illustrates the concept of a VPN.

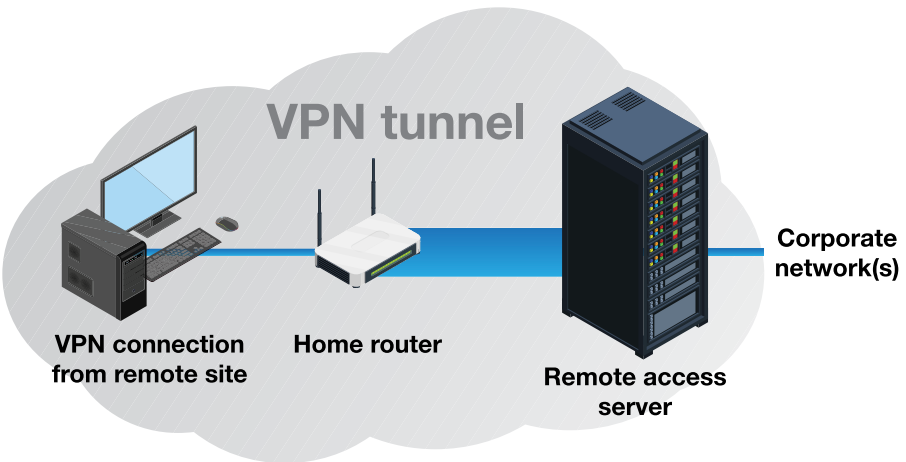


FIGURE 18.43 VPN connectivity

VPNs (virtual private networks) serve multiple purposes beyond security. They allow for anonymous browsing by masking a user's IP address and can bypass network restrictions, enabling access to blocked content. VPNs also provide access to geographically restricted media and secure public Wi-Fi connections by encrypting internet traffic. In addition, they allow for anonymous file downloads, which makes them a valuable tool for managing an organization's online presence and security. It is even possible to set up a computer to serve as a VPN server. Before configuring the

VPN, you should know which protocol you will be using on both sides of the connection: PPTP, L2TP/IPsec, SSTP, or OpenVPN.

TECH TIP

Both sides of the VPN tunnel must match

The two devices used to create a VPN tunnel must have identical VPN settings, or the VPN tunnel will not be formed.

To configure a VPN in Windows, you must have a VPN profile configured through Control Panels or Settings:

> Use the *Network and Sharing Center* Control Panel > select the *Set up a new connection or network* link > *Connect to a workplace* > *Next* > *Use my Internet connection (VPN)* > enter the IP address or fully qualified domain name of the network device on the other end of the VPN connection > *Next* > enter the required credentials > click *Connect*.

> An alternative is to use *Settings* to access the *Network & Internet* link > *VPN* > *Add a VPN connection* > use *VPN provider* to select *Windows (built-in)* > type a name in the *Connection name* textbox > type the IP address or name of the other end of the VPN connection in the *Server name or address* textbox.

Internet Appliances

An important strategy for servers, apps, and network traffic is the use of a load balancer. A **load balancer** is used when you have redundancy in the network. For example, if you have multiple servers for the same app, the load balancer can direct traffic so that one particular server doesn't get overloaded. A load balancer can be a piece of hardware, deployed as a virtual appliance, or it can be used in a cloud environment. A load balancer can work using different types of algorithms, including these:

> **Least connections:** Tracks how many active connections are used on a particular device and sends traffic onward to the one that has the smallest number of connections.

> **Least response time:** Tracks the number of connections as well as the average response time in order to forward traffic onward.

> **Round robin:** Sends traffic to each device, one after another, much as a card dealer deals cards to players. This is a good method to use if all the receiving devices are equal in their capabilities.

> **Weighted round robin:** Similar to round robin except weighting values can be given so that a particular device that has more capabilities is sent more traffic.

Other devices that an IT staff member should be familiar with include the UTM, IDS, and IPS. A unified threat management (**UTM**) system is a single device that commonly provides multiple security functions such as content filtering, antivirus, antispyware, anti-malware, firewall, and intrusion detection and prevention. The device might also have the capability to route, accept VPN connections, and provide NAT. **Content filtering** involves using a device or security software to screen data for specific web addresses, websites, web domains, emails, or files that are defined as being suspect. This is similar to applying parental controls on a home Windows computer.

An intrusion detection system (**IDS**) is hardware or software that constantly monitors and scans network traffic for malicious traffic or violations of defined security policies. An IDS is considered

a passive system; it doesn't take action but just detects and sends data, reports, and alerts to the network management team (see Figure 18.44). It is like a babysitter whose job is to just tend to the kids (the network data). If there is a fight (a security threat), the babysitter notifies the parents (the network personnel), who deal with the problem.

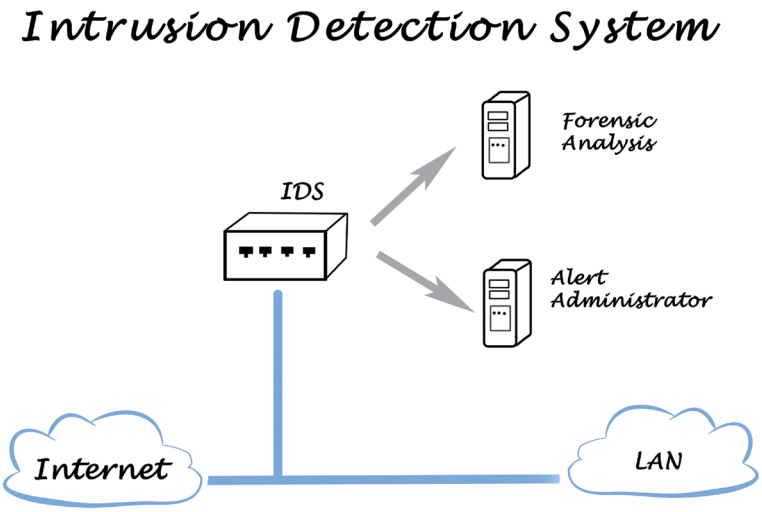


FIGURE 18.44 IDS

A device that is similar to an IDS is an intrusion prevention system (**IPS**). An IPS is an active system; it constantly monitors and scans network traffic for malicious traffic and violations of security policies, and it takes appropriate action, such as sending an alarm, resetting connections, blocking traffic, disabling ports, or dropping packets. An IPS is like a school teacher who is serving as a hall monitor and can issue detentions, break up fights, and restore order to the hallway.

Sometimes, an IDS and an IPS are both used in a network design, with the IDS inspecting the network traffic and reporting the information and the IPS taking preventive action.

Wireless Network Security Overview

Traditionally security has been a concern when installing wireless networks because originally security was disabled by default, and there was lack of knowledge about default passwords and misconfigured wireless settings. Wireless LANs (WLANs) are much more secure today than when they first began to be used.

Wireless access points (APs) are an integral part of a wireless LAN and are normally mounted on the ceiling or on a wall where they are inconspicuous. Sometimes they are mounted in or above the ceiling tile in a special enclosure.

Data transmitted over air can be in clear text, which means that with special frame capturing software (packet sniffers or analyzers) on a computer with a wireless NIC installed, the data can be captured and viewed. Negotiation between the wireless devices and the AP can be in clear text so that information can be captured. Every frame includes a source MAC address. Someone with a wireless device and free hacking software can capture the frame to use the MAC address to gain access to other resources—although hackers are not usually this obvious. (This is known as session hijacking or MAC spoofing.) By default, most APs transmit their SSIDs in clear text. All these issues must be considered when installing a wireless network.

TECH TIP

How a firewall helps a wireless computer

A firewall can protect a computer connected to a wireless network; however, the firewall cannot prevent the outgoing wireless data from being hijacked. The firewall simply protects a hacker from accessing the computer.

Mobile Device Management

Mobile device management (**MDM**) can help with security by enabling a technician to view and manage mobile devices (see Figure 18.45). MDM software can be used to push application updates, enforce security policies, track devices, or remotely wipe data or the operating system from a device. A tracking module is available on some mobile devices and is used to track the device and provide recovery/wiping options that can be used in the event that the device is lost or stolen. **Configuration profiles** may be used to define wireless networks or VPN settings and preconfigure apps, app settings, and device encryption settings.

MDM policies vary from one company to another, but they commonly define operating systems supported as well as password and security requirements. Optional related policies might include the following:

- Password storage
- Software/firmware installation
- Application updates
- System updates
- Backup process
- VPN connectivity
- How to report lost or stolen devices
- Steps involved when a security breach occurs
- Data storage

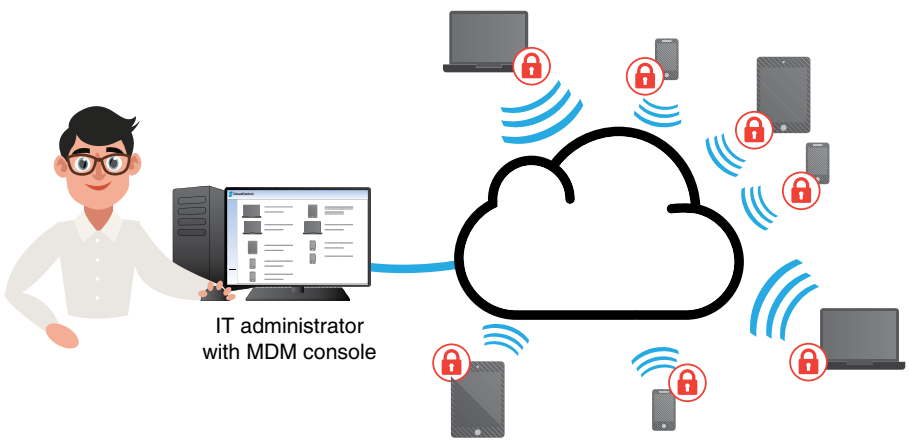


FIGURE 18.45 Mobile device management (MDM)

Wireless Security

Security on wireless devices has always been a concern, and several options can be used. These are the most common options:

- WEP
- WPA
- WPA2
- WPA3
- TKIP
- AES

TECH TIP

Mobile device security options must match AP settings

Whatever security is configured on an access point must be used on any mobile device that uses the wireless network.

Wired Equivalent Privacy (**WEP**) encrypts data that is being transmitted. WEP commonly has two versions: 64-bit and 128-bit. With WEP enabled, the shared secret key is normally entered into the wireless NIC configuration window. Vendors have a variety of ways of inputting this alphanumeric key, but normally it is input in either hexadecimal or ASCII characters. WEP can be hacked but may have to be used if one device on the network is incapable of higher-level security.

An improvement on WEP is Wi-Fi Protected Access (WPA), which has been enhanced with newer versions called WPA2 and WPA3. **WPA2** uses Temporal Key Integrity Protocol (**TKIP**) or Advanced Encryption Standard (AES) to improve security. TKIP is an improvement over WEP in that the encryption keys change, and AES is even better than TKIP. WPA2 includes dynamic negotiation between the AP and the client for authentication and encryption algorithms (see Figure 18.46). WPA2 is a common choice for securing wireless networks until all the devices can support WPA3. **WPA3** uses Simultaneous Authentication of Equals (SAE) encryption instead of pre-shared keys, which prevents attackers from using dictionary attacks to gain access to the wireless network. WPA3 also has features that help with on-path (man-in-the-middle) and evil twin attacks.

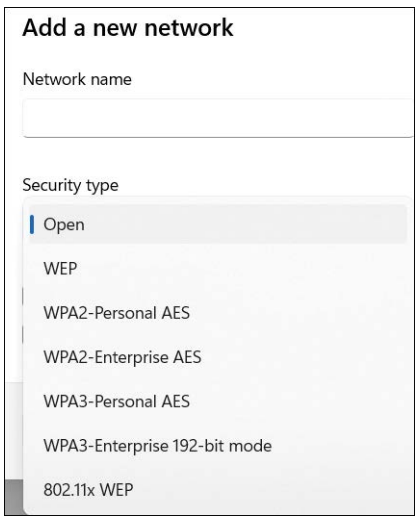


FIGURE 18.46 Windows 11 wireless security options

Figure 18.46 shows the security options available if you are manually adding a wireless network. Figure 18.47 shows the process for manually adding a WPA2 wireless network that has security applied for a Windows 10 computer. Figure 18.48 shows an example of where security encryption is selected on a wireless router.

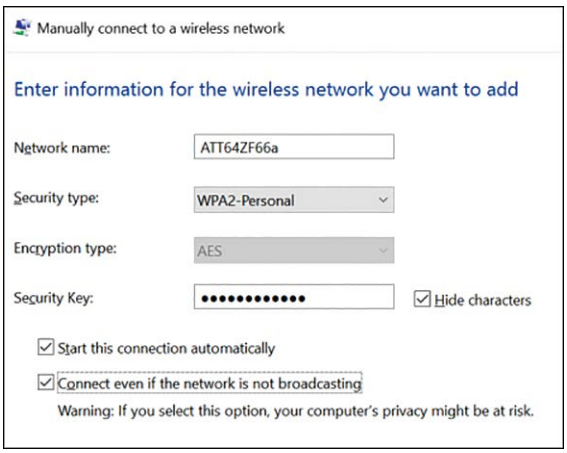


FIGURE 18.47 Windows 10 wireless security window

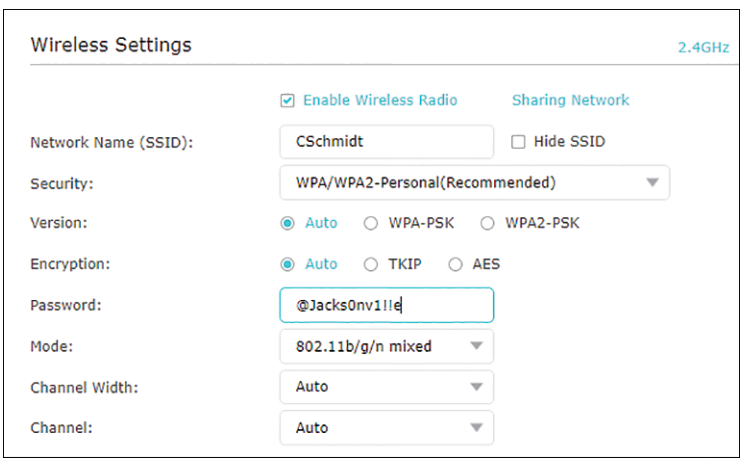


FIGURE 18.48 Sample security window on a wireless router

You can commonly set up a wireless router as a firewall and configure security settings. Some routers allow configuration of a **screened subnet**, also known as a DMZ. Figure 18.49 shows where you enable this and provide the IP address of the server or computer that will be in the DMZ.

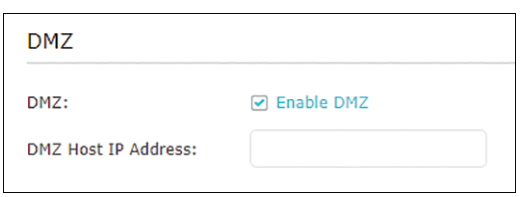


FIGURE 18.49 DMZ configuration on a wireless router

On wireless networks, **MAC address filtering** (also known as MAC filtering) allows only the devices that have been manually entered into the access point to transmit data. MAC filtering is used with a limited number of wireless devices and when those devices' MAC addresses are known by the person who configured the access point. Any new personnel or wireless devices have to be added to the access point manually to use the wireless network.

TECH TIP

Who would use MAC filtering?

Most access points have a limited number of MAC addresses (20 to 50), so MAC address filtering tends to be used only by small companies that want to have strict control of who gets onto the wireless network.

Some wireless routers can be configured for content filtering (also called web filtering, domain filtering, or parental controls), which involves entering websites to block. You can also configure **IP filtering** by either selecting IP addresses that are not allowed or selecting IP addresses that are allowed, as shown in Figure 18.50.

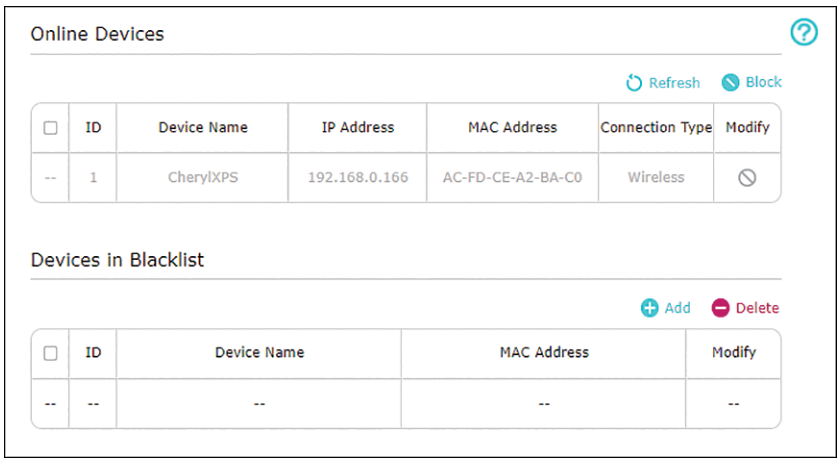


FIGURE 18.50 Wireless router IP filtering

Wireless routers also have security settings related to TCP and UDP ports. These are usually in the advanced security link. Look for SPI (Stateful Packet Inspection) or DoS protection settings. Note that all ports that are not being used should be disabled.

WPS

Wi-Fi Protected Setup (**WPS**) is configured based on the SSID and WPA2 wireless security key for an AP or a client's devices. It supports 802.11a, b, g, n, and ac devices, including computers, access points, consumer electronics, and phones. There are four ways to configure a wireless network using WPS:

- A personal identification number (PIN) is entered. This PIN is sometimes found on a sticker or display on the wireless product.
- A USB device attaches to the AP or wireless device to provide configuration information.
- A button is pushed or clicked. This method is known as push button configuration (PBC).
- With near field communication (NFC), the wireless device is brought close to the AP (or a device known as the registrar), and the configuration is applied. RFID tags are suited for this method.

TECH TIP

Avoid WPS

Because of security issues with WPS, disable this mode if possible and do not use it.

AP Default Settings

All wireless networks have security features. A SOHO AP/router comes with a default password and SSID, but many such devices ask you to change the password the first time you access the AP/router. To secure management access, change both the default password and SSID as soon as the access point is powered on. Default passwords are posted on the internet, and a hacker could use that information to lock out access from the access point. If you need to be able to remotely access an AP, make sure you enable SSH.

TECH TIP

Never leave an access point password set to the default

After powering up an access point and connecting to it, one of the first things to do is change the default password.

Firmware

Firmware is software that is embedded into hardware. Firmware can be upgraded in network routers, switches, access points, firewalls, and so on. Companies update firmware as security issues become known, when enhancements become available, or to support new technology. In a corporate environment, it is critical that firmware updates be applied. The process for obtaining and applying firmware updates varies per vendor but is commonly done through a web browser window used to access the network device.

SSID Broadcasting

As mentioned in Chapter 13, the service set identifier (SSID) announces to wireless devices that a particular wireless network is in the area. With **SSID broadcasting**, the access point periodically sends out a beacon frame that includes the SSID. This should be changed to a descriptive setting if it is being broadcast so users can easily select from the list of wireless networks in the area. SSID broadcasting can be disabled as a preventive measure so that the wireless network is not announced in the area. Look back at Figure 13.44 to see how this might be configured on a wireless router.

TECH TIP

Reduce transmit power

If adjacent companies or people nearby are using the guest wireless network, reduce the signal power to reduce the range of the wireless network.

Wireless AP/Router Installation Checklist

Many wireless access points have the capability to route. A router, whether standalone or integrated with a wireless access point, connects wired and wireless networks together. A router also enables DHCP to service both wired and wireless networks and provides a firewall for network security.

Many of the parameters needed for wireless NIC configuration are also needed for access point installation. However, installing an access point is more involved because the access point is the central device in the wireless network. Answer the following questions *before* an access point is installed to help with the installation:

- What SSID is to be used?
- What static IP address will be assigned to the device?
- Is WEP, WPA, WPA-PSK, WPA2-PSK, WPA3, TKIP, AES, or any other security option enabled?
- What security key lengths, security keys, or passphrases are used?
- Will **guest access** be needed? If so, create a separate SSID for that wireless network.
- Is MAC filtering enabled?
- Is there power available for the access point? Note that some access points can receive power through a Power over Ethernet (PoE) switch.
- How will the access point be mounted or placed? Is mounting hardware provided with the access point, or does extra equipment have to be purchased? If the AP is out in the open, could a disgruntled employee access it and change the settings?
- Where should the access point be mounted for best coverage of the wireless network area? Where should the antenna be placed, or how should it be angled? Perform a site survey to determine how to achieve the best performance. Temporarily mount the access point. With a laptop that has a wireless NIC and site survey software, walk around the wireless network area to see the coverage range. The site survey can also be conducted by double-clicking the network icon on the taskbar; the signal strength is shown in the window that appears. Move the access point as necessary to avoid attenuation and obtain the largest possible area coverage.
- What channel ID will be used?
- Will the access point connect to the wired network and, if so, is there connectivity available where the access point will be mounted?

Wireless networking is an important and popular technology. Technicians today must be familiar with wireless devices as corporations and home users install these types of products.

Wireless Security Conclusion

Wireless security is an important issue. The following list recaps some of the important issues and provides recommendations for securing a wireless network:

- Change the default SSID and password. Make the password as long as possible and be sure it includes non-alphanumeric characters.
- Enable encryption on the access point to the highest level possible while still allowing wireless NIC access. Use authentication when possible.
- Put the wireless network on its own subnetwork and place it behind a firewall, if possible.
- In a small company, consider enabling MAC authentication (MAC filtering) for company devices.
- If supported, authenticate using an authentication server.
- If the SSID is manually configured, periodically change the SSID.
- Assign a static IP address to the access point rather than use DHCP for it.
- Disable remote management on the access point if it is not going to be used.
- If guest access is not needed but is on by default on the AP, disable it.
- Place the access point in the center of the wireless network and not next to an outside window.
- Use wireless network scanning software to test the network security.
- When using a public wireless network such as a hotspot, use a VPN to access a corporate network.

- When viewing private or financial data, make sure the website uses the HTTPS protocol so that it encrypts the data using Transport Layer Security (TLS) or the older Security Socket Layer (SSL) protocol.
- If a rogue access point (an unauthorized AP) is found on the network, disconnect the device and confiscate it. Try to determine who owns the device and report the owner to IT security personnel.

Wireless networks have a strong presence today and will continue to do so in the future. The 802.1x and 802.11 standards are constantly being improved to tighten security for wireless networks so that they rival wired solutions.

IoT Device Security

IoT devices are rapidly being integrated into homes and corporate devices, but they are often sources of security breaches. Put smart devices on a separate network, make sure they are configured for automatic updates, use strong passwords on them, and secure the router that allows them to connect to the internet.

Wireless Network Troubleshooting

Troubleshooting wireless networks is sometimes easier than troubleshooting wired networks because of the mobility factor. A wireless device can be used to troubleshoot connectivity, configuration, security, and so on. Most wireless network problems stem from inconsistent configuration. The standards deployed must be for the lowest common denominator, although some routers have combination settings such as WPA/WPA2 or WPA2/WPA3.

The following list includes questions about wireless networking that are designed to steer a technician in the right direction. Most of these issues have been discussed in previous sections, but it is nice to have the following troubleshooting list in one spot:

- Is the SSID correct?
- Is the wireless NIC seen by the operating system? (Use Device Manager to check.) Check the mobile device for a button/key combination to disable the wireless NIC.
- Has the correct wireless encryption setting been configured?
- Can other devices attach to the access point? If not, check the access point.
- Is anything causing interference or attenuation? Check antenna placement.
- Is there a channel ID overlap problem?
- If a wireless printer is to be shared across the network, ensure that the printer attaches to the company protected wireless network and not the open (guest) wireless network unless you want customers to use the printer.
- Is a program from the wireless NIC manufacturer being used instead of using Windows to control the wireless NIC? If the customer wants to use Windows instead of the software provided, access a command prompt with elevated privileges. At the prompt, enter `netsh wlan show settings`. From the output, determine whether the Windows automatic wireless configuration is disabled. You may have to disable the wireless NIC and uninstall the vendor software to use Windows to control the NIC.

Security Incident Response

Many companies define what to do when a security incident has occurred. However, in some businesses or for an incident that occurs on a home network, people are not always sure what to do. These are the steps to take:

Step 1. Identify the issue. (See Table 18.16 for issues and best practices.)

Step 2. Report the issue through the proper channels (see Table 18.16).

Step 3. Preserve the data/device by documenting the incident and securing any storage device, if possible. Consider the **order of volatility** and preserve the most volatile data first, such as the data in RAM. Determine what apps are running, what documents are open, what websites have been accessed recently, and so on. Note that in some cases, the storage device must be preserved, and it must be copied to another machine to ensure that no data is modified. Ensure that the documentation includes everything, including any changes or moves. Use a chain-of-custody form that travels with the data/device as more people get involved. Chain-of-custody forms commonly include the following information:

> What is the issue (with data, a device, or something else)?

> How did you get involved with the evidence?

> When did you see the issue?

> What did you do to handle the issue?

> To what person did you turn over the issue, data, device, and so on?

TABLE 18.16 Incident reporting and actions

Type of event	Action to take
Virus	Disconnect the computer from the internet and log all actions. Do not power off the computer or reboot it. Run a full antivirus scan. Notify the appropriate personnel, as outlined in the security policy. Do not forget that other IT personnel may need to be notified, such as network personnel who may need to block connections to contain the spread of the virus, or personnel responsible for corporate messaging, for example. You may also need to contact legal or public relations personnel. You can also notify your internet provider and file a complaint with the FBI Internet Crime Complaint Center.
Spyware	Use freeware or a software application to remove the spyware. Many of the security suites have a method of reporting found incidents. Submit a report using the FTC Consumer Complaint Form.
Phishing	Notify the agency from which the contact was received. Report the incident to the U.S. Computer Emergency Readiness Team (CERT).
Child exploitation	Use parental control software to prevent this. Log off immediately and notify your local police department and/or the nearest FBI field office. You can also report the event to the National Center for Exploited and Missing Children.
Software piracy	Report incidents of organized software piracy to the Software & Information Industry Association (SIIA) and the Business Software Alliance (BSA).

If a security incident occurs and you do not know what to do, talk to your supervisor (see Figure 18.51). They should have the experience to guide you or know to whom they should go to resolve the issue. If you feel uncomfortable talking to your supervisor about this, consider going to the human resources department or a higher administrator. The BSA and other organizations allow anonymous reporting. Reporting and documenting security violations is important, especially in the business environment. It is every person's responsibility to be security aware and responsible.

FIGURE 18.51 Report security violations

A Final Word About Security

Whether for a wired or wireless connection, standalone PC or networked PC, or full desktop computer, laptop, tablet, or smartphone, data and device security are important. Security measures must always be taken. Technicians must be aware of the latest threats, take proactive measures to implement security, and share their knowledge with users so the users can take proactive steps. Security risks and threats cause technicians a lot of work and time. These threats and attacks cost billions in lost data and time to businesses. Because most technicians do not see themselves as a dollar figure on a spreadsheet, they don't realize that if the business loses money as a result of security threats, the business has to cut costs, and one of those costs could be the technical position. Think about it and be proactive in guarding against security threats.

TECH TIP

Follow all policies and security best practices

It is very important for technicians to follow corporate policies and security best practices. If in doubt, ask your supervisor or ask for a copy of your organization's policies and practices.

SOFT SKILLS: BUILDING CUSTOMER TRUST

It is fitting in the security chapter to discuss building a trust relationship with the customer. Trust begins with professionalism. Be professional in your attire, attitude, written communication, and oral communication. Trust also includes being honest with the customer. If you are going to be late, let the customer know that. If you need to do more research, explain the situation. No one can be expected to know all technical information.

Trust also involves being honest if you find confidential material. Do not use or discuss any material you see while in a customer area. If you see confidential material, let the customer know you have seen the material. If the material is a password, let the customer know and recommend that they change the password immediately.

Do not touch or move things or papers in a customer's area. Also do not try to work around a mess. Instead, ask the customer to move or put things away to clear the area you need. Simply explain that you need space to determine and/or repair the problem.

Trust involves giving customers documentation related to the product just installed or replaced. Trust involves doing what you say you will do. If you say you will call back to check on the situation in the next 24 hours, do so. If you say you will drop off the documentation the following week, do that. Be true to your word.

Trust also involves being honest about billing. Do not overcharge customers. When presenting customers with an invoice or a work order, explain the details with patience. Do not allow customers to argue with you over facts or time. Your time is valuable, too.

You never know where you are going to meet your next boss. Every time you step into a customer's area or talk to a customer, it might lead to a professional reference, a job recommendation, a job lead, or a promotion. Part of building the customer relationship is building trust. Be professional in all that you do. See Figure 18.52.

FIGURE 18.52 Building customer trust

Chapter Summary

- A security policy guides a company in security matters. The policy defines things such as physical access, antivirus, acceptable usage of devices and data, password policies, email usage guidelines, remote access strategies, and emergency procedures.
- Physical security can include door access, key control, authentication methods (such as the use of smart cards), door locks, key fobs, RFID, biometric devices, guards, access control vestibules, physical protection of network devices (such as servers, APs, switches, and routers), video surveillance, alarm systems, motion sensors, bollards, fences, lighting, magnetometers, and privacy filters.
- Document shredding can help with corporate data security. If a third party is providing this service, ensure that the company provides a certificate a destruction.
- Authentication involves proving you are the person gaining access to a system or a network. Multifactor authentication requires multiple means of proof to be more secure. Authentication servers such as RADIUS or TACACS+ servers can be used, and they might use the Kerberos in order to prevent packets from being altered or read.
- BIOS/UEFI security options include configuring a supervisor/user password, using a TPM chip, disabling unused ports, disabling USB ports, and disabling device options.
- To protect the operating system, use NTFS and have a plan for updating the operating system, web browser, antivirus, anti-malware, and antispyware. Encrypt files and folders as necessary. Use BitLocker and TPM technologies, implement a firewall, and disable AutoRun and AutoPlay.
- If a computer with sensitive data on the hard drive is to be donated, moved, or sold, securely erase the drive, degauss the drive, shred the drive, or drill through the drive platters and then destroy the pieces with a hammer.
- If virtualization is used, ensure that each virtual machine has adequate protection (firewall, antivirus, anti-malware, and antispyware).
- After a security scan, any virus or malware files that are quarantined must be manually deleted.
- The Windows Guest account should be disabled; the administrator account should be renamed and have a strong password. User accounts should limit rights to only the rights the person requires to do their job; this is known as the principle of least privilege.
- Ensure that data is backed up routinely on site or in the cloud. Backup strategies include full, incremental, differential, and synthetic.
- Permissions should be assigned appropriately to remotely accessed files and folders. Use either share permissions or NTFS permissions (for more control) but not both on the same network share. If a file is placed in a folder that has permissions, the file inherits the folder permissions. Effective permissions are the bottom-line permissions someone has when group permissions and individual permissions have been granted.
- A hijacked browser can cause a different home page to appear, a particular web page to be displayed, a rootkit or other malware to be installed, different DNS settings to be applied, or a new or updated HOSTS file to be applied.
- Email applications protect against spam, and you can also create rules to block messages from a particular source or subject line.
- On a wireless network, implement encryption and authentication. Change default SSIDs and passwords.
- When a security incident occurs, identify the issue, report it through the proper channels and to the appropriate authorities, and preserve the data by using a chain-of-custody form.
- When dealing with a customer, a coworker, or your boss, maintain your professionalism and do everything you can to build trust.

A+ CERTIFICATION EXAM TIPS

- ✓ This chapter includes information related to both the CompTIA A+ Core 1 (220-1201) and CompTIA A+ Core 2 Exam (V15) exams. It is the most complex chapter in the book because many security issues need to be experienced to know exactly what things to try when problems arise.
- ✓ Review all of the acronyms in the exam objectives and know what they mean. Security has a fair share of them, including FRT, ACL, MFA, SMS, TOTP, OTP, SAML, PAM, DLP, IAM, PIN, SSO, UAC, EFS, WPA, TKIP, AES, RADIUS, TACACS+, PUP, EDR, XDR, DoS, DDoS, SQL, BEC, EOL, BYOD, SOHO, PII, UEFI, MDM, UPnP, SSID, GFS, DRM, EULA, NDA/MNDA, VNC, SSH, RMM, SPICE, and WinRM.
- ✓ Be familiar with wireless configuration on both the client and router/AP: default username, firmware update, SSID, channels, encryption, SSID broadcasting, IP and content filtering, firewall, disabling guest access, port forwarding/mapping, turning off TCP/UDP ports that aren't used, DHCP reservations, WAN IP address, UPnP, and screened subnets.
- ✓ Know login options, including SSO, fingerprint, username/password, PIN, facial recognition, and multifactor authentication. Be familiar with these security concepts: ACLs, principle of least privilege, email security (including how DKIM, SPF, and DMARC are used for spam management as part of DNS and how TXT messages are used), hardware tokens, software tokens, SMS, voice calls, and authenticator apps.
- ✓ Acquaint yourself with these security items: TPM, VPN (and be able to configure a VPN on a Windows computer), UTM, proxy server, and load balancer.
- ✓ Know what to do if you find prohibited content/data and what PII is.
- ✓ Review hard drive security, including BitLocker and what to do with a hard drive when moving it to another device or simply removing it.
- ✓ Practice security measures that a technician must implement, such as viewing hidden files, using an administrator account/rights, assigning Windows user roles, and adjusting browsers.
- ✓ Practice manually configuring a wireless router/AP with security settings and a wireless NIC.
- ✓ Review what to do with security problems such as computer slowdowns, certificate warnings, browser redirection, desktop alerts, false antivirus alerts, and altered files. Know the steps to take to remove malware. Be able to configure Windows Defender Firewall and Windows Defender Antivirus, and understand how to use the Windows Privacy settings.
- ✓ Be able to implement backup and recovery. Know the difference between full, incremental, differential, and synthetic backups.
- ✓ Be familiar with just-in-time access and the zero trust model.
- ✓ Configure basic firewall settings, including screened subnet (DMZ), port forwarding, NAT, UPnP, allow lists/deny lists, and MAC filtering settings.
- ✓ Explain the purpose of MDM, port security, and the following Active Directory concepts: login script, domain, group policy/updates, organizational units, home folder, folder redirection, and security groups.
- ✓ Configure BIOS/UEFI security settings including passwords, drive encryption, TPM, and HSM.
- ✓ Describe Windows users and groups, including administrator, guest, and standard user. Review NTFS permissions, administrative shares vs. local shares, permission propagation, and inheritance factors.

Key Terms

3-2-1 backup, acceptable use policy, access control vestibule, ACL, Active Directory, administrative share, adware, AES, alternative location, anti-malware, antivirus, authentication, authentication failure, authenticator application, authorization, backup testing, badge reader, biometrics, BitLocker, BitLocker To Go, bollard, boot password, boot sector virus, brute force, business email compromise (BEC), BYOD, Certificate Manager, certificate of destruction, change the default admin user account password, configuration profile, content filtering, cryptominer, data at rest, DDoS, degaussing, desktop alert, dictionary attack, differential backup, directory service, disable AutoPlay, disable AutoRun, disable the guest account, DLP, DMZ, DNS TXT, door lock, DoS, drive wipe, DRM, Dumpster diving, EDR, effective permissions, EFS, encryption, email security gateway, end-user education, equipment lock, EULA, evil twin, facial recognition technology, failed attempts, fileless, fingerprint scanner, firewall, folder redirection, full backup, full device encryption, GDPR, `gpedit.msc`, grandfather-father-son backup, group policy, group policy editor, guest access, hardware token, hidden share, home folder, HSM, identity access management, identity synchronization, IDS, impersonation, in-place/overwrite, incineration, incremental backup, inherited permissions, IP filtering, IPS, join a domain, just-in-time access, Kerberos, key, key fob, keylogger, load balancer, local security policy, local share, log off when not in use, login script, low-level format, MAC address filtering, magnetometer, malware, man-in-the-middle, MDM, MDR, Microsoft Defender Antivirus, missing files, MNDA, mobile digital key, multifactor authentication (MFA), NAT, NDA, non-compliant system, NTFS permissions, off-site storage, on-site storage, on-path [attack], one-time password/passcode (OTP), open source, order of volatility, organizational unit, palm print scanner, password manager, passwordless, patch/update management, patching/OS updates, PCI, PHI, phishing, PII, PIN, piracy, port forwarding, port mapping, port security, potentially unwanted program (PUP), principle of least privilege, privileged access management, proxy server, QR code phishing, RADIUS, ransomware, RDP, recycling, restrict login time, retinal scanner, RFID, RMM, rogue antivirus, rootkit, run as administrator, SAML, screened subnet, secure boot, secure DNS, security group, security policy, share permissions, shoulder surfing, shredding, single sign-on, smart card, smishing, SMS, social engineering, soft token, software firewall, spam, spam gateway, spear phishing, SPICE, spoofing, spyware, SQL injection, SSH, SSID broadcasting, stalkerware, standard format, synthetic backup, TACACS+, tailgating, Telnet, third-party vendor, time-based one-time password (TOTP), timeout/screen lock, TKIP, TPM, Trojan, trusted source, UAC, untrusted source, unprotected system, unwanted notification, UPnP, USB lock, username and password, UTM, virus, vishing, VNC, voice recognition technology, VPN, WEP, whaling, Windows Defender Firewall, Windows Hello, WinRM, WPA2, WPA3, WPS, XDR, XSS, zero day [attack], Zero Trust model

Review Questions

1. Match each security policy component with the appropriate definition from the following list.

   ____ Physical access

   ____ Acceptable use

   ____ Remote access

   ____ Password

   a. The specific web browser that is allowed to be installed

   b. Defines whether you can send the code used to access an account (such as shared network storage) via email

   c. The type of security required for a remote VPN connection

   d. The time, day, and year someone entered a network server room

2. Describe multifactor authentication.

   _____

   _____

3. In what situation would an access control vestibule be used?

   a. When multiple people share the same area and each screen can be seen by one of the other people

   b. For physical security

   c. When the access server is unavailable or busy with other requests

   d. When a SAN is being used

4. Which wireless security feature would be most likely to be used in a small company where the staff are the only individuals using the wireless network and a couple of the laptops are older ones?

   a. VPN

   b. IDS

   c. WPA3

   d. WPA2

5. List five recommendations for protecting the operating system.

   _____

   _____

   _____

   _____

   _____

   _____

   _____

   _____

   _____

6. What is BitLocker?

   a. A wireless security setting

   b. A method used to secure passwords for websites, users, and files using TPM

   c. Online secure storage

   d. A utility that encrypts an entire disk volume, including operating system files, user files, and page files

7. [T | F] A new file is created and stored in an encrypted folder. The file must be manually encrypted because it was added after the folder was encrypted.

8. Describe the security rights for a subfolder when the parent folder is shared.

_____

9. List three password guidelines you would recommend that a company use.

_____

_____

_____

_____

_____

10. Where are domain user passwords stored?

[local database | registry | network server | the cloud]

11. A network administrator in a large corporation goes to a popular network vendor site to research security settings, but a message appears, saying that this particular site cannot be accessed and is blocked. What security measure most likely caused this message?

a. BitLocker

b. Magnetometer

c. Port security

d. Content filtering

12. Describe the difference between a local security policy and a domain policy.

_____

_____

_____

13. What is needed to configure a computer for a proxy server? (Choose two.)

[IP address of the proxy server | MAC address of the proxy server | administrator name on the proxy server | IP address of the local computer | MAC address of the local computer | port number on the proxy server | administrator password on the local computer]

14. What is the purpose of a screened subnet (DMZ)?

_____

_____

_____

15. [T | F] A virtual machine used in a small company should have anti-malware installed.

16. Which phishing terms describes an attempt to get information or something from corporate executives?

[smishing | whaling | vishing | scareware | spear phishing]

17. No one can ping a specific Windows computer. What administrative tool can be used to change this default behavior?

[Windows Firewall | Local Security Policy | File Explorer > Internet options | Windows Defender]

18. What type of unsolicited internet message records the URLs visited and keystrokes used?

[virus | grayware | spam | spyware]

19. An unofficial email sent from your bank asks you to click a link to verify your account information. What type of social engineering is this?

[phishing | grayware | spyware | VPN]

20. Match the incident on the left with an action on the right. Even though some of the incidents might have multiple answers, each answer is used only once.

____ virus	**a.** BSA
____ child exploitation	**b.** police department
____ software piracy	**c.** CERT
____ phishing	**d.** FBI Internet Crime Complaint Center

Exercises

Exercise 18.1 Examining the Security Incident Response

Objective: To become familiar with security incident response

Procedure: Answer the following questions.

1. Place the security incident response tasks in the appropriate order.

   ____ First

   ____ Second

   ____ Third

   a. Report the incident through the proper channels.

   b. Preserve the data/device(s) involved.

   c. Identify the threat.

2. A college requires that each employee use the last four digits of their Social Security number to access the copier. Which type of security threat is this? Describe how you would respond to the incident if you were an IT security person for this college.

   a. Malware

   b. Sensitive PII

   c. Security policy

   d. Licensing

   _____

   _____

3. Your neighbor asks if they can borrow your application code. They promise they will not register the application. How will you respond to this, given that it is a personal request and not a professional one? To whom would you report this, if anyone?

   _____

   _____

4. You work as an IT support person for a company. The user complains of slowness when opening files. A security scan shows evidence of malware. Place the steps in the order in which they will be carried out.

   Step _____: Remediate the infected system.

   Step _____: Investigate and verify the symptoms.

   Step _____: Quarantine the infected system.

Exercise 18.2 Wireless Security

Objective: To become familiar with wireless security options

Procedure: Match the scenario to the correct term. Each answer is used only once.

Scenario:

a. Manually type Layer 2 addresses into a table.

b. Commonly used channels are 1, 6, and 11.

c. The most common corporate wireless security protocol is used.

d. Don't broadcast the name of the network.

e. Nearby companies get a stronger wireless signal than employees.

f. Uses SAE encryption.

g. Someone can easily get into the AP settings.

h. Easy to configure but has security risks.

i. Outdated software in hardware.

Term:

____ WPA2

____ WPA3

____ MAC filtering

____ Move AP and/or antenna

____ 2.4 GHz

____ WPS

____ Disable SSID broadcasting

____ Default settings

____ Update firmware

Exercise 18.3 Data Security

Objective: To become familiar with regulated data

Procedure: Answer the questions.

1. Match each description with the correct term related to regulated data.

Description:

a. U.S. companies are subject to this rule when engaging in trade in the European Union.

b. This sensitive data should be encrypted when in storage or in transit.

c. The 1996 HIPAA law prompted regulations related to this.

d. Banks, businesses, colleges, airlines, and railroads are subject to these standards if credit cards are accepted as a payment method.

Term:

____ PHI

____ PCI

____ GDPR

____ PII

2. [T | F] Personally identifiable information must be encrypted.

_____

_____

3. [T | F] A U.S. citizen who retires to Italy is not subject to the GDPR but is only subject to U.S. federal laws.
4. Which information would be considered nonsensitive PII? (Choose all that apply.)

   [name | user ID | password | email address | passport number | Social Security number]
5. Of the four types of regulated data, which two are most likely to be encountered by a PC technician who works at a college? (Choose two.)

   [PII | PCI | GDPR | PHI]

Activities

Flip the CLASSROOM

Internet Discovery

Objective: To become familiar with researching computer security concepts using the internet

Parts: A computer with internet access

Questions: Use the internet to answer the following questions.

1. Access the Internet Crime Complaint Center to answer the following questions. At the time of writing, the URL is https://www.ic3.gov.

   List three ways that artificial intelligence (AI) might be used in a security threat.

   _____

   _____

   _____

   _____

   _____

   Why do criminals use cryptocurrency for illicit transactions, according to this website? Write the answer and the URL at which you found the answer.

   _____

   _____

2. Access the U.S. Computer Emergency Readiness Team website and access the technical user link to answer the following questions. At this writing, the URL is https://www.us-cert.gov.

   List three things the Cybersecurity Performance Goals (CPG) assessment can do for a company or which industry sectors they have specific goals for.

   _____

   _____

   _____

   _____

   List two training events or important security news items listed at the site and explain how you think they would be beneficial to you.

   _____

   _____

3. Access the National Institute of Standards and Technology Computer Security Resource Center (CSRC) website to answer the following questions. At this time, the URL is https://csrc.nist.gov.

   Access the glossary of security terms and find the term ACL (access control list).

   What are ACLs, and how do they relate to computer security?

   _____

   _____

   Access the CSRC Projects link. List one security section related to software security that you find interesting and define one term from that section that is not in this chapter.

   _____

   _____

4. Use a browser search to answer the following questions.

   What percentage of software installed is pirated in the current year? List the answer and the URL of the website where you found this information.

   _____

   _____

   What is the current maximum fine for software piracy in the United States?

   _____

   _____

Soft Skills

Objective: To enhance and fine-tune a future technician's ability to listen, communicate in both written and oral forms, and support people who use computers in a professional manner

Activities:

1. Prepare a presentation on any topic related to network security. The topic can relate to wired or wireless security. Share your presentation with the class.
2. In small groups, find a security policy on the internet or use any of your school's computer policies. Critique the policy and make recommendations for how the policy could provide for stronger security.

   _____

   _____

Critical Thinking Skills

Objective: To analyze and evaluate information as well as apply learned information to new or different situations

Activities:

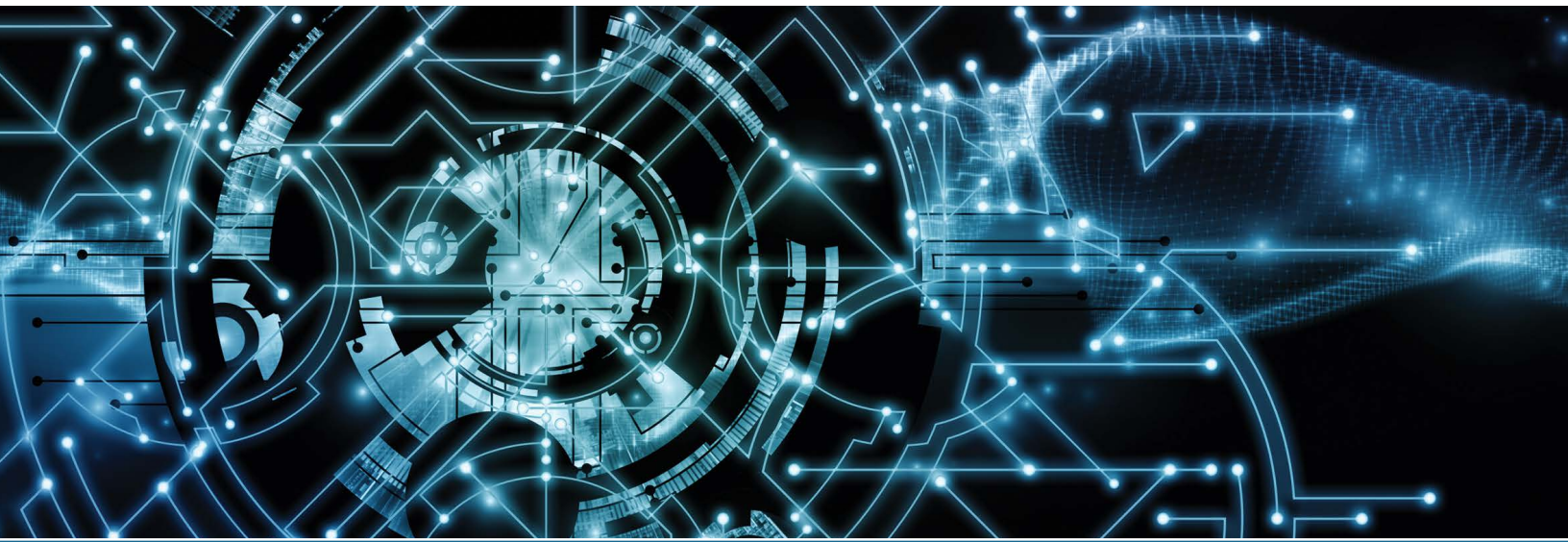
1. Create a wired workgroup network. Before users are created, determine what security policies will be enforced. Document the security policy. Also determine what activities are logged. Share folders between the computers with security implemented. Document the network shares and policies. View and capture activities logged and include those captures with the documentation. Present your design, implementation, and monitoring to the class.

   _____

2. In teams, build a wired and wireless network with security in place. Document the security as if you were presenting it to a home network customer who hired you to build and implement it.

   _____

19 Operational Procedures



In this chapter you will learn:

- Proper personal safety precautions and equipment
- Workplace safety precautions, procedures, and equipment
- How to protect computer equipment from airborne pollutants
- How to dispose of waste (computers, mobile devices, batteries, laser printer toner cartridges, and monitors)
- Types of IT documentation
- Change management processes
- Proper communication skills

CompTIA Exam Objectives:

- ✓ 1202-2.9 Compare and contrast common data destruction and disposal methods.
- ✓ 1202-4.1 Given a scenario, implement best practices associated with documentation and support systems information management.
- ✓ 1202-4.2 Given a scenario, apply change management procedures.
- ✓ 1202-4.3 Given a scenario, implement workstation backup and recovery methods.
- ✓ 1202-4.4 Given a scenario, use common safety procedures.
- ✓ 1202-4.5 Summarize environmental impacts and local environment controls.
- ✓ 1202-4.6 Explain the importance of prohibited content/activity and privacy, licensing, and policy concepts.
- ✓ 1202-4.7 Given a scenario, use proper communication techniques and professionalism.
- ✓ 1202-4.10 Explain basic concepts related to artificial intelligence (AI).

Operational Procedures Overview

Being up-to-date on the latest safety precautions and procedures regarding both personal and workplace safety is beneficial to all involved. This chapter reviews the role that federal, state, and local governments play in protecting human health and the environment by operating regulated recycling and disposal sites for electronics. Also covered are the dangers of damaged batteries that leak acid and how to handle those situations. We review why and how:

- Electronics need to be protected from moisture, dust, extreme temperature fluctuations, and weight-bearing loads.
- Toxic fumes can cause degradation of components.
- Electronic waste (computers, mobile devices, batteries, laser printer toner cartridges, and monitors) is considered toxic waste.
- It is important to protect computer equipment with surge (power) suppressors, personal enclosures, and clean rooms.
- Personal protective equipment and personal safety techniques are necessary.
- It is important to properly handle and store electronics using antistatic bags, ESD straps, and ESD mats.
- Equipment grounding, self-grounding, and fire safety knowledge are important.

Paperwork is a part of any job, and it is especially critical in IT, where systems cross all parts of the business. Technicians use IT documentation as reference material and as a historical record of IT devices. Change is also a constant in IT, and change management is therefore important. This chapter covers the type of documentation commonly used and created within the IT department as well as the change management process. Finally, we discuss why looking, acting, and *thinking* like a professional, along with having good communications skills, are necessary for an IT professional.

Workplace Safety Precautions and Procedures

The federal government mandates that all companies must have workplace safety precautions and procedures posted and in effect. Most employers provide education and training on those procedures. Some precautions and procedures are a matter of common sense. For example, it is clearly important to remove the power cord and/or battery before working on a PC or mobile device, and most people will not walk on a slippery floor if a "Wet Floor" sign is posted. As a technician, you will want to keep your work area relatively neat to avoid hampering other workers or potentially causing an accident. Determine where you can safely install your computer and network equipment. You want to make sure to practice good **cable management**, ensuring that cables do not pose a tripping hazard. (Chapter 13, "Networking," further discusses good network cable management techniques.)

When an accident occurs, do the following:

- Immediately notify medical personnel, if needed.
- Report the incident to a supervisor.

The supervisor must then complete an incident report (see Figure 19.1).

TECH TIP

Always comply with local government regulations

There are many government regulations regarding workplace safety, and there are also local government regulations related to disposal requirements. Check with your supervisor if you are unsure about an unsafe environment or have questions about processes.

FIGURE 19.1 Incident report

OSHA

The Occupational Safety and Health Administration (**OSHA**) is a division of the U.S. Department of Labor. OSHA promotes safe and healthy working conditions by enforcing standards and providing workplace safety training. In addition, Environmental Protection Agency (EPA) standards and local government regulations specify that workplace environments should be free of harmful and/or hazardous chemicals or situations.

An important form required by OSHA is a material safety data sheet (**MSDS**), which outlines handling, storage procedures, disposal, and first aid on a potentially harmful or hazardous substance that you may come in contact with while working. Because MSDSs are available to employees, anyone working with these substances should review this important information. A similar form is the safety data sheet (SDS), which outlines similar information regarding chemicals.

Fire Safety

It is rare for electrical fires to occur in computers, but it is important to have **electrical fire safety** knowledge in case a fire does happen. If a fire occurs inside a computer or peripheral, evacuate everyone and unplug the equipment, if possible. Do not put yourself in harm's way in attempting to do this. A Type C or Type A-B-C fire extinguisher can be used to put out the fire. **Type C fire extinguishers** are made specifically for electrical (Type C) fires. **Type A-B-C fire extinguishers** can be used for Class A, Class B, and Class C fires.

Here's some quick information about classes of fires:

> Class A fires involve paper, wood, cloth, or other normal combustibles.
> Class B fires involve flammable liquids and gases.
> Class C fires involve electrical or electronic equipment.

In order to use a Type A-B-C or a Type C fire extinguisher, follow these steps:

Step 1. Pull the fire alarm.

Step 2. Pull out the fire extinguisher pin (see Figure 19.2).

Step 3. Aim the fire extinguisher nozzle at the base (bottom) of the fire.

Step 4. Squeeze the fire extinguisher handle and move the nozzle back and forth in a slow sweeping motion.

FIGURE 19.2 Pull the fire extinguisher pin

A Review of Safety Equipment in the Technical Field Kit

Let us examine three simple and inexpensive products that are essential parts of a technical field kit. Your personal protective equipment (PPE) should consist of safety goggles or glasses, gloves, and a dust mask/air filter mask. All of these items can be purchased at most hardware, drug, and grocery stores.

Safety goggles or glasses (see Figure 19.3) protect eyes from injury or irritation due to metal chips, wires, sparks, dust, airborne particles, debris, or any liquids or contaminants that might be in the working environment. Even though prescription eyeglasses provide some protection, it is wise to have a pair of safety glasses or goggles that fit over prescription eyeglasses.

FIGURE 19.3 Safety goggles

For some situations, such as when working with laser toner, it is important to wear gloves and a dust mask or an **air filtration mask** to prevent inhalation of harmful airborne particulates, smoke, odors, and fumes. When you use **compressed air**, dust and debris are an issue. Use a **vacuum**, when possible, to remove dust and debris, but if in doubt, wear a mask. Dust masks like the one shown in Figure 19.4 are available in many stores.

FIGURE 19.4 Dust mask

Personal Safety

Personal and equipment safety is paramount in IT. Having proper personal safety precautions and equipment will facilitate repairs by getting you into a routine of automatically putting on safety glasses or goggles, gloves, and a dust mask (when applicable). It will lessen the chance of electrostatic discharge, of forgetting a repair step, or of a careless mishap because your safety procedures will become second nature to you. Other important things to remember follow:

- Remove jewelry, watches, dangling necklaces/earrings, or ID lanyards that could get caught, hooked, or entangled in equipment you're working near.
- Disconnect power cords.
- Be sure that the work area is clear of liquids (coffee, soda, water bottles) and foods that may spill or otherwise contaminate the equipment.
- Remember to use good **lifting technique** (such as using your legs, not your back) and get help when lifting more than 50 pounds.
- Be familiar with the location of the nearest fire extinguisher and the nearest fire exit.

Environmental Impacts

Awareness has been raised in the past few decades about "going green," and the "reduce, reuse, recycle" movement is practiced in many communities. Collectively, as a society, we can make a huge impact. Individually, we can make a difference by being good stewards of our resources. Every state and many cities have specific guidelines about how to dispose of electronics or e-waste (see Figure 19.5). These rules must be followed by technicians who replace broken computer equipment. If you are unsure about how to get rid of any piece of broken electronic equipment, contact your direct supervisor for instructions.

FIGURE 19.5 E-waste

The following list provides alternatives and suggestions for being environmentally conscious about discarding electronics:

- Donate equipment that is operational to schools and charities so that those who do not have access to technology can get some exposure. If the operating system is not transferred to another system, leave the operating system on the machine and provide proof of purchase along with documentation. Do not forget to erase all data stored on the computer before donating it.
- Recycle outdated electronics. If devices are so outdated that a school or charity cannot use them, consider recycling. Many companies accept old electronics and have found ways to reuse some of their parts.
- Remove parts that do work and donate or recycle them.
- Buy electronics that are designed to save resources and are easy to upgrade.
- Check with the computer or component manufacturer to see if it has a recycling program. Most of them do.

Electronic Disposal/Recycling

Computers and other electronic devices contain materials such as beryllium, chromium, cadmium, lead, mercury, nickel, and zinc. The number of these materials in landfills increase dramatically every year and can pose a threat to our environment. Each city/state has its own laws about disposing of electronics. Important disposal and handling measures should be taken with old heavy monitors that contain cathode ray tubes (CRTs), cell phones, tablets, batteries, and laser printer toner cartridges.

Cell phones and tablets are now classified as toxic waste in the United States because of the lead they contain. Lead-free phones do not solve the problem because of the zinc, nickel, copper, and

antimony within them. Manufacturers are not always been willing to take back old phones because extracting the gold, copper, silver, and other metals can be expensive.

Follow local guidelines on disposal, and look to see if the manufacturer of your new device has a trade-in program; donate to an organization that helps victims of violence, soldiers, or charities; or use a responsible recycler. The website e-stewards.org can help you find responsible e-waste recycling locations.

Don't forget to erase your data and remove the SIM card and any memory storage before donating or recycling a cell phone or tablet. Wear a mask and gloves while handling any broken parts. Place parts in a plastic bag and seal before disposing of it properly.

Batteries contain acids that can potentially burn or hurt body parts. Batteries can introduce lead and acid into the environment; thus, they need to be recycled (see Figure 19.6). Use protective gear such as gloves when handling batteries.

FIGURE 19.6 Battery recycling

Lithium-ion (Li-ion) batteries used in mobile devices and laptops may need to be replaced in the following cases:

> If the device has been subjected to extreme temperature changes
> If the device was dropped, crushed, or flooded with liquid
> If the device has sustained up to 500 cycles of discharge and recharge

The contents of a lithium-ion battery are under pressure; thus, Li-ion batteries can explode or catch on fire (see Figure 19.7) if subjected to high temperatures. If you see a bulging Li-ion battery, hear one hiss, or feel one that is overheated, immediately move the device away from anything that might catch on fire. If possible, remove the battery and put it in a safe fireproof place. If it catches on fire, use a foam or A-B-C fire extinguisher.

FIGURE 19.7 Li-ion battery on fire

Recycling all batteries is important. Refer to your local municipality's regulations for recycling and disposing of Li-ion batteries.

Toner Safety and Disposal

The **toner** in laser printer toner cartridges is not earth friendly. It takes approximately 450 to 1,000 years for a print cartridge to fully decompose. Here are some options that are better than putting it in the trash:

> Look at the original packaging and see if the company has a recycling program. You might be able to drop the used cartridge off at a specific location or receive a mailing label to send in the used cartridge.
> Determine if the store where you purchased the cartridge has a recycling program.
> See if your county has a recycling option or a company that will accept the used cartridge.

Toner is also not human friendly. If you accidently inhale toner, you could experience headaches, eye irritation, and itching. If you come into contact with it, toner can cause itchiness and skin irritation. Figure 19.8 shows some spilled toner.

FIGURE 19.8 Spilled toner

Here are some points to remember about toner safety:

- Remember to always wear some type of rubber or nitrile gloves and a dust mask when handling toner cartridges. Inhalation of toner particles can cause respiratory damage equivalent to that of smoking.
- Do not attempt to clean up any loose toner particles with a regular vacuum sweeper as the toner particles may seep into the vacuum's motor and melt. Use a vacuum with a high-efficiency particulate air (HEPA) vacuum bag.
- Allow the printer (and cartridge) to cool before repairing or replacing the cartridge. The fusing assembly and heated toner can cause severe burns. You should wait after copying or printing before doing any service or removing a toner cartridge.

Component Handling and Storage

Proper handling and storage of electronic parts and equipment reduces the chance of electrostatic discharge (ESD). ESD is sneaky. It damages, weakens, and destroys electronic equipment—often without the technician being aware that it has happened. Atmospheric conditions play a part in ESD in that the potential for ESD is greater when the **humidity** (moisture in the air) is low. Make sure to place or store electronic equipment in a well-ventilated, cool, low to moderate humidity space. Antistatic bags for storage, ESD straps and mats for repair jobs, and self-grounding knowledge and techniques are all discussed in Chapter 5, "Disassembly and Power." The following is a brief review:

- Remember to use **antistatic bags** (see Figure 19.9) for storing adapters, drives, RAM, and motherboards when not in use for an extended period of time.
- When repairing a computer, wear an antistatic strap, **ESD strap**, antistatic gloves, and/or antistatic heel strap to prevent ESD (see Chapter 5). Caution: The voltages are very high within the high-voltage power supply of a laser printer. Do not attempt to work on unless you have special training.
- Place a computer that is being repaired on an **ESD mat**. A mat may have a snap to which you can fasten an antistatic wrist strap.
- If an antistatic wrist strap or antistatic heel strap is not available, it is recommended that you rest your non-dominant arm on an unpainted metal part, leaving your dominant hand free to work on the component parts. This **self-grounding** method is an effective way of keeping yourself and the computer at the same voltage potential. You will have, of course, previously disconnected the power supply to the computer.

FIGURE 19.9 Antistatic bag

Electronic Safety: Equipment Grounding

Homes and businesses have a consistent shared (or panel) ground on all electrical outlets (see Figure 19.10). Businesses have a similar grounding system but might also include additional independent grounding by using ground plates, ground bars, and a ground bus. As a technician, you don't have to design this, but you do have to be aware of it.

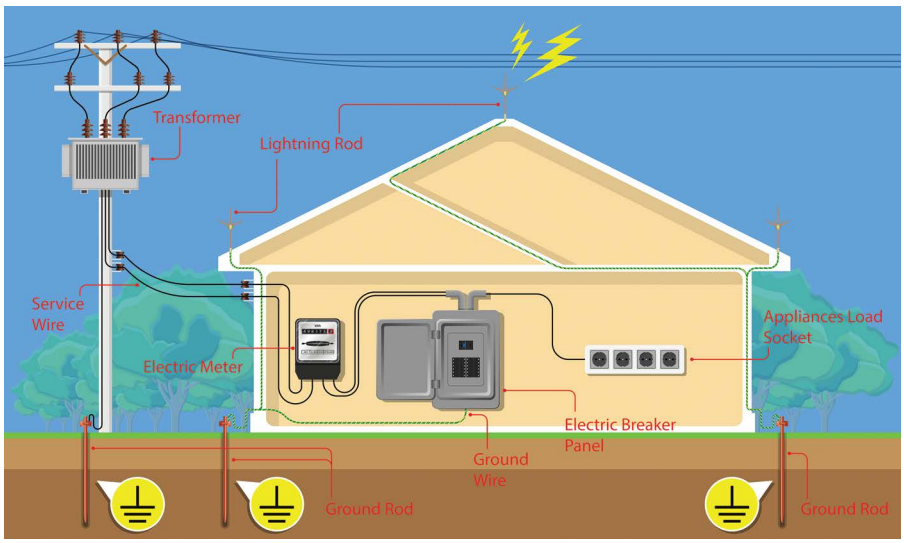


FIGURE 19.10 Equipment grounding

Equipment grounding means that the components in a device such as a computer are at the same voltage potential. Grounding is important to personal safety because consistent grounding minimizes the potential for voltage to be applied to places where it shouldn't be applied. For example, if a piece of equipment is not grounded, someone could receive a shock or be electrocuted simply by touching it (see Figure 19.11). As a technician, you might see a grounding wire connect to a network rack or battery backup system. Review Chapters 5 and 13 for more information about power and grounding.

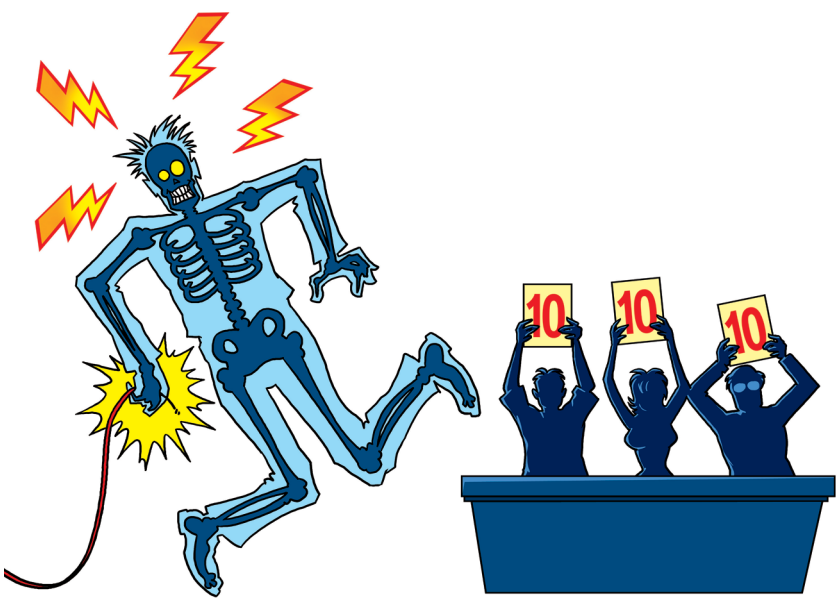


FIGURE 19.11 Electrical shock

Proper Power Handling and Adverse Power Conditions

You should always disconnect power before working on or inside equipment. Ground yourself and try to keep humidity between 45% and 55% to prevent or reduce the threat of ESD. Use an ESD strap or antistatic gloves to prevent ESD. Don't work inside power supplies unless properly trained.

There are two adverse AC power conditions that can damage or adversely affect a computer: overvoltage and undervoltage. **Overvoltage** occurs when the output voltage from the wall outlet (the AC voltage) is over the rated amount. Normally, the output of a wall outlet is 110 to 130 volts AC. When the voltage rises above 130 volts, an overvoltage condition exists. The power supply converts the AC voltage to DC. An overvoltage condition is harmful to components because too much DC voltage destroys electronic circuits. An overvoltage condition can be a surge or a spike.

When the voltage falls below 110 volts AC, an **undervoltage** condition exists. If the voltage is too low, a computer power supply cannot provide enough power to all the components. Under such conditions, the power supply draws too much current, causing it to overheat and weakening or damaging the components. An undervoltage condition may be a brownout or sag. Table 19.1 explains these power terms.

TABLE 19.1 Adverse power conditions

Major type	Subtype	Explanation
Overvoltage	Spike	A spike lasts 1 to 2 nanoseconds. A nanosecond is one-billionth of a second. A spike is harder to guard against than a surge because it has short duration and high intensity.
	Surge	A **power surge** lasts longer (3 or more nanoseconds) than a spike. A surge is also called transient voltage. Causes of surges include lightning, poorly regulated electricity, faulty wiring, and devices that turn on periodically, such as elevators, air conditioners, and refrigerators.
Undervoltage	**Brownout**	In a brownout, power circuits become overloaded. Occasionally, an electric company intentionally causes a brownout to reduce the power drawn by customers during peak periods.
	Sag	A sag occurs when the voltage from the wall outlet drops momentarily.
	Blackout	A blackout is a total loss of power.

Surge Protectors

A **surge suppressor**, also known as a surge strip or surge protector, is commonly a multi-outlet strip that offers built-in protection against overvoltage. Surge protectors do not protect against undervoltage; they protect against voltage increases. Figure 19.12 shows a surge suppressor.

FIGURE 19.12 Surge suppressor

A surge protector commonly has an electronic component called a metal oxide varistor (**MOV**), which protects the computer or device that plugs into one of the outlets on the surge strip. An MOV is positioned between the AC coming in and the outlet into which devices are plugged. When a surge occurs, the MOV prevents the extra voltage from passing to the outlets. An MOV has some drawbacks, however. If a large surge occurs, the MOV will take the hit and be destroyed, which is better than damaging the computer. However, with small overvoltages, each small surge weakens the MOV. A weakened MOV might not give the proper protection to the computer in the event of a bigger surge. Also, there is no simple check for an MOV's condition. Some MOVs have indicator lamps attached, but they indicate only when the MOV has been destroyed, not when it is weakened. Still, having an indicator lamp is better than having nothing at all. Some surge protectors also have replaceable fuses and/or indicator lamps for fuses. A fuse works only once and then is destroyed during a surge in order to protect devices plugged into surge protector outlets. Figure 19.13 shows a surge protector that has done its job.

FIGURE 19.13 Blown surge protector

TECH TIP

Do not create a trip hazard with a surge protector

When installing a surge protector, install it in such a manner that it does not cause a trip hazard due to the cord lying in an area where people walk.

Several surge protector features deserve consideration. Table 19.2 outlines some of them.

TABLE 19.2 Surge protector features

Feature	Explanation
Clamping voltage	The level at which a surge protector starts protecting the computer. The lower the value, the better the protection.
Clamping speed	The amount of time that elapses before protection begins. The lower the value, the better the protection. Surge protectors cannot normally protect against power spikes (overvoltages of short duration) because of their rated clamping speed.
Energy absorption/ dissipation	The ability of a surge protector to absorb or dissipate energy. The greater the number of joules (a unit of energy) that can be dissipated, the more effective and durable a surge protector is. A surge protector with a higher joules rating is more effective.

Feature	Explanation
TVS (transient voltage suppressing) rating	This is also known as response time. The lower the rating, the better. For example, a 330 TVS-rated surge protector is better than a 400 TVS-rated one.
UL rating	Underwriters Laboratories (UL) developed the UL 1449 VPR (voltage protection rating) standard to measure the maximum amount of voltage a surge protector will let through to the attached devices.

The federal government designates surge suppressor grades—A, B, and C. Suppressors are evaluated on the basis of 1,000 surges at a specific number of volts and amps. A Class A rating is the best.

Electric companies offer surge protection for homes. Frequently, there are two choices. A basic package protects large appliances, such as refrigerators, air conditioners, washers, and dryers. It allows no more than 800 volts to enter the electrical system. A premium package protects more sensitive devices (TVs, stereos, and computers) and reduces the amount of voltage allowed to 323 volts or less. Some suppressors handle surges up to 20,000 volts. The exterior surge arrestor does not protect against voltage increases that originate inside the building, such as those caused by faulty wiring.

TECH TIP

Which surge strip to buy?

When purchasing or recommending a surge protector, be sure it conforms to the UL 1449 standard and has an MOV status lamp. Also, check to see if the vendor offers to repair or replace any surge-protected equipment that is damaged during a surge.

Common criteria used when buying a surge suppressor include the following:

- Cable length
- Number of outlets
- Room to connect peripheral power connectors that may take additional space
- Diagnostic LED(s)
- Integrated circuit breaker
- Outlets that power off when not in use for nonessential electronics such as lamps, speakers, or printers
- Outlets that are always on for devices such as cordless phone handset cradles, modems, and external hard drives
- Insurance
- UL 1449 compliance

Surge protectors do not provide the best protection for a computer system because most provide very little protection against other adverse power conditions. Even the good ones protect only against overvoltage conditions. Those with the UL 1449 rating and an MOV status lamp are usually more expensive.

Line Conditioners

An alternative for computer protection is a line conditioner. **Line conditioners**, sometimes known as power conditioners, are more expensive than surge protectors, but they protect a computer from overvoltages, undervoltages, and adverse noise conditions over electrical lines. A line

conditioner monitors AC electricity. If the voltage is too low, the line conditioner boosts voltage to the proper range. If the voltage level is too high, the line conditioner clamps down the voltage and sends the proper amount to the computer.

Power Failures

A battery backup provides AC power when power from the wall outlet fails, such as during a brownout or blackout. The power is provided by a battery within a unit. Two different types of battery backups are available for home and business computers and devices: uninterruptible power supplies (UPSs) and standby power supplies (SPSs). Let's look at the differences between the two types.

UPS

A **UPS**, sometimes called an online (or true) UPS or a line-interactive UPS, provides power to a computer or other device for a limited amount of time when there is a power outage. A UPS provides enough time to save work and safely shut down the computer. Some operating systems do not operate properly if power abruptly cuts off and the computer is not brought to a logical stopping place. A network server, the main computer for a network, is a great candidate for a UPS. Network operating systems are particularly susceptible to problems during a power outage. A UPS might have a connection for a cable and special software that automatically maintains voltages to the computer, quits all applications, and powers off the computer. Some UPS units have USB and/or network connections as well (see Figure 19.14).

FIGURE 19.14 Front and back of a UPS

A UPS also provides power conditioning for the devices attached to it. The AC power is used to charge a battery inside the UPS. The battery inside the UPS supplies power to an inverter. The inverter makes AC for the computer. When AC power from the outlet fails, the battery inside the UPS continues to supply power to the computer. The battery inside the UPS outputs DC power, and the computer accepts (and expects) AC power. Therefore, the DC power from the battery must be converted to AC voltage. AC voltage looks like a sine wave when it is in its correct form, but cheaper UPSs produce a square wave (especially when power comes from the battery) that is not as effective. Some computer servers, systems, and peripherals do not work well on a 120VAC square wave, modified sine wave, simulated sine wave, or quasi-sine wave. Figure 19.15 illustrates a sine wave and a square wave.

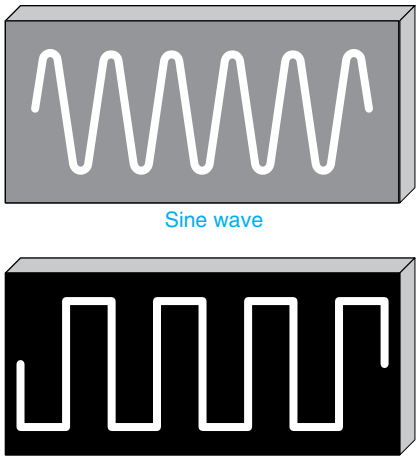


FIGURE 19.15 Sine wave and square wave

TECH TIP

Do not plug a laser printer into a UPS unless it has a rating less than 1400VA

Most UPSs cannot handle the very high current requirements of a laser printer. Other devices to avoid attaching to a UPS include space heaters, vacuums, curling irons, paper shredders, and copiers.

A UPS can provide the best protection against adverse power conditions because it protects against overvoltage and undervoltage conditions, and it provides power so a system can be shut down properly. When purchasing a UPS, be sure that the amount of battery time is sufficient, the amount of current the UPS produces is sufficient, and the output waveform is a sine wave.

A UPS has a battery inside that is similar to a car battery (except that the UPS battery is sealed). Because this battery contains acid, you should never drop a UPS or throw it in the trash. All batteries fail after some time, and most UPSs have replaceable batteries. Figure 19.16 shows a CyberPower UPS that produces a simulated sine wave (which would be fine for a home system).

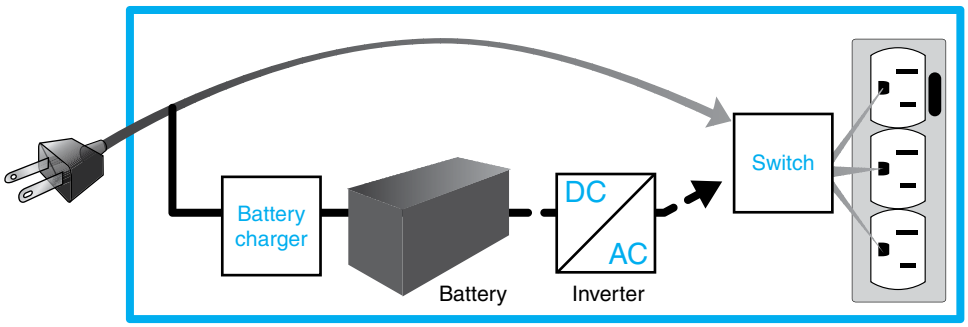
FIGURE 19.16 CyberPower UPS (with simulated sine wave output)

Standby Power Supply (SPS)

A device similar to a UPS is a standby power supply (SPS). Much like a UPS, an **SPS** contains a battery, but an SPS battery provides power to the computer only when it loses AC power. It might not provide constant power, as a UPS does. It might use a simulated sine wave. An SPS is not as effective as a UPS because the SPS must detect a power-out condition first and then switch over to the battery to supply power to the computer. As a result, SPS switching time is important. Any time under 5 milliseconds is fine for most systems.

Comparison of UPSs and SPSs

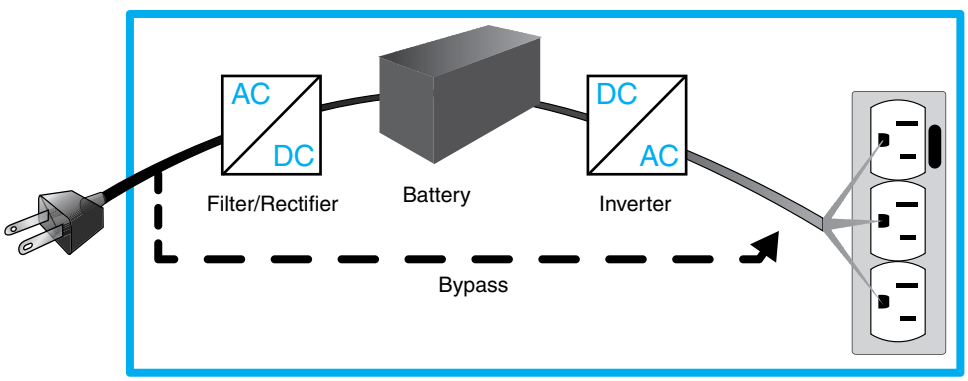
Sometimes it is difficult to discern between UPS and SPS products. When providing protection and battery backup for a home computer, an SPS or simulated sine wave output might be fine for the supplied power time and the reduced cost. Figures 19.17 and 19.18 show the differences between how some SPSs and UPSs work.



SPS/Line interactive UPS normal operation (solid line)
1. AC power is brought through the UPS.
2. The battery is charged simultaneously.
3. With some units, small over- or undervoltages are evened out before sending through the UPS.

SPS/Line interactive UPS abnormal power operation (dashed line)
1. When high voltage or large undervoltage for some units and with loss of power present in all units, DC power from the battery is sent to the inverter for as long as the battery lasts.
2. The DC power is converted to AC and provided to the attached devices.

FIGURE 19.17 SPS/line-interactive UPS operation



Online UPS normal operation (solid line)
1. AC power is brought into the UPS and cleaned up by the filter and converted to DC by the rectifier.
2. The battery is charged and outputs DC to the inverter.
3. The DC is converted to AC and provided to the attached devices.

Online UPS abnormal power operation (dashed line)
1. When the battery has died, the attached devices still receive power through the bypass circuit.

FIGURE 19.18 Online UPS operation

Protection Measures

The EPA's Clean Air Act sets national standards for pollutants. Particulate matter (PM)—or airborne particle pollution—is among these pollutants. PM can be extremely detrimental to humans, causing respiratory problems or loss of visibility due to haze or smog. Make sure you always wear an air filter or mask when working in any environment where harmful airborne particles such as dust and debris are present. For **dust cleanup**, use a vacuum to remove PM where possible.

Some companies utilize an enclosure assembly for desktops or laptops to protect parts from PM and other hazardous conditions. Such a case is constructed to house a computer while allowing access to operate keyboards, mice, and flash drives. Some vendors target the military and civilian markets with "rugged" models or enclosures designed for youngsters. Figure 19.19 shows a computer case designed for a rugged environment.

Computer enclosures can also be purchased to protect equipment against impact or weather conditions. One or more air filters may be needed for a nontraditional computer area, such as at a construction site. A kiosk (see Figure 19.20) is likely to contain a lockable area for the computer contained within.

FIGURE 19.19 Rugged industrial computer enclosure

FIGURE 19.20 Kiosk

Temperature and Humidity Control

Computers generate heat. When many units are being used in the same space—whether in a clean room or in a classroom—it may be necessary to provide a cooler ambient room temperature. It is best to look at the location for any computer or network equipment to ensure that it is safe and well ventilated. Computers and network gear operate best in **temperatures** between 60 and 75 degrees Fahrenheit.

TECH TIP

A temperature that is comfortable for you is good for a computer, too

A good rule of thumb related to computer temperatures is that if you are comfortable in the room, the room is probably an appropriate temperature for the computer.

High levels of humidity can cause computer equipment to short-circuit because the moisture corrodes the contact points and interrupts connectivity. Low humidity increases the chance of a technician causing ESD and causing damage to electronics when handling them. Dust and debris abrade, plug, and smother connection points and retard or interrupt flow of electricity.

Temperature and humidity are both important in the care and operation of computers and other electronic devices. For example, if a laptop is left outside in a car overnight in the winter and brought inside to a warm area in the morning, condensation will most likely form inside the case. Over time, this would reduce the effectiveness of the connectivity points. It could also prevent the computer from booting properly when first turned on.

Proper **ventilation** is important for any electronic device. Check to make sure a unit's fan is not blocked. Heat generated from an electronic device, if not properly ventilated, can cause overheating and damage to the unit. Refer to Chapter 5 for more information on temperature and humidity control.

IT Documentation

For IT personnel, technical skills are important, but written and oral communication skills are just as important. A negative trend in recent years in those entering the technical arena is the decline in the ability to write clearly. Although being able to write clearly is important when documenting what has been done in the IT department, it is not everyone's favorite thing to do (see Figure 19.21).

FIGURE 19.21 Documentation is required of IT personnel

Every IT job requires documentation, and frequently this documentation is part of a standard operating procedure (**SOP**) that details what to do to complete a specific task, such as the procedures and approvals that must be done for custom software to be installed. Here are some examples of IT documentation:

- Help desk personnel must log initial problems.
- PC repair technicians must document what was done for billing and historical purposes.
- Technicians are required to close help desk problems with a written explanation of what was done.
- Updates to departmental documentation must be made in some instances.
- Regulations or corporate policies may require some documentation when an incident occurs.

In order to understand common operational procedures related to documentation, let's look at the practices associated with several types of documentation:

- Network topology diagrams
- Service-level agreements (SLAs)
- New user/exiting user checklist
- Knowledge base/articles
- Artificial intelligence (AI)
- Incident documentation
- Asset management
- Policies

Network Topology Diagrams

In addition to creating documentation, IT personnel must often update documentation. This might include using and updating **network topology diagrams** when moves, adds, or changes (MACs) are done, such as when someone changes cubicles or new personnel are due to arrive. You might have to refer to a network topology diagram to get an IP address of a printer being installed or update the diagram to document what IP address you assigned to the printer. A network topology diagram might be a high-level one, as shown in Figure 19.22, or a more granular drawing. Some network drawings are very detailed and include port numbers, IP addresses, VLAN numbers, rooms and locations of access points, and so on.

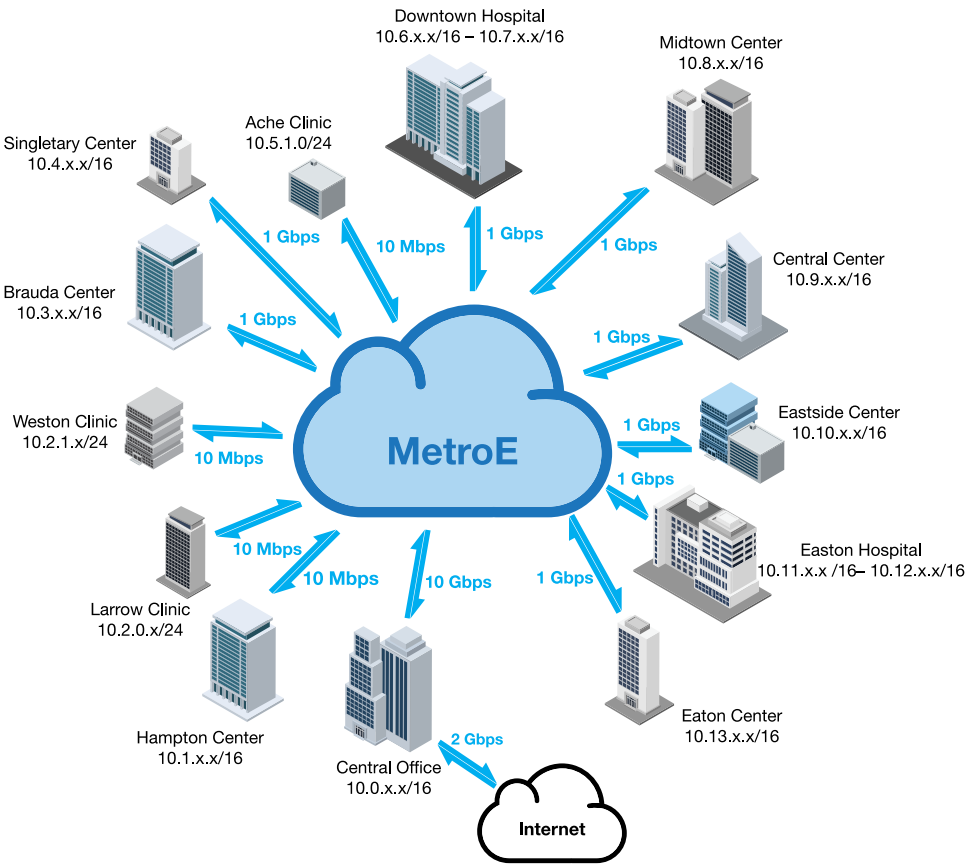


FIGURE 19.22 High-level network topology diagram example

Service-level Agreements (SLAs)

Network outages need to be documented. For connectivity between sites or to the internet, a company is likely to have a service-level agreement (**SLA**) with an external/third-party provider. Usually the SLA calls for very high "up time." Medium to large companies may also have an internal SLA that defines the up time expectations for the wired and wireless networks. SLAs may also exist between one company and another computer, network, programming, application, cloud, or IT services companies.

New User/Exiting User Checklist

Many companies have specific IT-related tasks that are completed for a new employee, for an employee who is leaving, or for an existing employee who is moving. These tasks might include delivering a newly imaged machine or receiving any issued equipment or adding the person or removing their name and ID from the company directory, printers/copiers, phone directory,

authentication database, and email server. When a new employee is assigned, a typical checklist includes the following:

- Office location
- Need for a local printer or access to a network printer
- Need for any mobile devices
- Specialized software needed or customization of software
- Access to shared mailboxes, drives, or folders

Knowledge Base/Articles

A knowledge base is extremely helpful to a technician when solving a problem. A **knowledge base** is a collection of documents that provide answers to commonly asked questions and describe solutions to common problems. Examples of information included in a knowledge base include the following:

- How to reset an IP phone password
- How to request a wireless guest account
- How to report a spam or phishing incident
- How to configure a mobile device for email
- How to configure email with an out-of-office message
- How to do a web conference
- How to find and print to a network printer

A technician might copy information from a knowledge base document to send to a user or might directly send them a link to a document. Some companies or technicians might have collections of online articles that answer commonly asked questions and are used to help the technicians themselves and/or users. Apple, Microsoft, and other IT vendors also have their own knowledge bases to support their hardware, operating systems, or applications.

Artificial Intelligence (AI)

An emerging resource for finding information is artificial intelligence (AI). **AI** is a technology that uses collected and analyzed data to solve problems, learn from the data, and improve over time. AI makes use of machine learning, which is the ability to use computer systems to learn and adapt using algorithms and data. When you ask a question on your smartphone or type in a question on a website, you may get an AI-generated response. AI is also used in self-driving vehicles, speech/facial recognition, and virtual assistants. You can see its use in applications such as supplying corrected spelling, providing words/phrases, and generating resumes, papers, videos, presentations, data analysis, and predictive logic. You may be familiar with Apple's Siri, Amazon's Alexa, Google Assistant, or Microsoft Copilot.

AI is being used to provide first-level help desk support. Even though some jobs are being replaced by AI, the World Economic Forum projects that AI will create 25 more jobs than it replaces. In some industries, an **AI policy** may be in place that dictates when it is appropriate to use AI. When a company has a specific purpose for AI, that is known as a **private AI**. In contrast, a **public AI** app can be used by anyone, and its algorithms, datasets, and training models are pre-set and usually for general purpose. Private AI typically has greater data security, controlled data sources, and more control over data privacy than does public AI.

Because AI draws information from many sources, plagiarism is a problem, and a person obtaining AI-generated information has no idea where the data came from. **AI hallucinations** are a common problem that occurs when AI provides information that is plausible but factually incorrect or fabricated. Anyone using AI should realize the limitations and fact check any information provided. AI-generated information could also have biases due to the inherent flaws in the underlying data and

training, such as inaccuracies or preexisting biases and the design of the algorithms. Because this is an evolving technology, various stakeholders—including developers, policymakers, and industry groups—are working on establishing ethical guidelines, reviewing algorithms, and ensuring the use of inclusive datasets.

Incident Documentation

Incident documentation is used when an IT problem is solved. Most companies use an incident management system, a help desk, or some type of ticketing software for this. It is critical for technicians to clearly and succinctly document a problem, update the problem with progress notes, and then document what was done to solve the problem for historical and billing purposes, to keep track of how much support each department receives, and to help other technicians deal with similar problems in the future. Ticketing systems commonly require user information, device information (including location), and a description of the problem. Some companies use categories, such as servers or PC repair, so that problems can be directed to the correct IT divisions. The software might also allow users to assign severity levels, and a technician might need to become familiar with how to escalate a problem and the different escalation levels. Common information contained in incident documentation is shown in Figure 19.23.

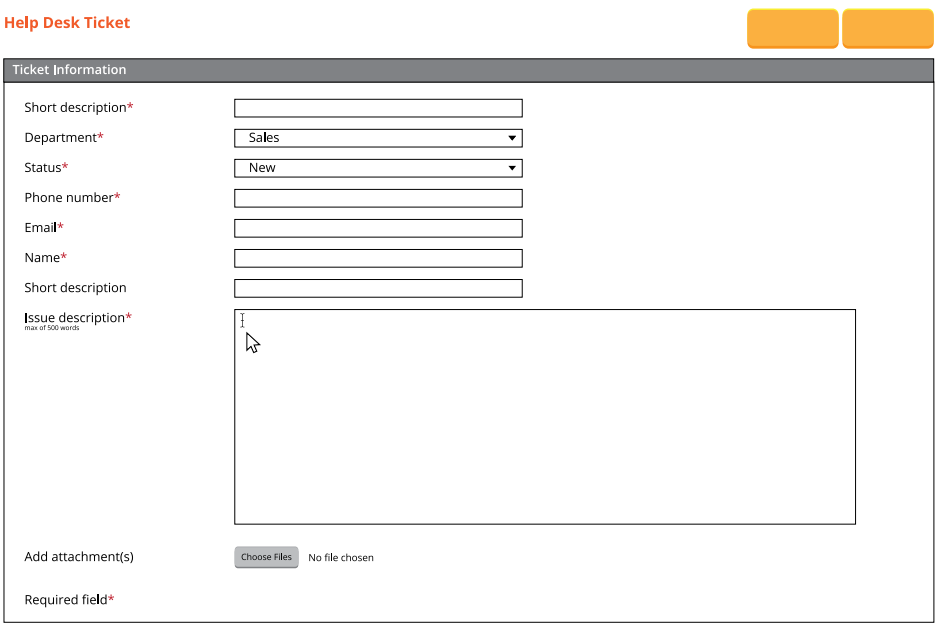


FIGURE 19.23 Help desk ticket example

At the end of a service call, a technician should provide the proper documentation on the services provided. This could include the following:

- Manuals
- Software or hardware boxes and materials that include proof of purchase, UPC codes, activation codes, registration numbers, and warranty information
- Invoice
- Research or information used in the repair that might benefit the customer
- Service ticket with details of work performed

Asset Management

IT personnel have to deal with new parts, computers, printers, and network devices all the time. Change is constant. It is important that you at least know what goes into getting those IT assets

through the **procurement life cycle**. It all starts with the planning process and defining what you want in a particular asset. That takes research. Then you set up a process for how to evaluate and select a specific product; in many cases, this is done in conjunction with the purchasing department. In medium-size to large companies, the purchasing department sends out quotation requests, and then a particular vendor is chosen and awarded a contract. Then comes the receiving/storage process, followed by delivery and implementation.

Many technicians do not like dealing with inventory management, but it is a fact of life in IT. Hardware is commonly documented using an inventory management system. Some help desk software or a configuration management database (**CMDB**) can be used for inventory management. A technician may use the inventory management system to print or view an **inventory list**. In addition, when a technician moves or installs a new piece of gear, they use the system to enter an **asset tag** number, which is a unique ID or an asset ID, and the relevant technical details, such as model number, serial number, and possibly the MAC address for a wireless device. It is also important to track **licensing** and **warranty** information as part of the inventory management process. The inventory management system shows the assigned user who is responsible for the hardware/software.

Inventory must be recorded regularly—typically once a year. As part of this process, a technician may be asked to use a scanner to scan the barcode on any item that costs over a specified dollar amount (see Figure 19.24). Items that cannot be found during the inventory period must be searched for and accounted for. Unfound items are listed on a report that is given to the executive leaders and board of directors. The report affects assets shown on the company balance sheet as well as net income on the income statement, and these write-offs can negatively affect both current employee bonuses and future capital budgets.

FIGURE 19.24 Technician doing inventory

Policies

Technicians may have to refer to specific policies in the normal course of their job or when issues arise. Four policies commonly relate to computer technicians:

> **Password policy:** Even though users are presented with information regarding the **password policy** every time they reset a password, they commonly request technical assistance with the process.

- **Acceptable use policy:** Any service/app used today will be subject to an **acceptable use policy** (AUP), and businesses also have their own AUPs that define what is allowed to be used or done when connected to the corporate network or using company-owned hardware/software. Technicians need to be familiar with the AUP and should refer users to it when necessary.
- **Regulatory and compliance policy:** Every industry (for example, healthcare, manufacturing) has unique regulations and compliance policies. For example, you may see a **splash screen** that states the criteria for accessing a device, a service, or a website. A technician must be familiar with any **regulatory and compliance policies** that apply because IT systems cross all departments within a company.
- **Security policy:** A **security policy** should outline what to do when a breach or an incident occurs, and it may include the AUP and password policy. Security policies are constantly being updated, and technicians should review them on a regular basis.

A technician does not need to know these policies verbatim but does need to know the gist of them and where to find them easily (see also Chapter 18, "Computer and Network Security").

Change Management

The IT department, whether in-house or outsourced, is a key part of any business because IT systems cross all departments. It is very important that an IT department use **documented business processes** and continue to update the documentation related to those processes. The IT department is a constant source of change—moves, adds, and changes (MACs) of PCs, printers, IP phones, monitors, servers, apps, and so on. The IT department should plan for change instead of being reactive to situations. For example, servers that are on old hardware or that have outdated network operating systems are vulnerable to attacks and/or failure. Planning and executing their replacement is better than waiting for each piece of equipment to die.

Change management is an organized way of systematically choosing and implementing IT changes. A business may have a very complex system that includes software that helps the company stay informed about, document, and implement changes. There are three basic situations for change management:

- **Freeze, or change freeze:** A **change freeze** is a time frame during which no changes are allowed to a specific IT system or all IT systems.
- **Maintenance window:** A **maintenance window** is a time frame during which planned changes occur, such as software updates, hardware upgrades, installation of new hardware/software, or platform changes (such as moving systems into the cloud).
- **Unfreeze:** Frozen systems are typically eventually unfrozen. An **unfreeze** means changes can be made again using the change management process

An example might help explain these three change management states. A college is planning a new rollout of the student enrollment system. The IT department would issue a change freeze for a specified number of weeks before the new system implementation so that no changes are made during this time. Then, during the maintenance window, the new system is installed and deployed. An unfreeze occurs after the maintenance window, and changes can be made again using the change management process.

A large company is likely to have a formal board known as a **change board**, change advisory board, software change control board, or change control board (CCB); whatever its name, this group makes decisions about which proposed changes are approved and implemented. Communication is key in change management. Changes are frequently communicated to stakeholders for **peer review**; these stakeholders are given a chance to provide input about the proposed changes.

Instead of using a change board, a company may implement a basic system that is just a formal check of the changes before they are implemented. There are also some changes that don't go through the change management process. These changes are things that don't affect other systems.

One of the most important things to remember about change management is that all feasible steps should be taken to minimize the negative impact of changes on users. Changes can impact users' time, system availability and capability, and security; some changes have consequences that are avoidable.

The management cycle for an IT project commonly involves four phases (see Figure 19.25):

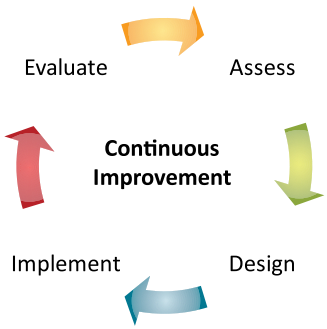


FIGURE 19.25 Management cycle

1. **Assess:** Determine the **purpose of the change**. Why is the change needed? Which corporate strategic goal(s) does the plan align with? The change management process typically starts with a request form and a **risk analysis** to determine the risks involved and whether the benefits outweigh the risks. The form typically lists one of the following change types:
   - **Standard change:** A **standard change** is a planned change—such as a software update, hardware upgrade, hardware replacement, or system change—that is of low risk to the company and preapproved within the department or company.
   - **Normal change:** A **normal change** is a planned change, such as moving the data center or installing a new system.
   - **Emergency change:** An **emergency change** is an unplanned change that resulted from something unexpected, such as a system failure, backup failure, vendor issue, or security breach.

   IT risks are varied. Here are a few to consider:
   - Costs associated with implementation compared to the benefits or potential gain/profits made
   - Skills provided by outside vendors or internal staff
   - Legal or compliance requirements
   - Length of time an upgrade would prolong the life of a system or an application
   - The amount of training and adjustment to new processes and procedures needed
   - The amount of downtime

   The output of a risk analysis is a **risk level** that can be a designation such as low, medium, or high or a numeric value with lowest and highest values provided as a reference. Figure 19.26 shows an example of the risk levels for a risk analysis. In this example, the value 1 is assigned to a proposed change that shows a low likelihood level, which means the risk is not very likely to occur often or to occur at all over a specific period of time, and the severity of the risk or the consequences of the risk are

low. This example also shows that the value 25 means the risk is likely to occur often or constantly and have some painful consequences for the company.

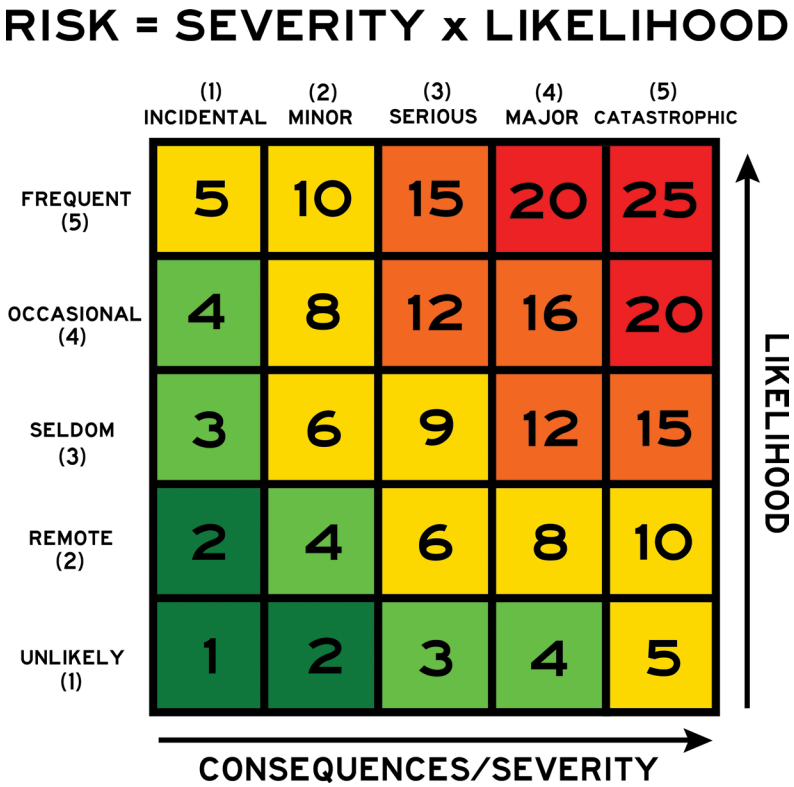


FIGURE 19.26 Sample risk analysis

2. **Design:** Make a plan for the change and share that plan. What is the timeline? What resources are needed? Who will do what? Who is the responsible staff member or manager? Are parts needed? What systems are affected? When will the change occur? What is the **scope of the change**? Defining limits of a project prevents project creep (that is, the tendency of a project to increase in complexity and depth). Project scopes include time, resources, money, deliverables, and acceptance criteria. Are other departments involved? If so, who is the contact person? Can the change be tested in a non-production environment (**sandbox testing**)? Can the change be piloted so it doesn't impact the company so much? Can **IT automation** help by delivering modifications to devices or applications, relieving humans of the job of making repetitive changes to multiple systems? What is the **rollback plan**, or at what step do things get reversed if the changes are not working? This might include reviewing the backup plan and testing backups in advance to ensure that they work. (See the "Backup/Restore" section in Chapter 18 to review the different types of backups.) A rollback plan, sometimes called a backout plan, might be part of a document called a statement of work (SOW) that outlines all activities, deliverables, timelines, reporting structure, and quality checks.
3. **Implement:** Execute the plan. Have meetings or establish an online method to share progress. **Document changes**. Correct any issues that are discovered. Have an **end-user acceptance** process in which the person who will be using the IT system verifies that it works appropriately.
4. **Evaluate:** Ensure that each part of the plan was done properly. Document findings.

IT projects tend to be repetitive in nature in that a project that has been finished will have to be done again in the future; documentation and lessons learned are therefore very important.

SOFT SKILLS: SKILLS TO SUCCEED

The importance of good work habits cannot be stressed enough, no matter where you are or what situation you are in. Good communication skills are priceless. Throughout history, battles have begun because of miscommunication and feuds have been sparked by careless comments. Many good relationships falter and/or disintegrate because people don't communicate with one another well. A poorly worded communication, an off-hand remark, a facial or hand gesture…any of these may be misinterpreted by the receiver without the sender even realizing that they have just offended someone. Let's explore some areas in which your job as a computer technician will involve good communication skills.

Customer Service

What comes to mind when you hear the two words *customer service*? A feeling of security and confidence? A rising panic accompanied by a fervent search for antacids and aspirin? Being of service to others is very rewarding, educational, and fun! Be the best customer service representative that you envision a customer service person to be. You have the skills and training to be tops! Let Figure 19.27 inspire you as a computer technician.

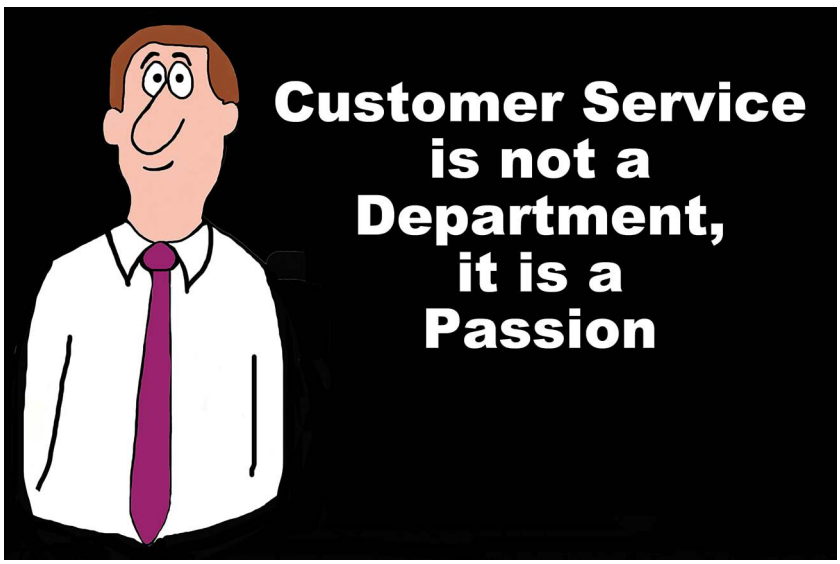


FIGURE 19.27 Customer service inspiration

You can set the tone and instill assurance by being the confident, caring professional that you've trained to become. You are the expert. You know more about computer problems than the customers, and they are looking to you to solve their problems. You have many avenues for tracking down solutions. Don't be shy about tackling new things. Stretch yourself. Allow new situations to be learning opportunities. Step out of your comfort zone.

When you have been called in to fix a company's computer, have your ID badge visible. Introduce yourself and state your business. Ask to speak to the person in charge of the device and wait until you are invited or escorted to the work area. Some customers like to hover—out of curiosity, safety concerns, boredom, insecurity, or for some other reason. Don't let that bother you. Reassure your customers that you are working diligently on their problem and are taking care of them. Other clients will disappear, and you won't have any interaction with them the entire time you're working. As long as you have their contact information, no problem. Focus on the task at hand.

Proper Language

Always address customers by their title: Dr. Schmidt, Mr. Schmidt, Director Durrence, Miss Hannah, Your Honor, Officer Young, Professor Brauda, and so on. Most dictionaries have a section in the back that lists titles and proper forms of address. Mind your manners.

Grooming

Be neat, clean, and well groomed. Wear clean clothes and good shoes. Wear properly fitting attire that will allow you to get in hard-to-reach places when needed (see Figure 19.28). If you are new to IT and unsure about attire, look again at the "Soft Skills" section of Chapter 10, "Mobile Devices," which discusses appearance. Be sure to match your attire to the environment. Three common environments are formal (such as a board meeting), business casual (for everyday work), and casual (for dirty work, such as cleaning out a wiring closet).

Employ good hygiene. Wash your hands and brush your teeth at least twice daily. Carry breath mints. Do you have dandruff? Do you smoke? Did you just enjoy a spicy lunch? Do a self-check before meeting a customer to avoid offending anyone or embarrassing yourself or the customer.

FIGURE 19.28 Dress appropriately

You are your most valuable asset. Take care of your body, mind, and spirit. Your inner self will be reflected outward. Dress like the professional you are. Always have clean hands when handling someone else's property. Never pick up or handle anything if you've been eating, drinking, or have just applied hand cream (which can leave a residue that might not come off). If you use cologne, hair spray, perfume, or scented lotion or cosmetics, avoid using too much as some people have reactions to odors (such as migraines, coughing episodes, or breathing problems).

Be Organized

Be able to flip open your case and pull out exactly the tool or paperwork you need. Not only does being organized save time, frustration, and, ultimately, money, it instills confidence in both your client and you. Rate yourself on organization skills (see Figure 19.29) and make organization a goal. Keep in mind that a messy, fumbling technician would not make a very good impression. Before going on a service call or calling a customer, have all the relevant parts, paperwork, tools, and so on organized and easy to locate.

Pick up after yourself and leave the area at least as clean as it was before you arrived. Reassure your customers that you are working diligently and systematically on their problems and are taking care of them. Focus on the task at hand.

FIGURE 19.29 Organization measure

Use Proper Language

Avoid using slang, profanity, and jargon. Avoid acronyms. (An acronym is a word formed from the first letter of each word in a longer term, such as SATA.) Every profession/industry has its own vernacular, and you don't want to confuse or intimidate your customers by using "geek speak" (see Figure 19.30).

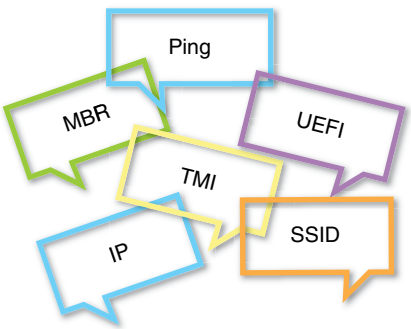


FIGURE 19.30 Avoid "geek speak"

Polish up your grammar skills. Rather than saying "Don't them look good?" or "I seen it doing this," say, "Don't they look good?" or "I saw it doing this." Do not use double negatives, such as "I don't got no paper with me." Brush up on your spelling and punctuation skills. Understand and properly use words such as too, two, and to; there, they're, and their; lie vs. lay; and so on. Write your reports in complete sentences. Type in a word processing application to get grammar suggestions. Then paste the text into an email message or technical support problem logging application.

Maintain a Positive Attitude and Project Confidence

Walk through the door with a purpose and a smile! Stand up straight, shoulders back, with your head held high. Offer your hand in friendship. Emphasize your customer's value with kindness, respect, and gratitude. Project confidence. The customer will be relieved to see you.

In many IT jobs, there is more work to do than time to do it. Technicians must constantly juggle to keep up with it all. Make sure you take allowed breaks and do non-technical things. If you are sitting in an office, greet and acknowledge a visitor as soon as possible. Use a phone or a tablet to

keep reminders for the day. If you are going to be late, call and let the customer know. Customers are often happy to rearrange their schedule and tasks to be available when a technician is coming. Courteous promptness will be rewarded.

Actively Listen

Listen attentively and maintain good eye contact. The customer will tell you what they want. Take notes. If using a tablet, explain to your customer that you are entering information about the problem to help figure out a solution. Be up front and let the customer see what you are doing.

Avoid interrupting the customer. Don't assume anything. Avoid finishing your customer's sentences to avoid seeming like you are rushing the customer. Make sure you are clear in what you are asking the user. Clarify their statements by asking open-ended questions to narrow the problem area, restate the issue, or further question them to verify that you understand the issue. Open-ended questions such as "What were you doing on the computer when the problem occurred?" or "What made you think there was a problem? How did the computer act differently?" After the customer has explained the problem, repeat it back to them to make it clear that you both understand the situation. Ask the customer what they would like to see happen (see Figure 19.31).

FIGURE 19.31 Building rapport with customers

Be Culturally Sensitive

Take the time to know your customers. Understand and accept that there will be differences between people, and it is not your place to judge. Be aware of things that you do that might be offensive to others. Always try to put yourself in your customers' shoes. Be aware of any facial expressions, hand gestures, or body movements you tend to make that may be deemed offensive or insulting. If the customer is doing something that you find offensive, you can politely ask them to stop. For example, if someone feels compelled to tell you a joke or an anecdote that is degrading, belittling, or humiliating to another person, immediately and politely ask them to stop. If the behavior continues, you could say, "I'm trying to do a professional job here, and I am offended by that."

Be on Time

It is better to be 10 minutes early than 5 minutes late. If something causes you to be late in reaching your next appointment at the agreed time, call that customer as soon as possible. Customers commonly get angry when techs are late, and by calling ahead, you can give them time to adjust. If you have kept a customer waiting—whether on the phone or in person—apologize, ask if you may go ahead with the work, and thank the customer. Be gracious.

Time Management

Time management is how much time you budget and then actually spend on doing each task throughout the workday. IT personnel tend to have busy schedules (see Figure 19.32). Be aware of how you might improve your time management and the things that contribute to time management.

FIGURE 19.32 Time management

Always remember that you are a paid employee, and time is money to the company. If you encounter a chatty person, politely explain that you are on your company's billable hours. Emphasize that you like to stay on schedule for all of your customers, and it's best for you to stay on task. Steer the customer toward talking about the problem at hand in a constructive way. For example, if the person is frustrated and is just blowing off steam, politely suggest that perhaps a break or a drink of water might help. This would allow some cooling-off time for the client and time for you to work alone. If the person becomes confrontational, it may be a good time for you to take a break.

Avoid Distractions

Give your customer your undivided attention. Be in the moment. Here are some best practices:

> Turn off your cell phone or switch to vibrate mode so that you are not interrupted with personal or professional calls.

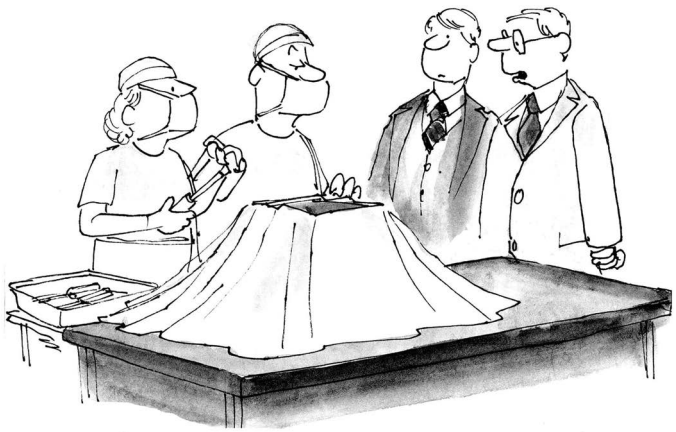
> Avoid looking at social media sites and doing any texting until you have finished with your customer.

- Avoid talking to coworkers while interacting with a client.
- Avoid gossiping.
- Avoid personal interruptions.
- Avoid checking your watch, drumming your fingers, yawning, rolling your eyes, sighing, and so on.

The most common customer complaints related to techs are that they feel ignored, not listened to or taken seriously, passed over or put aside, or kept waiting. Do what you can to ensure that you don't have any of these effects on your customers. Smile with your eyes as well as your mouth. Be pleasant and avoid being condescending. Avoid regaling your customers with stories of your personal life. This doesn't mean that small talk is off-limits. Just remember to keep it appropriate and professional. Remember that the customer is concerned about the immediate problem.

Don't Make Commitments You Can't Keep

Part of being professional is having integrity. Be businesslike with clients and ensure that the subjects you talk about are relevant to the job. Even though the tone is light in Figure 19.33, the point is to be professional and take your job seriously.



"The computer repair people take their job very seriously."

FIGURE 19.33 Be professional

Do not make off-handed promises in hopes of appeasing a client and don't make commitments you can't keep. It is much better to say, "I am not sure how long this will take [or cost]" or "I am not qualified in that particular area, but I can check on that for you and get back to you." Don't be afraid to call someone else for help. For example, if the problem you see is out of your area of expertise, call someone who is more experienced. If you do not have time to fix a particular problem but have committed to doing so, ask another technician for help. Many companies have tiers of technical support. There is probably someone senior or a manager who can offer you some advice after you have done all the research you can and exhausted your resources.

Dealing with a Difficult Customer or Situation

When you are faced with an uncomfortable situation, above all remember to breathe deeply and slowly. Not only will this provide your brain with oxygen-enriched blood, it will give you a moment to think and compose yourself before you answer. Here are some suggestions for dealing with difficult customers:

- Let the customer talk.
- Make good eye contact and give physical affirmation cues (for example, nodding your head "yes").
- Do not ever tell someone to "calm down." That is akin to scoffing and saying, "You don't have a legitimate complaint." Telling someone to "calm down" is likely to increase the person's anger.
- Do not argue with a customer or be defensive. Remember that the customer has been stewing and fuming about this particular problem and wants to tell you every last detail about it. Listen to them and don't interrupt or try to finish their sentences.
- Remind yourself that you have been trained in this field and are the expert. Don't dismiss the customer's problems. Acknowledge that they are understandably upset, frustrated, angry, and so on, and reassure them in a calm, steady voice that you are there to help.
- Avoid being judgmental.
- Be personable yet professional. Replies such as "I'll do my absolute best to help you" or "I'm sorry that this glitch has been so upsetting to you" or "Let's see what I can do for you" can go a long way toward defusing the situation. Let the client know that you have a hearty interest in their well-being—that you are genuinely concerned with helping.
- Be careful not to giggle or laugh inappropriately, or the customer may mistakenly think you are making fun of, belittling, or dismissing the problem.
- Avoid laughing constantly while talking. Some people do this—whether out of nervousness or habit—when engaged in conversation. Constant laughing could cause the other person to wonder what is so humorous about the situation.
- Always keep in mind what your customers want, need, and/or expect from you (or your company). Offer different repair/replacement options.
- Utilize resources that are available to you from which you can pull answers to solve the problem.
- Don't post work-related frustrations or experiences to social media sites. Use discretion and professionalism when discussing experiences/encounters.
- Go over and above the expected service.
- Pay attention to detail.

In order to keep the customer focused on the problem at hand, clarify customer statements by asking open-ended questions to narrow the scope of the problem; if necessary, restate the issue or ask questions to verify your understanding of the problem. Gently guide the customer by restating the problem and expanding a bit on the description. Do not frustrate a customer who seems to have some technical skills. Ask more open-ended questions to speed up the troubleshooting process, if possible. After the job is complete, be sure to follow up with the customer by allowing time for them to ask questions and thanking them for the opportunity to serve. Feedback keeps the lines of communication open and flowing between you and nurtures the active work relationship that is so vital to good customer service.

If someone is invading your space (getting too close for comfort), try stepping back a step. If this does not work, stop what you are doing, look the person in the eyes, and politely ask them to give you more room. If someone is verbally abusive to you or even physically abusive, step back and raise a palm (see Figure 19.34). Prevent the situation from escalating by keeping your voice in an even, professional tone. You can always ask the person to take a short break or excuse yourself to give them a moment. You have the right to a safe work environment.

FIGURE 19.34 Stop what you are doing; stay back

Set and Meet Expectations

A customer usually wants to know when their computer will be fixed. If you must give an estimated repair time, estimate a little longer than you anticipate. That way, if you finish earlier than you expected, you'll both be happy! Discuss and offer different repair or replacement options, if applicable. Keep your customer informed of your progress. A small morsel of information from time to time helps quell the anxiety about an unknown situation ("Here's where we are now…" or "Just checking in to let you know that…"). This type of interaction reassures the customer that you are actively working to fix the problem. No one likes wondering or waiting. Think back to when you first encountered problems and frustrations when working with a computer. Treat others as you would like to be treated.

Appropriately Handle Confidential and Private Materials

Discretion is another integral part of professionalism. Remember to be cognizant of all who may be in the area. Keep information private; for example, hard copies and faxed materials should be secured in folders—not spread around on a table for any passerby to read. Speak in such a manner that no one else can hear. Keep your laptop and mobile devices password protected. Keep your own personal information private. You wouldn't want a third party to expose your private information, would you?

When working for a client, if you notice what seems to be sensitive information (for example, passwords taped somewhere, documents left in a printer, employee evaluations), it is best practice to ask the client to remove that information. Also, it is prudent to notify the client if you might have inadvertently seen sensitive information so that the client can take any necessary measures (for example, change the password). If you spot a bad security practice such as a password taped somewhere, take the opportunity to talk about security in today's environment.

Never discuss a customer's business or your professional matters with anyone—while sitting in a restaurant, at a public venue, on social media, or even in off-hand conversation. A 1942 American World War II poster by Designer Seymour R. Goff exclaimed, "Loose lips might sink ships," meaning it's important to beware of frivolous or unguarded talk because you never know who may be listening.

Closing Remarks

No IT person is perfect. All you can do is strive to be the best professional possible. Try to do the right thing, be professional, be honest, and apologize if you are in the wrong, and people will recognize that you are doing the best you can. Keep learning. Even if you remain in the same job for some time, there will be new technologies and areas that you can improve upon.

Good luck to you in your IT profession! It is a wonderful field, and there are always opportunities to slide into something new. An inspiring quotation to leave you with comes from Vincent van Gogh: "Your profession is not what brings home your weekly paycheck. Your profession is what you're put here on earth to do with such passion and such intensity that it becomes spiritual in calling."

Chapter Summary

- Three of the most important items you should have in your technician kit are safety goggles, gloves, and a dust mask/air filter mask. These are your PPE.
- Power issues include overvoltage conditions such as a surge or spike that can be managed with surge protectors, power conditioners, and UPSs. Power conditioners and UPSs help with undervoltage conditions such as sags. Two types of battery backups are UPSs and SPSs. A UPS is the only device that powers a computer when a blackout occurs.
- Ensure that a surge protector has a Class A rating and adheres to the UL 1449 standard.
- You have the right to expect a safe working environment. Federal government agencies such as OSHA and the EPA work hand in hand with state and local governments to regulate, enforce, and promote safe work practices—both for individuals and for the environment.
- A good computer technician knows how to recycle and/or dispose of electronic waste (specifically how to handle batteries, toner cartridges, CRT monitors, PCs, cell phones, and tablets) and understands the importance this makes to the health of humans and the environment.
- Federal government agencies, such as OSHA and the EPA, work in tandem with state municipalities and local governments to monitor environmental impacts of toxic waste. Batteries, mobile devices, computers, and printers all contain toxic metals that, when tossed into landfills, can leach out into the surrounding soil and water. Most municipalities have electronic waste recycling/disposal toxic waste handling sites.
- IT documentation is an important part of any IT staff member's job and is used for reference and sometimes requires updating.
- Change management is a requirement for documented business processes within IT. A risk analysis should be done as part of the change management process to determine if a change is worth the risk of implementation. A rollback and backup plan should also be part of any IT project.
- Proper communication and positive interaction with customers are required of IT professionals. Avoid using profanity, jargon, and slang. Address customers by using their title and surname.
- Attentiveness to customers means making good eye contact, listening actively, avoiding interrupting or finishing the customer's sentences, and taking detailed notes.
- Keep personal business and activities out of the workplace.
- Hygiene, appearance, manners, and confidence are important traits to possess.
- Look, act, dress, and think like a professional, and you will be a professional.

A+ CERTIFICATION EXAM TIPS

- ✓ Be cognizant of personal safety techniques and issues, including removing power before working on a PC, being careful while lifting and minding weight limitations, taking measures to know and promote electrical fire safety and cable safety, and using an air filter mask and/or safety goggles when appropriate. Be sure to comply with all local government regulations.
- ✓ Know the purpose of MSDSs and the documentation associated with handling or disposal of materials. Also be familiar with temperature, humidity, and ventilation requirements for electronic equipment. Be cognizant of where to place equipment based on these requirements. Clean up dust and use compressed air and a vacuum when needed.
- ✓ Compare equipment needed for power surges, brownouts, and blackouts, including battery backup options and surge suppressors.
- ✓ Explain equipment grounding and be familiar with proper component and power handling, including the use of self-grounding techniques, antistatic bags, ESD straps, and ESD mats. Be familiar with government safety regulations.
- ✓ Describe environmental impacts and local environmental controls for batteries, toner, and other devices and assets, such as PC hardware, CRTs, cell phones, and tablets.
- ✓ Be familiar with and know when to use the following types of documentation: knowledge base articles, incident documentation, regulatory and compliance policy, acceptable use policy, SLAs, regulatory compliance requirements, incident reports, and standard operating procedures (which may also include standard things, such as a new user or user termination setup list, and things that are not so standard, such as the requirements for a custom software package installation).
- ✓ Be familiar with how asset management and the procurement life cycle relate to IT, including inventory lists, a database system, asset tags/IDs, barcodes, assigned users, and warranty and licensing information.
- ✓ Be familiar with IT ticketing systems and the information that is entered or provided to IT staff: user, device, problem description, category, severity, and escalation levels. Be sure to use clear and concise information when documenting a problem, including progress notes and the resolution.
- ✓ Be able to describe best practices related to documentation and change management. Be able to explain the difference between a change freeze and a maintenance window. Know the differences between standard, normal, and emergency changes. As part of the change management process, describe the purpose of a change, the scope of the change, and a plan for the change. Include a risk analysis and provide a risk level to determine whether the change is worth the business risk. The change implementation might include sandbox testing to lower the risk factor. Include peer review and end-user acceptance testing as part of the plan. Documentation should include a rollback and backup plan as well as information on the changes implemented.
- ✓ The change management process may include a change board that determines whether an IT change is approved. A document that might be created in the change management process is a SOW, which outlines the purpose and scope of the plan, affected systems and impact on the company, responsibilities, responsible staff member, due dates, and a rollback plan.
- ✓ Communication techniques and key areas of professionalism include the following: Dress appropriately for the job and situation (whether in formal or business casual attire); use proper language; maintain a positive attitude; project confidence; actively listen; avoid interrupting the customer; be culturally sensitive; use appropriate titles; be on time; avoid distractions; be able to deal with a difficult customer or situation (don't argue or be defensive, don't be dismissive regarding the problem, avoid being judgmental); clarify customer statements with open-ended questions; set and meet expectations; communicate the status of an issue's resolution with the customer; and deal appropriately with customers' confidential and private information.

✓ At this point, you've learned about every topic that is covered on the CompTIA A+ exams. Now you should take time to specifically prepare for the certification exams and get the professional credentials you have earned. Refer to the Introduction to this book for details on the 220-1201 and 220-1202 CompTIA A+ exams, including how to sign up for them. And note that Pearson, the publisher of this book, is offering you an exclusive deep discount on several types of certification exam preparation resources. See the Introduction to this book and the advertisement inserts in the back for more details. Take a look at what Pearson has to offer and figure out which resource(s) would work best for your study style. Good luck!

Key Terms

acceptable use policy, AI, AI hallucinations, AI policy, air filtration mask, antistatic bag, asset tag, blackout, brownout, cable management, change board, change freeze, change management, CMDB, compressed air, document changes, documented business processes, dust cleanup, electrical fire safety, emergency change, end-user acceptance, equipment grounding, ESD mat, ESD strap, humidity, incident documentation, inventory list, IT automation, knowledge base, licensing, lifting technique, line conditioner, maintenance window, MOV, MSDS, network topology diagram, normal change, OSHA, overvoltage, password policy, peer review, power surge, private AI, procurement life cycle, public AI, purpose of the change, regulatory and compliance policy, risk analysis, risk level, rollback plan, safety goggles, sandbox testing, scope of the change, security policy, self-grounding, SLA, SOP, splash screen, SPS, standard change, surge suppressor, temperature, time management, toner, Type A-B-C fire extinguisher, Type C fire extinguisher, undervoltage, unfreeze, UPS, vacuum, ventilation, warranty

Review Questions

1. You are working in an area that has multiple cubicles with multiple PCs. You see smoke coming from the laser printer in the area where you are working. You pull the fire alarm, tell everyone to leave (and they do), and grab the fire extinguisher. Now what do you do?

   a. Push the lever to engage or activate the pump inside the extinguisher.

   b. Pull out the fire extinguisher pin.

   c. Aim the nozzle at the printer.

   d. Squeeze the handle and slowly move the nozzle back and forth.

2. A bank has an IT policy which states that no changes may be made to any system that deals with customer data during the last week of the month because customer statements are being produced. Which change management term does this describe?

   [emergency change | SOW | security policy | change freeze]

3. On which device would a PC technician most likely see a grounding wire?

   [patch panel | air vent | wiring rack | laser printer]

4. A company is implementing new payroll software. The project manager has outlined the scope of the project, responsibilities, due dates, and quality assurance checkpoints. What is missing from this plan?

   [end-user acceptance | network topology diagrams | backup testing | backout plan]

5. A computer technician's repair kit should always include which of the following?

   a. Pen, paper, and ID badge

   b. Soap, toothbrush, and toothpaste

   c. Surge suppressor, laptop enclosure case, and resealable antistatic bags

   d. Safety glasses/goggles, gloves, and dust mask/air filtration mask

6. Which UL rating and surge suppressor class would be best when ordering new surge strips for a small business? (Choose two.)

   [UL 497 | UL 1283 | UL 1449 | Class A | Class B | Class C]

7. Which part of the change management cycle would include an evaluation of whether a particular IT change is worth implementing?

   a. Plan scope

   b. Risk analysis

   c. Backup plan

   d. Plan purpose

8. What is a safety risk related to old or damaged batteries?

   a. They can leak acid.

   b. They can contain lead.

   c. They can contain water.

   d. All sizes are interchangeable.

9. Equipment grounding means which of the following?

   a. The equipment is tethered to a desk.

   b. The components in a computer are all the same voltage potential.

   c. The technician wears a tether device.

   d. Someone could receive a shock or be electrocuted from simply touching the case.

10. Which method is best for cleaning up scattered laser toner particles?

a. Use a hair dryer to blow away the residue.

b. Use moist paper towels to wipe up particles.

c. Use your shirt sleeve to make them disappear.

d. Use a vacuum cleaner equipped with a HEPA filter.

11. In what situations would it be most appropriate for an IT technician to wear business casual attire instead of wearing business formal attire? (Choose two.)

a. When going to a business to repair a PC

b. When meeting with the chief information officer (CIO) and some board members regarding an idea they had for saving money in the department for the company.

c. When presenting the latest departmental statistics on downtime and escalations to the VP of business affairs

d. When attending a virtual meeting of the change management board regarding an upcoming project

e. When representing the company at a local business event

12. What is the best way to dispose of mobile devices, PCs, monitors, toner, and batteries?

a. Burn them in bonfires.

b. Dump them in landfills.

c. Deposit them in a local municipality-approved receptacle.

d. Call 911.

13. In the event of an electrical fire, which types of fire extinguishers would be best? (Choose two.)

a. Type A fire extinguisher

b. Type B fire extinguisher

c. Type C fire extinguisher

d. Type D fire extinguisher

e. Type A-B-C fire extinguisher

14. A device that protects electronic equipment from an increase in power but not a decrease or an outage is a _____.

[battery backup | surge suppressor | CRT | UPS]

15. When encountering a difficult or confrontational customer, the best thing to do initially is which of the following?

a. Step back and take a few deep breaths before responding.

b. Call a supervisor.

c. Suggest taking a short break.

d. Reschedule the appointment.

16. [T | F] Federal, state, and local governments do not interact with one another concerning toxic waste issues.

17. Which safety measure would be helpful in a network wiring closet that is filled with particulate matter (PM) and that is being cleaned for the first time in years as the cabling is reorganized?

a. air filtration mask

b. HEPA vacuum

c. compressed air

d. UL 1449 device

18. Laser toner cartridges _____.

a. are easily recycled anywhere

b. can be donated to charities

c. can be refilled many times

d. must be disposed of in an approved regulated receptacle

19. A user has requested help downloading and installing software on the corporate laptop. Which of the following IT documentation types would a technician use in this case?

[security policy | inventory management | article | network topology diagram | acceptable use policy]

20. Which items would be used as part of inventory management? (Choose two.)

[asset tag | flatbed scanner | incident documentation | barcode | AUP]

Exercises

Exercise 19.1 Determining a Power Solution

Objective: To be able to determine the proper power solution for a particular situation

Procedure: Match one of the power solutions to each situation. Note that a particular power solution may be the answer for more than one situation.

Power solutions:

a. Surge suppressor

b. Power conditioner

c. UPS

d. SPS

____ A company has a very old building that has one corporate division. The company suspects a power issue in the lowest room because the three PCs located there continually reset.

____ A particular network rack has a switch that is used to connect to every executive on a single floor. The president of the company has requested that these executives' computers remain powered as long as possible, even when power to the building is lost.

____ A home tower computer has two monitors, powered speakers, and a printer attached, and it needs to be protected from an overvoltage condition.

____ A cubicle in a company has only two outlets. The cubicle contains a thin client computer, a monitor, and an IP phone.

____ An entrepreneur has a home office with a server that stores company data, a PC, three monitors, and a printer. The owner wants to be protected in over- and undervoltage situations with clean power to all devices.

____ A gamer would like to have power provided even when power to the house is lost but does not want the cost of a UPS.

Exercise 19.2 Determining the Type of Documentation Needed

Objective: To be able to determine which type of documentation is needed in a particular situation

Procedure: Match one of the documentation types to each situation. Note that each documentation type is the answer for only one situation.

Documentation types:

a. Network topology diagram

b. Knowledge base/articles

c. Incident documentation

d. Regulatory and compliance policy

e. Security policy

f. Inventory management

Situations:

____ A technician has solved a problem that required reloading a computer due to a virus infection.

____ A technician has moved a barcoded network printer to a newly created divisional copy room.

____ A technician is responding to a complaint about wireless connectivity in a particular area. The technician needs to know how many access points are in the area and the coverage area.

____ A technician working in a hospital notices that a computer is displaying private patient health information.

____ A person calls the help desk because of a problem with changing the domain password. The technician needs to know the company's exact password requirements.

____ A technician needs to connect an IP phone and needs to know which switch port has been programmed for the appropriate phone VLAN.

Activities

Flip the CLASSROOM

Internet Discovery

Objective: To obtain specific information on the internet regarding administrative procedures

Parts: Computer with internet access

Questions: Use the internet to answer the following questions.

1. Research how to dress professionally for your job. Write three things that impressed you the most about the advice given and whether you found the website helpful or confusing. Write the URL where the information was found.

_____

_____

2. Locate at least two videos of poor technician interaction/service with customers. Compare these scenarios with the lessons in this book and write how the techs in the videos could improve their skills.

_____

_____

3. Research at least two local municipalities that have approved regulated sites for recycling and disposal of computer and electronic equipment. List what they advise for their communities. Describe differences in their regulations. List the URL for each municipality.

_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

4. Research electrical fire safety videos. Combine the information from this book with what you learn from the fire safety videos. Document what new things were shown. How confident are you that you could extinguish an electrical fire? List the URL where your information was found.

_____
_____

5. Research at least five healthy things to do for yourself every day. Decide which ones you'd like to implement. List the URLs where your information was found.

_____
_____

Soft Skills

Objective: To enhance and fine-tune a future technician's ability to listen, communicate in both written and oral forms, and support people who use computers in a professional manner.

Activities:

1. Refine your customer skills by play-acting situations with another student. One student should take the role of the technician, and the other should take the role of the customer. Instead of asking "Did you do _____?" ask "When did you do _____?" "What happened when you did _____?" or "When did you first notice _____?" Rate each other, using positive words. You can give negative feedback, but do it in a positive manner. For example, if the person spoke in a low tone, but the words were good, you might give the following feedback: "Your explanation was very good, but I had a hard time hearing you. You might want to speak up just a bit louder."
2. Hone your job interviewing skills by practicing with another student. Be prepared with questions about the company with which you are seeking employment. Think ahead to what questions a prospective employer might ask you.

_____
_____
_____

3. In a group with other students, inspect the fire extinguisher in the room and then research electrical fire safety. After becoming familiar with fire safety signs and exit routes for the classroom, create a scenario to demonstrate fire safety. Produce an escape route, act out the scenario, and present an escape route drawing to the rest of the class.
4. Build a virtual wardrobe that is appropriate for your future job. Research websites and record in a professionally formatted document descriptions of the garments you would choose. Don't forget accessories such as shoes, hats, purses/briefcases, computer bags, and so on. Share and discuss with other students why you chose specific items. Provide feedback to other students on their choices. Optionally place your findings in a presentation to be shared with others.
5. Using either ChatGPT, Microsoft Copilot, or Google Assistant or Gemini, enter a question about the different methods that can be used to re-image a PC. Document the AI tool you used, the question you typed, and the results. Based on the results, ask another question and document the same information. Document how accurate you think the AI-provided information was. Share in groups of three.

Flip the CLASSROOM

Critical Thinking Skills

Objective: To analyze and evaluate information as well as apply learned information to new and different situations.

Activities:

1. Break into groups of three students. Each group receives a box containing different old electronic devices, components, and/or batteries. With your group, research local municipality regulations regarding recycling and/or disposal of electronic waste. Present your findings to the class. Aggregate all the groups' findings into a single table. Offer to share this table with the school.
2. Engage in conversation with as many friends and acquaintances as your instructor specifies. Ask them about and record specific problems they encounter with their mobile devices and laptops. What problem occurs most? What new problems were presented that were unfamiliar to you? What solutions would you offer to these people? Record all your data in table form and present it to the class.
3. Divide into groups of three or four students. As a group, consider the following information: A local veterans' home has 100 computers and 10 printers; 96 computers and 8 printers are used by the staff, 4 computers and 2 printers are used by the veterans. The computers and printers used by the veterans experience a high rate of downtime. Think of different reasons the veterans' computers and printers might be frequently nonfunctional. Offer at least three solutions to improve the situation.

_____

_____

_____

_____

_____

_____

_____

4. Prepare a change management plan for any of the solutions proposed in Question 3.

_____

5. Use the internet to locate a video that features a technician using poor communication skills. List things that were recommended in this chapter that were not addressed in the video or that the technician could have handled differently.

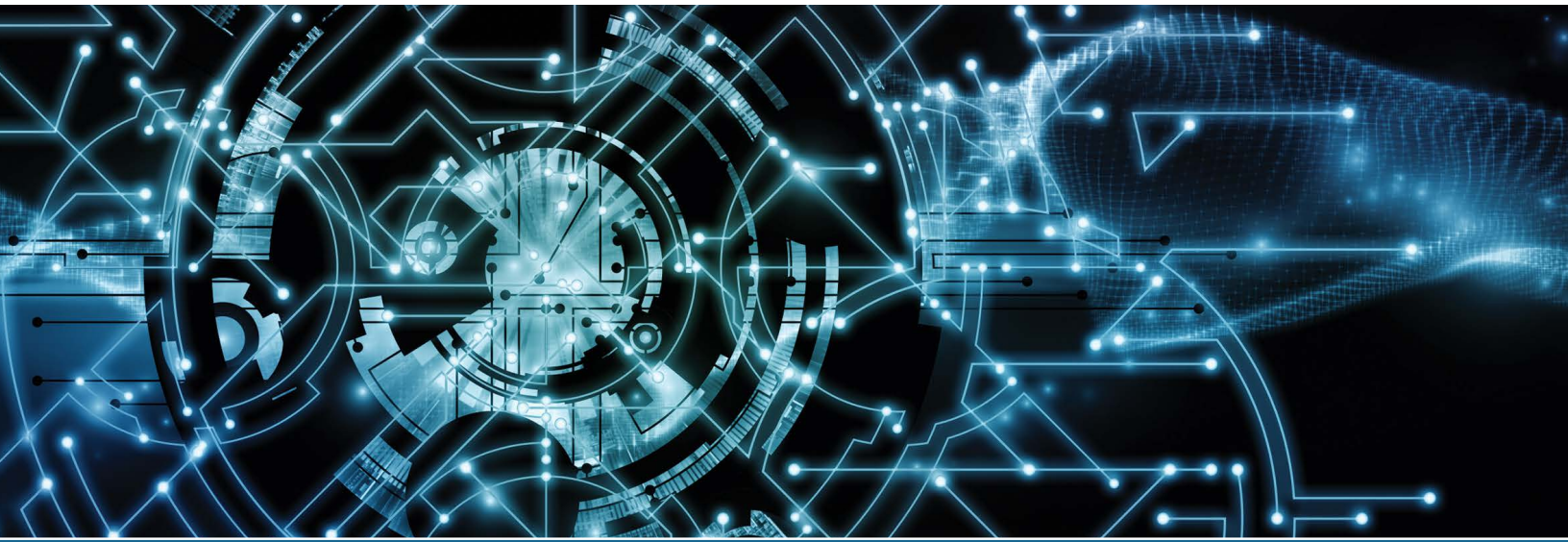
_____

6. Find current news stories that feature safety issues related to technology.

_____

This page intentionally left blank

A Subnetting Basics



In business, the subnet mask assigned to a device commonly is not the default mask based on the class of IP address being used. For example, at a college, the IP address 10.104.10.88 and subnet mask 255.255.255.0 are assigned to a computer. The 10 in the first octet shows that this is a class A IP address. A class A IP address has a default mask of 255.0.0.0. The 255 in the subnet mask is made up of eight 1s in binary in the first octet (11111111) followed by all 0s in the remaining octets (00000000.00000000.00000000).

The purpose of a subnet mask is to tell you (and the network devices) which portion of the IP address is the network part. The rest of the address is the host portion of the address. The network part of any IP address is the same 1s and 0s for all computers on the network. The rest of the 1s and 0s can change and be unique addresses for the network devices on the same network. The following important rules relate to subnetting:

- The network number *cannot* be assigned to any device on the network.
- The network number contains all 0s in the host portion of the address. Note that this does not mean that the number will be 0 in decimal (as explained next).
- The broadcast address (the number used to send a message to all devices on the network) *cannot* be assigned to any device on the network.
- The broadcast address contains all 1s in the host portion of the address. Note that this does not mean that the number will be 255 in decimal.

Consider the IP address and mask used in the earlier example: 10.104.10.88 and 255.255.255.0. Put these numbers in binary, one number on top of the other, to see the effects of the subnet mask:

```
     10          104         10          88
00001010.01101000.00001010.01011000
11111111.11111111.11111111.00000000
```

The 1s in the subnet mask show which bits in the top row are the network part of the address. The subnet mask is always a row of consecutive 1s. Where the 1s stop is where the network portion of the address stops. Keep in mind that this does not

have to be where an octet stops, as in this example. A good technique is to draw a line where the 1s in the subnet mask stop, as shown in the example that follows:

```
      10              104             10        |     88
0 0 0 0 1 0 1 0 . 0 1 1 0 1 0 0 0 . 0 0 0 0 1 0 1 0 | 0 1 0 1 1 0 0 0
1 1 1 1 1 1 1 1 . 1 1 1 1 1 1 1 1 . 1 1 1 1 1 1 1 1 | 0 0 0 0 0 0 0 0
```

TECH TIP

Subnet mask in prefix notation

Subnet masks in network documentation are commonly shown in prefix notation, using a slash with the number of consecutive 1s found in the subnet mask. For example, 10.104.10.88 255.255.255.0 can be shown as 10.104.10.88/24, and 192.168.10.213/27 is the same as a 255.255.255.224 subnet mask.

At this point, there is no other purpose for the subnet mask. You can get rid of it, as shown in the example that follows:

```
      10              104             10        |     88
0 0 0 0 1 0 1 0 . 0 1 1 0 1 0 0 0 . 0 0 0 0 1 0 1 0 | 0 1 0 1 1 0 0 0
```

All 1s and 0s to the left of the drawn line are the network portion of the IP address. All devices on the same network will have this same combination of 1s and 0s up to the line. All 1s and 0s to the right of the drawn line are in the host portion of the IP address:

```
                Network                          Host
      10              104             10        |     88
0 0 0 0 1 0 1 0 . 0 1 1 0 1 0 0 0 . 0 0 0 0 1 0 1 0 | 0 1 0 1 1 0 0 0
```

The network number—the IP address used to represent an entire single network—is found by setting all host bits to 0. The resulting number is the network number:

```
                Network                          Host
      10              104             10        |      0
0 0 0 0 1 0 1 0 . 0 1 1 0 1 0 0 0 . 0 0 0 0 1 0 1 0 | 0 0 0 0 0 0 0 0
```

The network number for the network device that has the IP address 10.104.10.88 is 10.104.10.0. To find the broadcast address, the IP address used to send a message to all devices on the 10.104.10.0 network, set all the host bits to 1:

```
                Network                          Host
      10              104             10        |    255
0 0 0 0 1 0 1 0 . 0 1 1 0 1 0 0 0 . 0 0 0 0 1 0 1 0 | 1 1 1 1 1 1 1 1
```

The broadcast IP address is 10.104.10.255 for the 10.104.10.0 network. This means that hosts can be assigned any addresses between the network number 10.104.10.0 and the broadcast address 10.104.10.255. Another way of stating this is that IP addresses 10.104.10.1 through 10.104.10.254 are usable IP addresses on the 10.104.10.0 network.

Consider the IP address 192.168.10.213 and the subnet mask 255.255.255.224 assigned to a computer in a college. What would be the network number and broadcast address for this computer? To find the answer, write 192.168.10.213 in binary octets. Write the subnet mask in binary under the IP address:

```
   192          168          10           213
1 1 0 0 0 0 0 0 . 1 0 1 0 1 0 0 0 . 0 0 0 0 1 0 1 0 . 1 1 0 1 0 1 0 1
1 1 1 1 1 1 1 1 . 1 1 1 1 1 1 1 1 . 1 1 1 1 1 1 1 1 . 1 1 1 0 0 0 0 0
```

Now draw a line where the 1s in the subnet mask stop:

```
   192          168          10           213
1 1 0 0 0 0 0 0 . 1 0 1 0 1 0 0 0 . 0 0 0 0 1 0 1 0 . 1 1 0|1 0 1 0 1
1 1 1 1 1 1 1 1 . 1 1 1 1 1 1 1 1 . 1 1 1 1 1 1 1 1 . 1 1 1|0 0 0 0 0
```

Remove the subnet mask because it is not needed anymore:

```
   192          168          10           213
1 1 0 0 0 0 0 0 . 1 0 1 0 1 0 0 0 . 0 0 0 0 1 0 1 0 . 1 1 0|1 0 1 0 1
```

Set all host bits to 0 to find the network number:

```
                    Network                          Host
   192          168          10           192
1 1 0 0 0 0 0 0 . 1 0 1 0 1 0 0 0 . 0 0 0 0 1 0 1 0 . 1 1 0|0 0 0 0 0
```

The network number for the network device that has IP address 192.168.10.213 is 192.168.10.192. To find the broadcast address, set all host bits to 1:

```
                    Network                          Host
   192          168          10           223
1 1 0 0 0 0 0 0 . 1 0 1 0 1 0 0 0 . 0 0 0 0 1 0 1 0 . 1 1 0|1 1 1 1 1
```

The broadcast address for the network device that has the IP address 192.168.10.213 is 192.168.10.223. Notice how all eight bits are used to calculate the number 223 in the last octet. Valid IP addresses are any numbers between the network number 192.168.10.192 and the broadcast IP address 192.168.10.223. In other words, the range of usable IP addresses is from 192.168.10.193 (one number larger than the network address) through 192.168.10.222 (one number less than the broadcast address). Practice problems in the following exercise help you explore this concept.

Exercise

Exercise A.1 Subnet Practice Exercise

Objective: To be able to determine the subnet number, broadcast address, and IP addresses that can be assigned to network devices

Procedure: Complete the following procedures and answer the accompanying questions.

1. Determine the network address for each of the following IP address and subnet mask combinations.

   210.141.254.122 255.255.255.192

   _____

   206.240.195.38 255.255.255.224

   _____

   104.130.188.213 255.255.192.0

   _____

   69.89.5.224 255.240.0.0

   _____

   10.113.71.66 255.128.0.0

   _____

2. Determine the broadcast address for the following IP address and subnet mask combinations.

   166.215.207.182 255.255.255.240

   _____

   198.94.140.121 255.255.255.224

   _____

   97.57.210.192 255.255.224.0

   _____

   133.98.227.36 255.255.192.0

   _____

   14.89.203.133 255.128.0.0

   _____

3. Determine the valid IP addresses on the networks that contain the following IP address and subnet mask combinations.

   131.107.200.34 255.255.248.0

   _____

   146.197.221.238 255.255.255.192

   _____

   52.15.111.33 255.255.248.0

   _____

   192.168.10.245/30

   _____

   209.218.235.117 255.255.255.128

   _____

CompTIA A+ Certification Exam Objectives

EXAM NUMBER: CORE 1 (220-1201)

Copyright © 2024 CompTIA, Inc. All rights reserved.

About the Exam

Candidates are encouraged to use this document to help prepare for the CompTIA A+ 220-1201 certification exam. In order to receive the CompTIA A+ certification, you must pass two exams: Core 1 (220-1201) and Core 2 (220-1202). The CompTIA A+ Core 1 (220-1201) and Core 2 (220-1202) certification exams will verify the successful candidate has the knowledge and skills required to:

- Install, configure, and maintain computer equipment, mobile devices, and software for end users.
- Service components based on customer requirements.
- Understand networking basics and apply basic cybersecurity methods to mitigate threats.
- Properly and safely diagnose, resolve, and document common hardware and software issues.
- Apply troubleshooting skills and provide customer support using appropriate communication skills.
- Understand the basics of scripting, cloud technologies, virtualization, and multi-OS deployments in
- corporate environments.

EXAM ACCREDITATION

The CompTIA A+ Core 1 (220-1201) and Core 2 (220-1202) exams are accredited by ANSI to show compliance with the ISO 17024 standard and, as such, undergo regular reviews and updates to the exam objectives.

EXAM DEVELOPMENT

CompTIA exams result from subject matter expert workshops and industry-wide survey results regarding the skills and knowledge required of an IT professional.

COMPTIA AUTHORIZED MATERIALS USE POLICY

CompTIA Certifications, LLC is not affiliated with and does not authorize, endorse, or condone utilizing any content provided by unauthorized third-party training sites (aka “brain dumps”). Individuals who utilize such materials in preparation for any CompTIA examination will have their certifications revoked and be suspended from future testing in accordance with the CompTIA Candidate Agreement. In an effort to more clearly communicate CompTIA’s exam policies on use of unauthorized study materials, CompTIA directs all certification candidates to the CompTIA Certification Exam Policies. Please review all CompTIA policies before beginning the study process for any CompTIA exam. Candidates will be required to abide by the CompTIA Candidate Agreement. If a candidate has a question as to whether study materials are considered unauthorized (aka “brain dumps”), they should contact CompTIA at examsecurity@comptia.org to confirm.

PLEASE NOTE

The lists of examples provided in bulleted format are not exhaustive lists. Other examples of technologies, processes, or tasks pertaining to each objective may also be included on the exam, although not listed or covered in this objectives document. CompTIA is constantly reviewing the content of our exams and updating test questions to be sure our exams are current, and the security of the questions is protected. When necessary, we will publish updated exams based on existing exam objectives. Please know that all related exam preparation materials will still be valid.

Copyright © 2024 CompTIA, Inc. All rights reserved.
From the Library of Zanas Haja

TEST DETAILS

Required exam	A+ Core 1 (220-1201)
Number of questions	Maximum of 90
Types of questions	Multiple-choice and performance-based
Length of test	90 minutes
Recommended experience	12 months of hands-on experience in an IT support specialist job role
Passing Score	675 (on a scale of 100–900)

EXAM OBJECTIVES (DOMAINS)

The table below lists the domains measured by this examination and the extent to which they are represented.

DOMAIN		PERCENTAGE OF EXAMINATION
1.0	Mobile Devices	13%
2.0	Networking	23%
3.0	Hardware	25%
4.0	Virtualization and Cloud Computing	11%
5.0	Hardware and Network Troubleshooting	28%
Total		**100%**

TROUBLESHOOTING METHODOLOGY KNOWLEDGE

During the job task analysis workshop for the A+ 220-1200 series, subject matter experts deemed the troubleshooting methodology an effective best practice that new job incumbents should be aware of and leverage as they engage in troubleshooting new issues on the job. However, while this methodology is practical, the decision was made to not include it in the exam. While the methodology itself will not be tested, there remains an emphasis on troubleshooting within the job role context. Therefore, the troubleshooting methodology section appears here as part of this "competency standard" but does not constitute a formal objective or part of the A+ certification exam. Training institutions that prepare individuals with very little technical knowledge and experience are encouraged to leverage this methodology, especially when such individuals might be applying for their first IT job.

The troubleshooting methodology includes the following steps:

- Identify the problem.
- Establish a theory of probable cause (question the obvious).
  - Research knowledge base/internet, if applicable.
- Test the theory to determine the cause.
- Establish a plan of action to resolve the problem and implement the solution.
- Verify full system functionality and, if applicable, implement preventive measures.
- Document findings/lessons learned, actions, and outcomes.

Copyright © 2024 CompTIA, Inc. All rights reserved.

1.0 Mobile Devices

1.1 Given a scenario, monitor mobile device hardware and use appropriate replacement techniques.

- Battery
- Keyboard/keys
- Random-access memory (RAM)
- Hard disk drive (HDD)/solid-state drive (SSD)
- Wireless cards
- Physical privacy and security components
  - Biometrics
  - Near-field scanner features
- Wi-Fi antenna connector/placement
- Camera/webcam
- Microphone

1.2 Compare and contrast accessories and connectivity options for mobile devices.

- Connection methods
  - Universal Serial Bus (USB)/USB-C/microUSB/miniUSB
  - Lightning
  - Near-field communication (NFC)
  - Bluetooth
  - Tethering/hotspot
- Accessories
  - Stylus
  - Headsets
  - Speakers
  - Webcam
- Docking station
- Port replicator
- Trackpad/drawing pad/track points

1.3 Given a scenario, configure basic mobile device network connectivity and provide application support.

- Wireless/cellular data network (enable/disable)
  - 3G/4G/5G
  - Hotspot
  - Wi-Fi
  - Subscriber Identity Module (SIM)/eSIM
- Bluetooth
  - Enable Bluetooth
  - Enable pairing
  - Find a device for pairing
  - Enter the appropriate personal identification number (PIN) code
  - Test connectivity
- Location services
  - Global positioning system (GPS) services
  - Cellular location services
- Mobile device management (MDM)
  - Device configurations
    - Corporate
    - Bring your own device (BYOD)
  - Policy enforcement
  - Corporate applications
- Mobile device synchronization
  - Recognizing data caps
  - Calendar
  - Contacts
  - Business applications
    - Mail
    - Cloud storage

Copyright © 2024 CompTIA, Inc. All rights reserved.

CompTIA

From the Library of Zanas Usis

2.0 Networking

2.1 Compare and contrast Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) ports, protocols, and their purposes.

- Ports and protocols
  - 20-21 – File Transfer Protocol (FTP)
  - 22 – Secure Shell (SSH)
  - 23 – Telnet
  - 25 – Simple Mail Transfer Protocol (SMTP)
  - 53 – Domain Name System (DNS)
  - 67/68 – Dynamic Host Configuration Protocol (DHCP)
  - 80 – Hypertext Transfer Protocol (HTTP)
  - 110 – Post Office Protocol 3 (POP3)
  - 143 – Internet Mail Access Protocol (IMAP)
  - 137-139 Network Basic Input/Output System (NetBIOS)/NetBIOS over TCP/IP (NetBT)
  - 389 – Lightweight Directory Access Protocol (LDAP)
  - 443 – Hypertext Transfer Protocol Secure (HTTPS)
  - 445 – Server Message Block (SMB)/Common Internet File System (CIFS)
  - 3389 – Remote Desktop Protocol (RDP)
- TCP vs. UDP

2.2 Explain wireless networking technologies.

- Frequencies
  - 2.4GHz
  - 5GHz
  - 6GHz
- Channels
  - Regulations
  - Channel selection
    - Widths
    - Frequencies
    - Bands
- Bluetooth
- 802.11 standards
- NFC
- Radio-frequency identification (RFID)

2.3 Summarize services provided by networked hosts.

- Server roles
  - DNS
  - DHCP
  - Fileshare
  - Print servers
  - Mail servers
  - Syslog
  - Web servers
  - Authentication, Authorization, and Accounting (AAA)
  - Database servers
  - Network Time Protocol (NTP)
- Internet appliances
  - Spam gateways
  - Unified threat management (UTM)
  - Load balancers
  - Proxy servers
- Legacy/embedded systems
  - Supervisory control and data acquisition (SCADA)
- Internet of Things (IoT) devices

Copyright © 2024 CompTIA, Inc. All rights reserved.
From the Library of Zanas Usis

2.4 Explain common network configuration concepts.

- DNS
  - A
  - AAAA
  - Canonical Name (CNAME)
  - Mail exchanger (MX)
  - Text (TXT)
    - Spam management
      - DomainKeys Identified Mail (DKIM)
      - Sender Policy Framework (SPF)
      - Domain-based Message Authentication, Reporting, and Conformance (DMARC)
- DHCP
  - Leases
  - Reservations
  - Scope
  - Exclusions
- Virtual LAN [local area network] (VLAN)
- Virtual private network (VPN)

2.5 Compare and contrast common networking hardware devices.

- Routers
- Switches
  - Managed
  - Unmanaged
- Access points
- Patch panel
- Firewall
- Power over Ethernet (PoE)
  - Injectors
  - Switch
  - PoE standards
- Cable modem
- Digital subscriber line (DSL)
- Optical network terminal (ONT)
- Network interface card (NIC)
  - Physical media access control (MAC) address

2.6 Given a scenario, configure basic wired/wireless small office/home office (SOHO) networks.

- Internet Protocol (IP) addressing
  - IPv4
    - Private addresses
    - Public addresses
  - IPv6
  - Automatic Private IP Addressing (APIPA)
  - Static
  - Dynamic
  - Subnet mask
  - Gateway

Copyright © 2024 CompTIA, Inc. All rights reserved.

2.7 Compare and contrast internet connection types, network types, and their characteristics.

- Internet connection types
  - Satellite
  - Fiber
  - Cable
  - DSL
  - Cellular
  - Wireless internet service provider (WISP)
- Network types
  - LAN
  - Wide area network (WAN)
  - Personal area network (PAN)
  - Metropolitan area network (MAN)
  - Storage area network (SAN)
  - Wireless local area network (WLAN)

2.8 Explain networking tools and their purposes.

- Crimper
- Cable stripper
- Wi-Fi analyzer
- Toner probe
- Punchdown tool
- Cable tester
- Loopback plug
- Network tap

Copyright © 2024 CompTIA, Inc. All rights reserved.

3.0 Hardware

3.1 Compare and contrast display components and attributes.

- Types
  - Liquid crystal display (LCD)
    - In-plane switching (IPS)
    - Twisted nematic (TN)
    - Vertical alignment (VA)
  - Organic light-emitting diode (OLED)
  - Mini light-emitting diode (Mini-LED)
- Touch screen/digitizer
- Inverter
- Attributes
  - Pixel density
  - Refresh rates
  - Screen resolution
  - Color gamut

3.2 Summarize basic cable types and their connectors, features, and purposes.

- Network cables
  - Copper
    - Categories
      - T568A/T568B standards
    - Coaxial
    - Shielded twisted pair
      - Direct burial
    - Unshielded twisted pair
  - Plenum-rated
  - Optical
    - Single-mode
    - Multimode
- Peripheral cables
  - USB 2.0
  - USB 3.0
  - Serial
  - Thunderbolt
- Video cables
  - High-definition Multimedia Interface (HDMI)
  - DisplayPort
  - Digital Visual Interface (DVI)
  - Video Graphics Array (VGA)
  - USB-C
- Hard drive cables
  - Serial Advanced Technology Attachment (SATA)
  - External SATA (eSATA)
- Adapters
- Connector types
  - RJ11
  - RJ45
  - F-type
  - Straight tip (ST)
  - Subscriber connector (SC)
  - Lucent connector (LC)
  - Punchdown block
  - MicroUSB
  - MiniUSB
  - USB-C
  - Molex
  - Lightning
  - DB9

3.3 Compare and contrast RAM characteristics.

- Form factors
  - Small Outline Dual In-line Memory Module (SODIMM)
  - Dual In-line Memory Module (DIMM)
- Double Data Rate (DDR) iterations
- Error-correcting code (ECC) vs. non-ECC RAM
- Channel configurations

Copyright © 2024 CompTIA, Inc. All rights reserved.

3.4 Compare and contrast storage devices.

- Hard drives
  - Spindle speeds
  - Form factors
    - 2.5-inch
    - 3.5-inch
- Solid-state drives
  - Communications interfaces
    - Non-volatile Memory Express (NVMe)
    - SATA
    - Peripheral Component Interconnect Express (PCIe)
    - Serial Attached SCSI [Small Computer System Interface] (SAS)
  - Form factors
    - M.2
    - Mini-serial Advanced Technology Attachment (mSATA)
- Drive configurations
  - Redundant Array of Independent Disks (RAID) 0, 1, 5, 6, 10
- Removable storage
  - Flash drives
  - Memory cards
- Optical drives

3.5 Given a scenario, install and configure motherboards, central processing units (CPUs), and add-on cards.

- Motherboard form factors
  - Advanced Technology Extended (ATX)
  - microATX
  - Information Technology eXtended (ITX)
- Motherboard connector types
  - Peripheral Component Interconnect (PCI)
  - PCIe
  - Power connectors
  - SATA
  - eSATA
  - Headers
  - M.2
- Motherboard compatibility
  - CPU socket types
    - Advanced Micro Devices, Inc. (AMD)
    - Intel
  - Multisocket
- BIOS/Unified Extensible Firmware Interface (UEFI) settings
  - Boot options
  - USB permissions
  - Trusted Platform Module (TPM) security features
  - Fan considerations
  - Secure Boot
  - Boot password
  - BIOS password
  - Temperature monitoring
- Virtualization support
- Encryption
  - TPM
  - Hardware security module (HSM)
- CPU architecture
  - x86/x64
  - Advanced RISC [Reduced Instruction Set Computer] Machine (ARM)
  - Core configurations
- Expansion cards
  - Sound card
  - Video card
  - Capture card
  - Network interface card
- Cooling
  - Fans
  - Heat sink
  - Thermal paste/pads
  - Liquid

3.6 Given a scenario, install the appropriate power supply.

- Input 110–120 VAC vs. 220–240 VAC
- Output 3.3V vs. 5V vs. 12V
- 20+4 pin motherboard connector
- Redundant power supply
- Modular power supply
- Wattage rating
- Energy efficiency

Copyright © 2024 CompTIA, Inc. All rights reserved.
From the Library of Zanas Usis

3.7 Given a scenario, deploy and configure multifunction devices/printers and settings.

- Properly unbox device and consider set-up location
- Use appropriate drivers for a given operating system
  - Printer Control Language (PCL) vs. postscript
- Firmware
- Device connectivity
  - USB
  - Ethernet
  - Wireless
- Public/shared devices
  - Printer share
  - Print server
- Configuration settings
  - Duplex
  - Orientation
  - Tray settings
  - Quality
- Security
  - User authentication
  - Badging
  - Audit logs
  - Secured prints
- Network scan services
  - Email
  - SMB
  - Cloud services
- Automatic document feeder (ADF)/flatbed scanner

3.8 Given a scenario, perform appropriate printer maintenance.

- Laser
  - Maintenance: Replace toner, apply maintenance kit, calibrate, and clean
- Inkjet
  - Ink cartridge, printhead, roller, and feeder
  - Maintenance: Clean printheads, replace cartridges, calibrate, and clear jams
- Thermal
  - Feed assembly
  - Special thermal paper
  - Maintenance: Replace paper, clean heating element, and remove debris
- Impact
  - Multipart paper
  - Maintenance: Replace ribbon, printhead, and paper

Copyright © 2024 CompTIA, Inc. All rights reserved.
From the Library of Zanas Usis

4.0 Virtualization and Cloud Computing

4.1 Explain virtualization concepts.

- Purpose of virtual machines
  - Sandbox
  - Test development
  - Application virtualization
    - Legacy software/OS
    - Cross-platform virtualization
- Requirements
  - Security
  - Network
  - Storage
- Desktop virtualization
  - Virtual Desktop Infrastructure (VDI)
- Containers
- Hypervisors
  - Type 1
  - Type 2

4.2 Summarize cloud computing concepts.

- Common cloud models
  - Private cloud
  - Public cloud
  - Hybrid cloud
  - Community cloud
  - Infrastructure as a service (IaaS)
  - Software as a service (SaaS)
  - Platform as a service (PaaS)
- Cloud characteristics
  - Shared resources vs. dedicated resources
  - Metered utilization
    - Ingress/egress
  - Elasticity
  - Availability
  - File synchronization
  - Multitenancy
-

Copyright © 2024 CompTIA, Inc. All rights reserved.

CompTIA

From the Library of Zanas Haja

5.0 Hardware and Network Troubleshooting

5.1 Given a scenario, troubleshoot motherboards, RAM, CPUs, and power.

- **Common symptoms**
  - Power-on self-test (POST) beeps
  - Proprietary crash screens
  - Blank screen
  - No power
  - Sluggish performance
  - Overheating
  - Burning smell
  - Random shutdown
  - Application crashes
  - Unusual noise
  - Capacitor swelling
  - Inaccurate system date/time

5.2 Given a scenario, troubleshoot drive and RAID issues.

- **Common symptoms**
  - Light-emitting diode (LED) status indicators
  - Grinding noises
  - Clicking sounds
  - Bootable device not found
  - Data loss/corruption
  - RAID failure
  - Self-monitoring and Reporting Technology (S.M.A.R.T.) failure
  - Extended read/write times
  - Low performance input/output operations per second (IOPS)
  - Missing drives in OS
  - Array missing
  - Audible alarms

5.3 Given a scenario, troubleshoot video, projector, and display issues.

- **Common symptoms**
  - Incorrect input source
  - Physical cabling issues
  - Burnt-out bulb
  - Fuzzy image
  - Display burn-in
  - Dead pixels
  - Flashing screen
  - Incorrect color display
  - Audio issues
  - Dim image
  - Intermittent projector shutdown
  - Sizing issues
  - Distorted image

5.4 Given a scenario, troubleshoot common mobile device issues.

- **Common symptoms**
  - Poor battery health
  - Swollen battery
  - Broken screen
  - Improper charging
  - Poor/no connectivity
  - Liquid damage
  - Overheating
  - Digitizer issues
  - Physically damaged ports
  - Malware
  - Cursor drift/touch calibration
  - Unable to install new applications
  - Stylus does not work
  - Degraded performance

Copyright © 2024 CompTIA, Inc. All rights reserved.

5.5 Given a scenario, troubleshoot network issues.

- Common symptoms
  - Intermittent wireless connectivity
  - Slow network speeds
  - Limited connectivity
  - Jitter
  - Poor Voice over Internet Protocol (VoIP) quality
  - Port flapping
  - High latency
  - External interference
  - Authentication failures
  - Intermittent internet connectivity

5.6 Given a scenario, troubleshoot printer issues.

- Lines down the printed pages
- Garbled print
- Paper jams
- Faded prints
- Paper not feeding
- Multipage misfeed
- Multiple prints pending in queue
- Speckling on printed pages
- Double/echo images on the print
- Grinding noise
- Finishing issues
  - Staple jams
  - Hole punch
- Incorrect page orientation
- Tray not recognized
- Connectivity issues
- Frozen print queue

Copyright © 2024 CompTIA, Inc. All rights reserved.

CompTIA A+ Core 1 (220-1201) Acronym List

The following is a list of acronyms that appears on the CompTIA Core 1 (220-1201) exam. Candidates are encouraged to review the complete list and attain a working knowledge of all listed acronyms as part of a comprehensive exam preparation program.

ACRONYM	DEFINITION
AAA	Authentication, Authorization, and Accounting
AAAA	Authentication, Authorization, Accounting, and Auditing
ACL	Access Control List
ADF	Automatic Document Feeder
AES	Advanced Encryption Standard
AMD	Advanced Micro Devices, Inc.
APFS	Apple File System
APIPA	Automatic Private Internet Protocol Addressing
ARM	Advanced RISC [Reduced Instruction Set Computer] Machine
ATX	Advanced Technology Extended
BEC	Business Email Compromise
BIOS	Basic Input/Output System
BSOD	Blue Screen of Death
BYOD	Bring Your Own Device
CAC	Calling-card Authorization Computer
CIFS	Common Internet File System
CMDB	Configuration Management Database
CNAME	Canonical Name
CPU	Central Processing Unit
DB-9	Serial Communications D-Shell Connector, 9 pins
DDoS	Distributed Denial of Service
DDR	Double Data Rate
DHCP	Dynamic Host Configuration Protocol
DIMM	Dual In-line Memory Module
DKIM	DomainKeys Identified Mail
DLP	Data Loss Prevention
DMARC	Domain-based Message Authentication, Reporting, and Conformance
DNS	Domain Name System
DoS	Denial of Service
DRM	Digital Rights Management
DSL	Digital Subscriber Line
DVI	Digital Visual Interface
ECC	Error-correcting Code
EDR	Endpoint Detection and Response
EFS	Encrypting File System
EOL	End-of-life
eSATA	External Serial Advanced Technology Attachment
ESD	Electrostatic Discharge
EULA	End-user License Agreement
exFAT	Extended File Allocation Table
FAT32	32-bit File Allocation Table

Copyright © 2024 CompTIA, Inc. All rights reserved.

From the Library of Zanas Haja

ACRONYM	DEFINITION
FRT	Facial Recognition Technology
FTP	File Transfer Protocol
GFS	Grandfather-Father-Son
GPS	Global Positioning System
GPT	GUID [Globally Unique Identifier] Partition Table
GUID	Globally Unique Identifier
HDD	Hard Disk Drive
HDMI	High-definition Media Interface
HSM	Hardware Security Module
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IaaS	Infrastructure as a Service
IAM	Identity and Access Management
IMAP	Internet Mail Access Protocol
IOPS	Input/Output Operations Per Second
IoT	Internet of Things
IP	Internet Protocol
IPS	In-plane Switching
ISO	International Organization for Standardization
ITX	Information Technology eXtended
KVM	Keyboard-Video-Mouse
LAN	Local Area Network
LC	Lucent Connector
LCD	Liquid Crystal Display
LDAP	Lightweight Directory Access Protocol
LED	Light-emitting Diode
MAC	Media Access Control
MAN	Metropolitan Area Network
MBR	Master Boot Record
MDM	Mobile Device Management
MDR	Managed Detection and Response
MFA	Multifactor Authentication
MMC	Microsoft Management Console
MNDA	Mutual Non-disclosure Agreement
mSATA	Mini-serial Advanced Technology Attachment
MSDS	Material Safety Data Sheet
MX	Mail Exchange
NDA	Non-disclosure Agreement
NetBIOS	Network Basic Input/Output System
NFC	Near-field Communication
NIC	Network Interface Card
NTFS	New Technology File System
NTP	Network Time Protocol
NVMe	Non-volatile Memory Express
OLED	Organic Light-emitting Diode
ONT	Optical Network Terminal
OS	Operating System
OTP	One-time Password (or Passcode)
PaaS	Platform as a Service
PAM	Privileged Access Management
PAN	Personal Area Network
PC	Personal Computer
PCI	Peripheral Component Interconnect
PCIe	Peripheral Component Interconnect Express

Copyright © 2024 CompTIA, Inc. All rights reserved.

ACRONYM	DEFINITION
PII	Personally Identifiable Information
PIN	Personal Identification Number
PIV	Personal Identity Verification
PoE	Power over Ethernet
POP	Post Office Protocol
POST	Power-on Self-test
PUP	Potentially Unwanted Program
RADIUS	Remote Authentication Dial-in User Server
RAID	Redundant Array of Independent Disks
RAM	Random-access Memory
RDP	Remote Desktop Protocol
ReFS	Resilient File System
RFID	Radio-frequency Identification
RJ11	Registered Jack Function 11
RJ45	Registered Jack Function 45
RMM	Remote Monitoring and Management
RSR	Rapid Security Response
SaaS	Software as a Service
SAN	Storage Area Network
SAML	Security Assertions Markup Language
SAS	Serial Attached SCSI [Small Computer System Interface]
SATA	Serial Advanced Technology Attachment
SC	Subscriber Connector
SCADA	Supervisory Control and Data Acquisition
SCSI	Small Computer System Interface
SIM	Subscriber Identity Module
SLA	Service-level Agreement
S.M.A.R.T	Self-monitoring Analysis and Reporting Technology
SMB	Server Message Block
SMS	Short Message Service
SMTP	Simple Mail Transfer Protocol
SODIMM	Small Outline Dual In-line Memory Module
SOHO	Small Office/Home Office
SOP	Standard Operating Procedure
SPF	Sender Policy Framework
SPICE	Software Process Improvement and Capability Determination
SQL	Structured Query Language
SSD	Solid-state Drive
SSH	Secure Shell
SSID	Service Set Identifier
SSO	Single Sign-on
ST	Straight Tip
TACACS	Terminal Access Controller Access-control System
TCP	Transmission Control Protocol
TKIP	Temporal Key Integrity Protocol
TN	Twisted Nematic
TOTP	Time-based One-time Password
TPM	Trusted Platform Module
UAC	User Account Control
UDP	User Datagram Protocol
UEFI	Unified Extensible Firmware Interface
UPnP	Universal Plug and Play
UPS	Uninterruptible Power Supply
USB	Universal Serial Bus

Copyright © 2024 CompTIA, Inc. All rights reserved.

ACRONYM	DEFINITION
UTM	Unified Threat Management
VA	Vertical Alignment
VDI	Virtual Desktop Infrastructure
VGA	Video Graphics Array
VLAN	Virtual LAN [Local Area Network]
VNC	Virtual Network Computer
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network
VRAM	Video Random-access Memory
WAN	Wide Area Network
WinRM	Windows Remote Management
WISP	Written Internet Service Provider
WLAN	Wireless LAN [Local Area Network]
WPA	Wi-Fi Protected Access
WWAN	Wireless Wide Area Network
XDR	Extended Detection and Response
XFS	Extended File System
XXS	Cross-site Scripting

Copyright © 2024 CompTIA, Inc. All rights reserved.

CompTIA A+ Core 1 (220-1201) Hardware and Software List

CompTIA has included this sample list of hardware and software to assist candidates as they prepare for the A+ Core 1 (220-1201) certification exam. This list may also be helpful for training companies that wish to create a lab component for their training offering. The bulleted lists below each topic are sample lists and are not exhaustive.

EQUIPMENT

- Apple tablet/smartphone
- Android tablet/smartphone
- Windows tablet
- Chromebook
- Windows laptop/Mac laptop/ Linux laptop
- Windows desktop/Mac desktop/ Linux desktop
- Windows server with Active Directory and Print Manager
- Monitors
- Projectors
- SOHO router/switch
- Access point
- VoIP phone
- Printer
  - Laser/inkjet
  - Wireless
  - 3-D printer
  - Thermal
- Surge suppressor
- UPS
- Smart devices (IoT devices)
- Server with a hypervisor
- Punchdown block
- Patch panel
- Webcams
- Speakers
- Microphones

SPARE PARTS/HARDWARE

- Motherboards
- RAM
- Hard drives
- Power supplies
- Video cards
- Sounds cards
- Network cards
- Wireless NICs
- Fans/cooling devices/heat sink
- CPUs
- Assorted connectors/cables
  - USB
  - HDMI
  - DisplayPort
  - DVI
  - VGA
- Adapters
  - Bluetooth adapter
- Network cables
- Unterminated network cable/connectors
- AC adapters
- Optical drives
- Screws/stand-offs
- Cases
- Maintenance kit
- Mice/keyboards
- Keyboard-Video-Mouse (KVM)
- Console cable
- SSD

TOOLS

- Screwdrivers
- Multimeter
- Wire cutters
- Punchdown tool
- Crimper
- Power supply tester
- Cable stripper
- Standard technician toolkit
- Electrostatic discharge (ESD) strap
- Thermal paste
- Cable tester
- Cable toner
- Wi-Fi analyzer
- Serial Advanced Technology Attachment (SATA) to USB connectors

SOFTWARE

- Operating systems
  - Linux

© 2024 CompTIA, Inc., used under license by CompTIA, Inc. All rights reserved. All certification programs and education related to such programs are operated exclusively by CompTIA, Inc. CompTIA is a registered trademark of CompTIA, Inc. in the U.S. and internationally. Other brands and company names mentioned herein may be trademarks or service marks of CompTIA, Inc. or of their respective owners. Reproduction or dissemination prohibited without the written consent of CompTIA, Inc. Printed in the U.S. 11273-May2024

From the Library of Zanas Usis

Glossary

The complete, searchable glossary for the *Complete A+ Guide to IT Hardware and Software* is available on the book's companion website.

To access it, follow these steps:

1. Visit www.pearsonITcertification.com/register.
2. Enter the print book ISBN: **9780135439777**.
3. Answer the security question to validate your purchase.
4. Go to your account page.
5. Click the **Registered Products** tab.
6. Under the book listing, click the **Access Bonus Content** link.

Glossary

Numerals and Symbols

.. (navigation command) From a Windows command prompt, the two dots (. .) represent the parent directory.

+12V A voltage level from the power supply that is used for drive motors, CPU, internal cooling fans, and the graphics card.

+5V A voltage level from the power supply that is used for electronics, the motherboard, adapters, ports, and peripherals.

1.8-inch A storage device form factor.

115V vs. 220V input voltage Some power supplies accept 120 V (listed as 115 V on the certification) or 220 V power from an electrical outlet.

10,000 RPM A hard drive speed. The faster the drive RPM, the faster the transfer rate.

15,000 RPM A hard drive speed. The faster the drive RPM, the faster the transfer rate.

2.4 GHz A common frequency used for 802.11 wireless networks.

2.5-inch drive A storage device form factor.

20-pin to24-pin motherboard adapter A way to connect an older power supply to an ATX motherboard.

20 + 4 connector A two-piece cable that connects into a 24-port motherboard connector as the major power connection from the power supply.

24-pin motherboard connector Main ATX motherboard power connector.

3.3V A common desktop power supply output voltage.

3.5-inch drive A storage device form factor.

3-2-1 backup Create three copies of the data (one primary and two copies). Use two different types of media and keep at least one copy off site.

32-bit architecture A device that has a processor that can handle 32 bits at one time.

3G Third generation of wireless cellular technology that allowed mobile devices to have faster internet connectivity.

3G/4G/5G Types of cellular networks shown by generation with 5G being the latest generation type.

4-pin 12V A power supply connector that is sometimes labeled AUX or 12V used to provide extra power to the processor.

4G Fourth generation of cellular network that supports IP telephony, gaming services, mobile TV, and video conferencing at speeds up to 1 Gb/s.

5 GHz A common frequency used for 802.11 wireless networks.

5,400 RPM A hard drive speed. The faster the drive RPM, the faster the transfer rate.

568A/B An ANSI/TIA/EIA Ethernet network cabling standard.

5G Fifth generation of cellular networks that does not have formal standards yet; supports speeds up to 10 Gb/s.

6-pin PCIe A power supply connector used to provide power to a video adapter.

64-bit architecture A device that has a processor that can handle 64bits at one time.

6 GHz A common frequency used for 802.11 wireless networks.

7,200 RPM A hard drive speed. The faster the drive RPM, the faster the transfer rate.

8-pin PCIe A power supply connector used to provide power to a video adapter.

802.11a An IEEE wireless standard that used the 5 GHz range and had speeds up to 54 Mb/s.

802.11ac (WiFi 5) An IEEE wireless standard that uses the 5 GHz range and supports speeds up to 4.9 Gb/s.

802.11ad A wireless standard that works in the 60 GHz range and is also known as WiGig.

802.11ax (WiFi 6) A wireless standard that uses the 2.4, 5, and 6 GHz ranges, improves wireless connectivity and throughput, and is backwards compatible with older 2.4 and 5 GHz devices.

802.11b The first IEEE wireless standard to hit the market; used the 2.4 GHz range and supported speeds up to 11 Mb/s.

802.11be (WiFi 7) A wireless standard that uses the 2.4, 5, and 6 GHz ranges and can block off part of a channel and still use the rest of the channel for data transmissions.

802.11e A wireless quality of service standard.
802.11g An IEEE wireless standard that was an upgrade to 802.11b and was backward compatible with it; used the 2.4 GHz range and had speeds up to 54 Mb/s.
802.11i A wireless security standard.
802.11n An IEEE wireless standard that uses both the 2.4 and 5 GHz ranges and that supports speeds up to 600 Mb/s.

A

.app An application package that contains the software, folders and other files required to install an application, usually in macOS.
/Applications A macOS system folder that contains built-in macOS apps like Mail, Calendar and Safari, as well as applications that the user installs.
ActiveSync A Microsoft product that allows data including contacts, email, and calendar synchronization between a mobile device and a Windows desktop computer.
APK A file format that can be used to distribute and install Android apps.
A record A DNS address record that holds the IPv4 address of a particular web address.
A/V (audio/video) A reference to sound and visual data, such as movies or stills.
AAA server A server used in a corporate environment that is used to verify credentials such as a username and password.
AAAA record A DNS record that holds the IPv6 address of a particular website.
AC (alternating current) The type of electrical power from a wall outlet.
AC circuit tester A device that checks a wall outlet's wiring.
acceptable use policy (AUP) A policy that defines rules regarding using a company network, data, and a specific application.
access control list (ACL) An access control list relates to the permissions for a specific object such as what is allowed to be done to the object (such as a file or directory) by particular users or operating system processes. A means of providing a security filter where traffic is allowed or denied based on configured parameters.
access control vestibule A method of separating a nonsecure area from a secure area to prevent unauthorized access and tailgating. Also known as mantrap.
access point A component of a wireless network that accepts associations from wireless network cards.
Accessibility A macOS System Settings tool that provides settings for options such as colors, zoom, voiceover, captions, and more.
Accessibility A Settings category used to configure Windows to accommodate the user's vision, hearing, dexterity, mobility, and focus preferences; also provides options for security and permissions.
account recovery option An option used when a Microsoft account or password has been forgotten.
account settings Settings required when putting a thick client or thin client onto a network.
Accounts A Windows Settings category that contains options for configuring local Microsoft Windows accounts, cloud accounts, work and school accounts, and linked devices.
ACL See *access control list.*
ACPI (Advanced Configuration and Power Interface) Technology that allows the motherboard and operating system to control the power needs and operation modes of various devices.
activation clock A timer for the Windows operating system. When creating an image, a technician must reset or re-arm the activation clock if a single activation key is used. This gives a 30-day (Windows 7) or 90-day (Windows 8/10) grace period before having to re-enter the product key.
Active Directory (AD) A service used on Microsoft Windows Server to manage network accounts and devices.
active listening An effective communication technique that ensures what the speaker says is accurately received.
Activity Monitor A troubleshooting tool in a macOS system that sees what processes and services are running, as well as what system resources are used.
Ad blocker Software that is made specifically to not show advertisements that appear in certain websites.
ad hoc mode A type of wireless configuration in which two 802.11 wireless devices can make a wireless network without the use of an access point.
adapter An electronic circuit card that inserts into an expansion slot. Also called a controller, card, controller card, circuit card, circuit board, and adapter board.
adding array (Disk Management) Right-click inside unallocated space of a drive > *New Spanned Volume* or *New Striped Volume* > select another drive to be added> select a drive letter and file system.

adding drive (Disk Management) Ensure that the drive is recognized by the BIOS and create a partition and format for a particular file system.

ADF (automatic document feeder) A feature on a printer or multifunction device that allows paper to be fed into the device to be copied, scanned, or faxed depending on the model and task.

ADF scanner A scanner that has the added feature of having an automatic document feeder (ADF) to allow multiple pages to be fed or input into the scanner.

ADK See *Windows Assessment and Deployment Kit*.

administrative privileges A security function in Windows that requires elevated security rights in order to execute specific commands. Use the *Run as administrator* option if blocked.

administrative share A share created by Microsoft for drive volumes and the folder that contains the majority of Windows files. An administrative share has a dollar sign at the end of its name.

Administrative Tools A Windows Control panel subcategory that contains higher-level utilities that are also found in other categories; known as Windows Tools in Windows 11.

administrator A person responsible for setting up and maintaining a system, such as a Windows computer. Logging in as an administrator allows settings to be changed that may not be allowed for other users.

ADSL (Asymmetrical DSL) A type of digital subscriber line (DSL) that provides speeds up to 150 Mb/s; it provides faster downloads than uploads.

Advanced Boot Options A Windows boot menu used to access tools used for troubleshooting. Press • when the computer is booting (and before Windows loads) to access the Advanced Boot Options menu.

Advanced Technology eXtended (ATX) A form factor for motherboards, cases, and power supplies.

adware Software that automatically appears and sometimes disrupts what we are doing on a website.

AES (Advanced Encryption Standard) Used in wireless networks and offers encryption with 128-bit, 192-bit, and 256-bit encryption keys.

AFP (Apple Filing Protocol) A set of rules for file services on an Apple device that uses macOS. AFP uses port 548.

AGP (accelerated graphics port) An extension of the PCI bus (a port) that provides a dedicated communication path between the expansion slot and the processor. AGP is used for video adapters.

AI (artificial intelligence) A technology that uses machine learning to analyze data and learn from that data in order to make predictions or take a particular action.

AI hallucinations AI-generated information that provides false or misleading information.

AI policy A corporate document that dictates the appropriate use of artificial intelligence.

air filter/mask The air filter or mask should be used whenever dust, airborne particles, or debris could cause personal issues. An air filter might also be used in an area where the air quality is not appropriate for a computer or networking equipment.

Airplane Mode Enables users to disable all wireless communication but still view a movie or play a game that does not require internet connectivity.

AirPrint An Apple print server.

alphanumeric character A character that can be a letter of the alphabet (uppercase or lowercase), a digit from `0` through `9`, or a punctuation mark or symbol, such as `@`, `#`, or `!`.

alternative location A data recovery solution where a different location is used in case of disaster.

AMD (Advanced Micro Devices) A company that makes processors, graphics processors, and chipsets. AMD is the largest rival of Intel for PC processors.

amp Short for ampere, a measurement of electrical current.

analog signal Used mainly by older video ports, modems, and sound devices; its signal strength varies in amplitude.

AND operator Used with two or more conditions and returns true only if all expressions are true.

Android A mobile device operating system.

Android OS A mobile device operating system.

antenna A component that attaches to a wireless device or is integrated into it. An antenna radiates or receives radio waves.

anti-malware Software used to protect the operating system and applications.

antistatic bag A plastic enclosure that protects electronic gear from being affected by static charges if the equipment is left exposed.

antistatic wrist strap A strap that connects a technician to a computer that equalizes the voltage potential between the two to prevent electrostatic discharge (ESD).

antivirus Software that protects the operating system and applications from malware.

AP (access point) See *wireless access point*.
APFS (Apple File System) An operating system developed and owned by Apple that is used on desktop computers and iPads. It uses GPT partitions and allows disk cloning.
APIPA (automatic private IP addressing) A Windows option that enables a computer to automatically receive an IP address from the range 169.254.0.1 to 169.254.255.254.
app fails to close The process to go through on a mobile device to manually stop the app. May require rebooting the device.
app fails to install On a mobile device, check that the app is compatible with hardware/OS and has available storage.
app fails to launch See if the app is already running. Close the app and reopen.
App Store An Apple tool that enables a user to shop for various applications to download on a device.
Apple Macintosh OS Any operating system on an Apple device, including OS X, iOS, and macOS.
application crash A situation in which a specific program quits working. In the Windows environment, use Task Manager to quit a crashed application.
application log Whenever an application is crashing or not operating properly, the operating system logs that issue. In Windows, use Event Viewer to see such information.
application spoofing A mobile app that is not from a trusted source.
application update In the corporate environment, MDM is used to push app changes to mobile devices after testing the change.
apply button An option within the Windows OS that makes any changes take effect immediately.
apply update After an operating system installation, do not forget to download and install the operating system and application updates as well as check for newer device drivers.
Apps A Windows Settings category that contains options for installing, uninstalling, and configuration applications.
apt Allows management of application packages
`apt-get` The Linux command-line interface tool that is the equivalent of Ubuntu Software Center; a utility to manage software.
APU (accelerated processing unit) A processor that combines a central processing unit (CPU) with a graphics processing unit (GPU).
ARM (Acorn RISC Machine) A type of processor used in mobile devices that requires low power, is fast, and is low cost.
ARM processor A type of processor used in mobile devices, servers, and microcontrollers that runs cooler, takes less power, and is cheaper than Intel and AMD processors.
array missing When a RAID array was working, but now it is missing, check for a virus, a failed drive, a failed controller, or the presence of a partition table left over if one of the drives was used previously in a non-RAID situation.
asset tag A method of IT inventory used on hardware and network items.
assigning/changing drive letter In Disk Management, right-click on a drive volume > *Change Drive Letter and Paths.*
attitude A person's behavior and/or mindset toward another person or a thing.
`attrib` A command that designates a file as hidden, archived, read-only, or a system file.
attribute An operating system condition used to hide, archive, make a file read-only, or designate a file as a system file.
audio issue A problem with sound output includeing on a projector. Check muting, volume settings, and cabling.
audio/video editing workstation A computer used to create and modify sound or video files. The computer commonly has multiple powerful multicore processors, maximum system RAM, specialized video and audio cards, one or more fast and large-capacity hard drives, good speakers, a high-quality mouse, dual displays, and possibly a digital tablet and scanner.
audit log Information saved on servers and printers that can be used when troubleshooting problems. On a printer or print server, this might be called a print log.
auditing Tracking network events such as logging onto the network domain. Auditing is sometimes called event logging or simply logging.
AUP See *acceptable use policy*.
authentication The process of determining whether a network device or person has permission to access a network.
authentication failure A potential problem when the issue could be a forgotten userID/password, a problem with the authentication server, a problem with the network somewhere along the communication path, or misconfigure permissions for a particular network resource.

authenticator application An app that can be downloaded and, if a site is configured to use it, provides an additional level of security for mobile devices sites.
authorization Controls what network resources—such as files, folders, printers, video conferencing equipment, fax machines, scanners, and so on—can be accessed and used by a legitimate network user or device.
Automatic Updates A method for getting newer Windows operating system files.
availability A desired network feature where the network is available to be used 99.999% of the time.

B

`.bat` A file extension used with a batch file (a file that has multiple commands that, when executed, run one after another). See also *batch file*.
b/s (bits per second) The number of 1s and 0s transmitted per second.
Back to My Mac A feature in the *System Preferences* iCloud menu that enables you to browse that Mac from another macOS device. The remote Mac appears as a shared device in Finder, enabling you to browse the file system.
Bluetooth and devices A Windows Settings category that contains many of the peripheral configuration options for the computer, such as USB, Bluetooth device, cameras, pointing device, and printers.
back up data Before making changes to a system, back up the data.
backlight A fluorescent lamp or LEDs that are always on for an LCD.
backup A precautionary technique used to have a secondary piece of hardware or backup software/files.
backward compatibility In software, the ability of an application to run on older operating systems.
badge reader A security device to allow entry into a space.
badging A method of securing a printer when an ID is scanned to allow printing.
bandwidth The width of a communications channel, which defines the channel's capacity for carrying data.
barcode A series of lines used to uniquely identify items. In IT, a barcode is commonly used on an asset tag for PC hardware and network items.
baseline A snapshot of a computer's performance (memory, CPU usage, and so on) during normal operations (before a problem or slowdown is apparent).
basic disk A Windows term for a drive that has been partitioned and formatted.
basic storage A Windows term for a partition. Contrast with *dynamic storage*.
batch file A Windows-based script that can only be interpreted by the Windows operating system. A batch file has the extension `.bat`.
battery A small self-contained unit used to power a device without using an AC outlet.
battery not charging In this situation, inspect the battery compartment. Try to charge with a different connector, such as a car adapter.
be on time A good work habit to have. If you are going to be late for work, contact your supervisor. If you are going to be late for a customer appointment, notify the customer.
biometrics The use of one or more devices that can authenticate someone based on one or more physical traits such as a fingerprint, an eyeball (retina), or a hand, or a behavioral trait such as voice or signature.
BIOS (basic input/output system) A chip that contains computer software that locates the operating system, POST, and important hardware configuration parameters. Also called ROM BIOS, Flash BIOS, or system BIOS. Replaced with UEFI BIOS.
BIOS password Protection that is not enabled by default for the BIOS/UEFI setup program.
bit An electrically charged 1 or 0.
BitLocker A Microsoft utility that encrypts an entire disk volume, including operating system files, user files, and paging files. The utility requires two disk partitions at a minimum.
BitLocker To Go A Microsoft application that can encrypt and password protect external drives and removable media that are 128 MB or larger.
blackout A total loss of AC power.
blank screen A problem with power (no power, bad power supply), CPU, CPU cooling, motherboard, no power to the display, disconnected video cable, faculty display, or turned off display.
blue screen *or* blue screen of death See *BSOD*.
Bluetooth A wireless technology for personal area networks (PANs).
BNC connector (Bayonet Neill–Concelman connector) A connector used on coaxial cable.
bollard An upright post that tends to be a set in front of a door used as a security deterrent.
boot The process of a computer coming to a usable condition.

bootable device not found An error message indicating you should check the boot order. If correct, the operating system needs to be installed or reloaded.
Boot Camp A boot loading utility designed to assist with partitioning, installation, and support in running Windows on a Mac.
boot options In the BIOS configuration settings, boot options prioritizes devices in the order in which the computer looks for boot files. Also known as boot drive order, boot sequence, or boot menu.
boot partition A type of partition found in Windows that contains the operating system. The boot partition can be in the same partition as the system partition, which is the part of the hard drive that holds hardware-specific files.
boot password A BIOS/UEFI setup option used to access the computer before the operating system loads.
boot process The specific order a device goes through to power up, locate an operating system, and automatically load services and applications.
boot sector Previously called DBR or DOS boot record, a section of a disk that contains information about the system files (the files used to boot the operating system).
boot sector virus A virus program placed in a computer's boot sector code, which can then load into memory. When in RAM, the virus takes control of computer operations. The virus can spread to installed drives and drives located on a network.
boot volume Holds the majority of the Windows operating system files. Can be the same volume as the system volume (which holds the Windows boot files.
`bootrec` A Windows command used to repair and recover from hard drive problems.
bps (bits per second) A measurement of speed.
BranchCache A wide area network (WAN) bandwidth optimization technology.
broadcast address An IP address that communicates with all devices on a particular network.
broken screen A mobile part that might have to be replaced and might require removing the keyboard, drive, memory, and motherboard to access the screens in order to replace.
brownout A loss of AC power due to overloaded electrical circuits.
browser extension Downloadable code to provide an enhanced browser feature or functionality.
browser patching A security update for a web browser.
browser plug-in An executable file downloaded to provide an enhanced browser feature or functionality.
browser synchronization Allows settings such as bookmarks and passwords to be coordinated across multiple devices when the user is signed into the account.
brute force A type of attack in which repeated attempts are made to try to gain access to a network device or stored material.
BSOD (blue screen of death) In Windows, the monitor screen displays all blue, and the computer locks or is nonfunctional.
buffered memory A type of memory in which the modules have extra chips (registers) that delay data transfers to ensure accuracy.
burn-in An image imprint, or ghost image seen on a display screen when an LCD or plasma display has been left on too long.
burning smell A symptom that there is something wrong with the power supply.
burnt-out bulb A possible issue when a projector does not display anything.
business email compromise (BEC) An email that appears legitimate (but isn't) and asks for what appears to be legitimate requests (but they aren't).
BYOD (bring your own device) A situation in which personal mobile devices are brought to the work environment and used on the wired or wireless network.
byte 8 bits grouped together as a basic unit.

C

`c` A Linux command used to list the contents of the current working directory.
cable management system A system that helps keep network cables neat and organized. Ladder racks are a type of a cable management system.
cable modem A modem that connects to the cable TV network.
cable stripper A tool used to cut away the sheathing over a cable's copper wire. Also called a wire stripper.
cable tester A tester that checks coaxial and UTP cable ends (depending on the model) to determine if cable terminals are suitable for use.
cache memory Fast memory designed to increase processor operations.
calendar A method of scheduling that is commonly synchronized across devices.

calibrate (inkjet) A printhead alignment process that must be performed when installing the printer and when replacing the printhead.

calibrate (laser printer) A maintenance task where you can adjust for print density.

capacitor swelling A bulging end or top of this small component indicates that it is time to change it or the component of which it is a part, including the motherboard.

carriage belt An internal inkjet printer part that moves the printhead.

Cat 5 Another name for Category 5 twisted pair cable that has a bandwidth maximum of 100 MHz, a maximum transmission speed of 100 Mb/s, and a 100-meter (328-foot) maximum cable distance.

cat used to concatenate (join) and display the contents of one or more files to the terminal, or to create new files.

Cat 5e Another name for Category 5e twisted pair cable that has a bandwidth maximum of 100 MHz, a maximum transmission speed of 1,000 Mb/s, and a 100-meter (328-foot) maximum cable distance. This type of cable reduces crosstalk found in Cat 5 cable.

Cat 6 Another name for Category 6 twisted pair cable that with the Cat 6a specification has a bandwidth maximum of 500 MHz, a maximum transmission speed of 10,000 Mb/s, and a 100-meter (328-foot) maximum cable distance.

Cat 6a A type of Ethernet cabling that has the wires twisted closer together than Cat6 so that speeds up to 10 Gb/s can be achieved up to 328' (100m); cabling sometimes have a thicker conductor and jacket.

Cat 7 A type of Ethernet cabling that commonly uses some form of shielded twisted pair (STP) cabling and supports speeds up to 40 Gb/s.

CCFL (cold cathode fluorescent lamp) The older flat-panel backlight technology used before LED backlights were used.

`cd` The same as the `chdir` command in Windows. Used from a Windows or a Linux/macOS command prompt to move into a different directory.

CDMA (Carrier Detect Multiple Access) A protocol used on older 2G/3G mobile networks.

cellular card Used to connect a laptop to a cell phone network.

cellular location service Software used to pinpoint where a mobile device can be found.

Certificate Manager A Windows tool used to view, modify, import, export, or delete a digital security certificate.

certificate of destruction A security measure that provides proof that printed material or stored data has been destroyed.

certificate warning Web browsers might present a certificate message that requires using the Microsoft Certificate Manager to see details about the certificate and view, modify, import, export, or delete the certificate.

change board A group of individuals who approve IT projects within an organization.

change default admin user account password A security best practice is to change the default admin user account password or create an account that has Administrator access and disable the default account.

change freeze A timeframe where no changes are allowed to a specific IT system or all IT systems.

change management The formal process of systematically choosing and implementing business changes.

channel A specific number that signifies the frequency used by a wireless device to transmit and receive. Also called a channel ID.

charging A laser printing imaging process that can also be known as conditioning. This process gets the drum ready for use by applying a uniform voltage on the drum surface by using a primary/main corona or a conditioning roller.

charging USB port A port that can provide power to charge and run an unpowered attached device such as a flash drive.

charm A Windows 8/8.1 sidebar item that, when displayed, provides quick access to a particular function, such as Search, Share Content, Start Screen, Devices, and Settings.

checkpoint In a virtualization environment, a copy or backup of the virtual machine (VM) at a particular point in time used to revert the VM to that point in time.

`chkdsk` A program that locates clusters that are disassociated from the appropriate data file.

`chmod` A Linux command that gives the file owner read, write, and execute permissions.

`chown` A Linux command that changes ownership.

Chrome OS An operating system supported by Google and Google partners that is used on laptops.

CIDR (classless interdomain routing) A type of subnet mask that does not have a classful boundary. CIDR is a method of allocating IP addresses based on the number of host addresses needed for a particular network.

CIFS (Common Internet File System) A version of Server Message Block (SMB) that can provide access to shared network devices, files, and printers, especially in a mixed environment of MAC and Windows computers. SMB/CIFS use port 445.

`cipher` A Windows command used to decrypt, modify, or copy an encrypted file.

CL rating (column address strobe [CAS] latency rating) The amount of time (number of clock cycles) that passes before the processor moves on to the next memory address. Chips with lower access times (CL rating) are faster than those with higher access times (larger numbers).

clarify customer statement A technique where the technician asks open-ended questions that provide more information than questions that result in just yes or no answers.

clean a laser printer A maintenance task where you vacuum inside a laser printer using a special vacuum bag.

clean install Loading of an operating system on a computer that does not already have one installed.

clean the heating element A maintenance process task for a thermal printer.

clean the printhead A task done through the printer software or, if clogged, taking a clean lint-free cloth to softly wipe the printhead.

cleaning A laser printing imaging process that describes removing residual toner from the drum by using a wiper blade or brush.

clear browsing data Removing all cookies, browsing history, and other data tracked by a web browser.

clear cache Used to troubleshoot browser issues such as a page not displaying correctly or not formatted properly.

clear jam A process of checking the printer paper path for obstructions or creased paper.

client-side DNS A situation in which individuals or businesses configure their computer to use one or more Domain Name System (DNS) servers to translate uniform resource locators (URLs) into IP addresses.

clock An electronic component that provides timing signals to all motherboard components. A PC's clock is normally measured in MHz.

clock speed The rate at which timing signals are sent to motherboard components (normally measured in MHz).

cloud services Functions provided through a network on devices that are either remote or they are local, but managed and configured through remote applications. Examples include wireless networking, network switches, servers, printing, scanning, and file storage.

cloud storage A method of preserving data in a remote location.

cluster The minimum amount of space that one saved file occupies.

CMDB (configuration management database) A computer or server that has software on it that provides for a structured way of collecting, analyzing, sorting, and displaying data.

cmdlet A function used and associated with a particular operation when creating tasks within PowerShell.

CMOS (complementary metal oxide semiconductor) A special type of memory on a motherboard in which Setup configuration is saved.

CMOS battery A small, coin-shaped lithium battery that provides power to CMOS memory.

CNAME record A type of DNS record that can be used to make DNS management easier. For example, www.pearson.com can be mapped to pearson.com.

coaxial A type of cabling used in video connections that has a copper core surrounded by insulation and shielding to protect against EMI.

collate In printing, complete copies of documents in numerical order one set at a time.

color depth The number of bits that control color and determine the maximum number of colors that can be displayed.

`command` A command issued from the Run utility in Windows to bring up a command prompt window.

`command /?` A command issued from the Run utility in Windows to list commands and options that are available for that particular command. Replace *command* with a particular command, such as `dir /?`.

command prompt Otherwise known as a prompt, or command-line interface (CLI) a text-based environment in which commands are entered.

command switch An option used when working from a command prompt that allows a command to be controlled or operated on differently.

command-line interface An operating environment that is not graphical and in which only typed commands are available.
comment In a script, a comment is used to explain what some part of the code does, but it is ignored by the computer when running the script.
community cloud A type of cloud deployment model that is a combination of a private cloud and a public cloud.
comparison operator A function used in scripting to evaluate two values.
compatibility A feature of hardware or software that allows functionality on multiple models.
Compatibility Mode A Microsoft Windows tool used to emulate older operating systems so that older applications or hardware can be used on a newer operating system.
compiled program Software that must be turned into machine language before it can execute.
component/RGB video Three RCA jacks commonly found on TVs, DVD players, and projectors. One connection is for luminescence (or brightness), and two jacks are for color difference signals.
compound condition A situation in scripting in which two test conditions are contained in a single statement.
compressed air A can of air whose top can be pressed to direct high-powered air that removes dust from hard-to-reach places such as under keys, under motherboards, and inside power supplies and devices.
compression Compaction of a file or folder to take up less disk drive space.
Computer Management A Windows tool that displays a large group of tools on one screen.
computer reboot A symptom that something is wrong with the power supply, CPU, or motherboard.
configuration profile Used in mobile device management (MDM) to push out settings and apps based on a user's role within a company.
connectionless A feature of UDP protocols that make data transfers faster, but packets can be dropped and are not resent as packets sent using application layer protocols that use TCP can be. Examples of application layer protocols that are connectionless are DHCP and TFTP.
connection-oriented A feature of TCP that creates a connection to a destination before data is sent. Examples of application layer protocols that are connection-oriented are HTTP, HTTPS, and SSH.
connectivity issues (printer) Check if correct printer is chosen and correct port. Check cabling. For networked printers ensure the wired or wireless network is available.
Console In macOS, a centralized place to find system and application logs and messages. It allows parsing manually or by searching for something specific.
construct In the 1960s, scientists proved that all programming code can be done using three constructs: sequence, selection (or decision), and repetition (or loops).
contacts People information that is stored in email as well as synchronized across devices.
container An app development environment where all the resources for particular code are held.
content filtering A device or software that screens data for suspect security risks.
context menu A menu of options usually available from the main menu that is brought up by right-clicking an item.
Continuity Camera A macOS feature that lets a user use their iPhone as a webcam for their Mac computer.
Continuity Markup A macOS feature that lets a user make marks with their Apple Pencil on an iPad or with their finger on an iPhone and see updates live on their Mac.
Continuity Sketch A macOS feature that lets a user create a sketch on an iPad or iPhone that automatically inserts into any document on their Mac.
continuity An electrical resistance measurement to see if a wire is good or broken.
continuous ink system A method of providing extra ink in an inkjet printer for heavily used printers.
continuous reboot A symptom of a CPU, motherboard, or power supply problem.
Control Panel A Windows utility that allows computer configuration such as adding or removing software, adding or removing hardware, configuring a screen saver, adjusting a monitor, configuring a mouse, installing networking components, and so on.
control plane A part of software-defined networking that is involved with the "brains" of whatever network device is being virtualized such as a routing table being built in preparation of routing data to a remote destination or MAC address table being built in order to do switching the data to a specific port to get the data to a specific device. Contrast with data plane.

convergence The use of the traditional data network for other type of traffic, like voice and video traffic (which used to have a network of their own).
`convert` A command issued from a command prompt that changes an older file system into NTFS.
copper cabling A type of cabling used to bring video channels into and throughout a home and with home and business wired networks that uses electrical pulses to represent data in contrast to light pulses used in fiber optic cabling.
`copy` A command used from a command prompt to transfer one or more files from one place to another.
`cp` A Linux command to copy a file. Short for copy.
CPU (central processing unit) See *processor*.
CPU socket The motherboard part where a processor inserts.
CPU speed The rate at which the CPU operates. It is the speed of the front side bus multiplied by the multiplier. Normally measured in GHz.
CPU throttling Reducing the clock frequency to reduce power consumption.
Credential Manager Where Windows stores login credentials such as usernames, passwords, and addresses.
crimper A tool that permanently attaches an RJ45 or RJ11 connector to a copper core cable.
crossover cable Cabling that connects two like devices (for example, two computers, two switches, two routers).
cross-platform virtualization Using virtualization to run a different OS than was intended for the machine such as Windows on a Mac computer.
cryptominer Malicious software code that uses a computer's processing power in order to do cryptomining of digital currency.
curl (short for Client URL) is a CLI tool that enables data transfer over various network protocols.
cursor drift A situation in which the mouse pointer moves across the screen even if no one is touching the input device. Commonly caused by improper touchpad sensitivity settings, outdated drivers, or malware.

D

.dmg A .dmg file is a disk image (similar to a .iso disk image file); often used to distribute and install MacOS applications.
DaaS (Data as a Service) A type of cloud service that provides data to a company.
DaaS (desktop-as-a-service) An outside company that provides the OS and apps to multiple computers.
Dash The universal search tool built in the macOS Launcher bar. It searches local content as well as internet sources, all of which can be enabled or disabled simply by opening up Dash.
data at rest Data that is stored in some location. Data at rest should be encrypted or passworded.
data cap A limit imposed by an internet service provider usually based on contract.
data plane A part of software-defined network that is involved with moving data from one location to another. Contrast with control plane.
Data Sources Also called Data Sources ODBC (open database connectivity), a programming interface that allows applications to access data from a database.
database server Holds data for applications and users in an organized way so that data can be stored, organized, managed, and analyzed for business operations.
DB9 A male port on older motherboards, networking equipment, and projectors. Also known as a serial or RS-232 port.
DBR (DOS boot record) An area of a disk that contains system files.
DC (direct current) The type of power a computer needs to operate.
DC jack A part on a laptop where the external power brick attaches.
`dd` In Linux, an advanced command-line interface command that copies and converts files.
DDoS (distributed denial of service) A type of security attack in which several computer systems are used to attack a network or device with the intent of preventing access such as to a web server.
DDR3 (Double Data Rate 3) An upgrade from DDR2 for speeds up to 1,600 MHz that better supports dual-core and quad-core processor-based systems.
DDR4 (Double Data Rate 4) Operates at a lower voltage and faster speeds than DDR3 and lower modules.
DDR5 (Double Data Rate 5) Lower voltage memory module that requires a DDR5 motherboard memory expansion slot.
dead pixel A pixel on an LCD monitor that does not illuminate. Displays commonly have one or more of these.
decision structure A decision (or selection) structure consisting of a test condition together with one

or more groups (or blocks) of statements. The result of the test condition determines which block of statements will be executed.

declaration To create a variable in a script, it must be declared. The exact syntax of how to do this is known as a variable declaration.

dedicated resources RAM, CPU, and storage space set aside for a particular application. Contrast with shared resources such as those used in a cloud environment where resources are shared between apps.

default gateway The IP address of a Layer 3 device, such as a router, that is directly connected to its immediate network. It tells a device on its network where to send a packet destined for a remote network.

default printer When a computer can use multiple printers, the one printer that all applications use by default. A computer user can change the printer to a different one through the Print dialog window. To mark a printer as default, right-click the printer icon and click the *Set as Default* option.

`defrag` The Windows command that starts the defragmentation process of reordering and placing files in contiguous sectors for better performance.

defragment the hard drive See *defragment*.

defragmentation A process of reordering and placing files in contiguous sectors.

degaussing Using a strong electromagnet (sometimes called a degausser or degaussing coil) to change a drive's magnetic field as a security measure for erasing a drive degausser.

degraded performance A decline or deterioration in the performance of a system, component, or service.

`del` A command issued from a command prompt that deletes a file or folder.

desktop The interface between the user and the applications, files, and hardware, which is part of the graphical user interface environment. It is the area in which all work is performed.

desktop alert A message that appears relating to the system or notifications chosen by the user, but can also be a security-related message regarding a problem or potential threat.

developer mode An Android setting that allows customizing a mobile device but could also open up security vulnerabilities.

developing A laser printer process in which toner is attracted to the laser printer drum.

device driver Special software that allows an operating system to access a piece of hardware.

device encryption Securing a device by making the stored data unreadable without a key.

Device Manager A Windows Control Panel utility used to manage hardware settings and software drivers.

Devices A Windows Settings subcategory used to manage Bluetooth settings, remove hardware devices, and configure other device settings.

Devices and Printers A Windows Control Panel utility used to view and manage devices, printers, and print jobs.

df Displays free disk space

DHCP (Dynamic Host Configuration Protocol) A method to automatically assign IP addresses to network devices from a pool of IP addresses. DHCP uses ports 67 and 68.

DHCP exclusion]An address that is not in the range configured on a DHCP server and are not dynamically assigned to end devices.

DHCP lease time The amount of time in minutes, days, or hours that a device that receives an IP address from a DHCP server gets to keep the address.

DHCP reservation One or more IP addresses set aside for specific network devices like routers, switches, and printers that need an IP address that does not change.

DHCP scope The starting IP address and ending IP address for a pool of addresses to be issued to network end devices.

DHCP server Software configured on a network server or router that issues IP addresses from its pool of numbers upon request to a network device.

dial-up network A network formed by using a modem that connects to the traditional phone network. The modem connects to a remote network device.

dictionary [attack] A brute-force security attack that tries to determine a password by using words in a dictionary in order to gain access to data.

differential backup A backup that backs up files that have changed since the last full backup (files that have the archive bit set to on) but in which the backup software does not reset the archive bit, as an incremental backup does.

dig dig command in Linux is a powerful tool for querying the Domain Name System (DNS) to retrieve information about domain names, such as IP addresses, MX records, and nameserver details, aiding in DNS troubleshooting and analysis.

digital signal A signal using 1s and 0s to represent data.

digital signature Confirms that the hardware or updated driver being installed is compatible with Windows; sometimes called driver signing.

digitizer Provides input into documents such as architectural drawings, technical plans, and photos. It can also be used to draw electronic pictures.

dim display In this situation, check display settings and the battery level. The display could require calibration.

DIMM (dual inline memory module) A style of 168-pin, 184-pin, 240-pin, or 288-pin memory chip normally used for RAM chips on Pentium and higher motherboards.

`dir` A command used from a command prompt that displays the contents of a directory.

direct burial cable A type of cable that has extra insulation, cover, and waterproofing added so it can be used underground without any additional protection.

directional antenna A type of antenna that radiates energy in a specific direction.

directory In older operating systems, an electronic container that holds files and even other directories. Today's operating systems use the term *folder*.

directory services A database of users, devices, apps, usernames, and passwords that are used to not only verify a user, but also to manage access privileges. Examples include Microsoft Active Directory, AWS Directory Service, and Azure Active Directory.

DirectX A Microsoft technology that integrates multimedia drivers, application code, and 3D support for audio and video.

disable a service In Windows, use the *Services* option from within the Computer Management console in order to disable a service that might be causing issues.

disable Autoplay AutoPlay is a setting that is used to control what happens when you insert media. A best practice for security is to disable this option.

disable Autorun A setting that dictates whether software or programs start automatically from discs, USB, or other drives.

disable guest account A Windows security best practice.

disable Windows application Use the System Configuration utility *Startup* tab to disable applications that start automatically.

disappearing files A symptom of malware.

discrete GPU (dGPU) A processor installed on a video card that does all the graphics processing instead of the motherboard CPU.

disk cache A portion of RAM set aside for hard drive data that speeds up hard drive operations. A cache on a hard drive controller is also known as a data buffer.

Disk Cleanup A Windows utility that helps free up hard drive space by emptying the Recycle Bin, removing temporary files, removing temporary internet files, removing offline files, and so on.

Disk Management A Windows tool used to partition and manage hard drives.

disk mirroring A process that protects against hard drive failure by using two or more hard drives and one disk controller. The same data is written to both drives. If one hard drive fails, the other hard drive continues to function. Disk mirroring is considered to be RAID level 1.

disk striping Another name for RAID 0, in which data is alternately written on two or more hard drives, thus providing increased system performance.

Disk Utility A powerful application that manages disks and images in macOS. The utility can rename, reformat, erase, repair, and restore disks. It should be approached with caution because the wrong usage could delete all data on the system or on an attached external disk.

`diskpart` A command-based utility used in preparing hard disk partitions and volumes for use.

`dism` (Deployment Image Servicing and Management) A Window utility used to repair and prepare Windows images.

DisplayPort A port, developed by Video Electronics Standards Association (VESA), that can send and receive audio and video signals. Used primarily for display devices and can connect to a single-link DVI or HDMI port with the use of a converter.

Displays A macOS System Settings tool that provides settings for managing the resolution, brightness, and color consistency of the displays. Manages layout when multiple displays are attached.

distorted image A display issue that can be caused by faulty electronics or broken/bent pins on a cable. The problem could also be a faulty display or video card/port.

DLP (data loss prevention) A strategy that uses software (AI and machine learning) and processes to detect, monitor, and protect corporate data.

DMZ (demilitarized zone) A network area that is separate from the corporate network but contains servers that are accessible to outside devices.
DNS (Domain Name System) Translates internet names into IP addresses. DNS uses port 53.
DNS server Application on network server that translates internet names into IP addresses.
DNS TXT A type of DNS message used by email apps to try and determine if a message is from a trusted source/domain.
Dock The shortcut organizational bar used for launching, switching, and managing applications in the macOS graphical user interface (usually the bar at bottom of screen).
docking station A part that has connections for a monitor, printer, keyboard, and mouse that allows a laptop computer to be more like a desktop system. Sometimes called a mobile docking station or a laptop docking station.
document changes The part of change management that creates a historical record of what changes occurred.
documented business processes A set of business documents that relate to how things are supposed to be done or have been done in the past.
Documents A default Windows folder where files are saved.
does not autorotate A problem with the device settings, another app, outdated OS, G-sensor, or accelerometer.
domain A term used in Windows server-based networks where users are required to have logins, and file storage, email, and web-based services are commonly provided. A way of organizing user accounts and network devices in Microsoft's Active Directory service.
domain access Allowing an account or a device onto a Microsoft corporate network.
door lock A keyless entry option for a smart home that allows keyless entry. It is also important to have a door lock of any type on the room(s) that hold network infrastructure equipment such as routers and switches.
DoS (denial of service) A type of security attack in which the intent is to make a machine or a network unusable.
dot matrix printer See *impact printer*.
double image A burn-in; an image seen on a display screen when an LCD or a plasma display has been left on for too long.
downloadable package A collection of files that can be downloaded from a source and then used on a computer; often used for installing software.
downstream Describes information pulled from the internet, such as when viewing web pages or downloading a file.
DRAM (dynamic random-access memory) One of two major RAM types, which is less expensive but also slower than SRAM. DRAM requires periodic refreshing of the stored 1s and 0s.
drawing pad A device used to draw, annotate an existing document or drawing, type, or write. Also known as a drawing tablet or graphics table. Commonly used by teachers, graphic artists, space planners, and engineers.
Drive (iCloud Drive) Apple's cloud service that for uploading, viewing, deleting and sharing files.
drive activity LED A light on the front of a hard drive that blinks when data is being retrieved or written.
drive encryption (BIOS) A BIOS/UEFI setting that scrambles all the data on the hard drive as a security measure.
drive not recognized A storage device error condition that indicates something is wrong with the physical settings, BIOS/UEFI settings, or cabling, or that there is a lack of power.
drive partition A method of allocating space on a hard drive that is recognizable by the operating system.
drive status A storage device state that can be viewed in Windows Disk Management.
drive wipe A technique that can be used to eradicate personal or corporate data from a hard drive before donating or reusing a computer.
driver See *device driver*.
DRM (digital rights management) Technology used to implement controls placed on digital media.
DSL (digital subscriber line) A type of internet connection that uses a traditional phone line. A filter is needed on each phone outlet that has a normal analog device attached to separate the analog sound from the internet data.
dual rank A type of memory module that has two single rank sets of DRAM chips. (Note that the CPU usually accesses only one rank at a time.)
dual-channel A system in which the motherboard memory controller chip handles processing of memory requests more efficiently by handling two memory paths simultaneously.

dual-rail power supply Describes two +12-volt lines available in a power supply.
dumpster diving A social engineering type of threat in which someone digs through trash in or out of the office as a way to get information.
duplex An assembly option that allows a printer to print on both sides of a paper without intervention. Duplex is also a NIC setting to choose between half (transmits in one direction at a time), full (transmits and receives simultaneously), or auto.
duplexing assembly An option available on some printers to allow two-sided printing.
dust cleanup An unsafe condition for technicians to work in without an air filter or mask.
DVI (Digital Visual Interface) A port on a digital video adapter that connects flat panel monitors to the computer.
DVI port A port on a video adapter that connects flat panel monitors to the computer.
DVI-to-HDMI adapter A video connector with a DVI connector on one end and an HDMI connector on the other.
`dxdiag` A Windows command to access DirectX software that helps resolve DirectX display and sound driver problems.
dynamic disk A Windows term for a volume that can be resized and managed without rebooting.
dynamic IP address A way of obtaining IP addressing information from a DHCP server.
dynamic storage A disk that has been configured for the Windows operating system that can be resized and managed without rebooting and contains primary partitions, extended partitions, logical drives, and dynamic volumes.

E

/etc/fstab fstab file specifies which file systems (disks or other directories) are mounted to the computer when it boots.
/etc/hosts Contains a list of hostnames and their associated IP addresses. Before the computer sends a hostname to a DNS server, it searches for the hostname and the IP address in /etc/hosts.
/etc/passwd Stores user account information like usernames, group IDs, and home directories.
/etc/resolv.conf file contains a list of network DNS servers. If the computer is connected to a network, the computer sends a hostname to a DNS server and the DNS server responds with the IP address associated with that hostname
/etc/shadow Actual passwords are stored in /etc/shadow, which is encrypted for security purposes.
Easy Transfer A free application from Microsoft that copies files and operating system settings to another drive, removable media, over a network, or to another storage location.
ECC (error correcting code) RAM Uses a mathematical algorithm to verify data accuracy on the data within a memory module.
`echo off` A command used from a command prompt that prevents characters from displaying on the screen.
echo image See double image.
EDR (Endpoint Detection and Response) A security platform used to protect computers, laptops, and servers.
effective permissions The final permissions granted for a particular resource. Folder permissions are cumulative—the combination of the group and the person's permissions. The deny permission overrides any allowed permission set for a user or a group. When NTFS and shared folder permissions are both used, the more restrictive of the two becomes the effective permissions.
EFS (Encrypting File System) A Windows encryption feature in which only the authorized user may view or change a file encrypted with EFS.
egress Cloud providers may charge for how much data leaves the cloud.
elasticity The ability for a provider to expand software and hardware quickly in response to a customer's needs.
electrical fire safety Knowledge of how to extinguish an electrical fire using fire extinguisher Type A-B-C or fire extinguisher Type C.
Email & accounts A Windows Settings tool used to manage email, calendar, and contacts apps, as well as accounts for other apps.
email security gateway Filtering that uses machine learning and artificial intelligence to check inbound and outbound email for spam, malware, sensitive corporate data, and phishing.
embedded system A computer that has a specific function within a larger system, such as in medical, manufacturing, or airport industries.

emergency change An unplanned change management type that came as a result of something unexpected happening.

EMI (electromagnetic interference) Electronic noise generated by electrical devices.

encryption A method of securing data from unauthorized users in which data is converted into an unreadable format.

end-of-life A term used with hardware or software that typically means the vendor no longer supports the product.

end-user acceptance A part of change management in which the person who will use an IT system tests the changes to ensure that the deliverables or outcomes have been met.

end-user education A great security method to use because by educating users, security issues get reported and dealt with earlier with less damage to a company. Part of a technician's job might be to teach a user how to do something to avoid technical issues or to prevent security issues.

energy efficiency rating A set of standards applicable to power supplies.

ENERGY STAR A set of energy efficiency standards including those related to total energy requirements and low power mode(s) and an efficiency standard that a product must meet to achieve this standard.

environment variable A variable that describes the environment in which a program runs. It contains a name and a value, where the value is the path to the program identified by the variable name.

EPEAT rating system A rating system that works with the Environmental Protection Agency (EPA) to identify products that have a green (and clean) design.

equality operator A method in scripting used to compare two values. Another name for comparison operator or equals operator.

equals operator A method in scripting used to compare two values. Another name for comparison operator or equality operator.

equipment grounding The components in a device like a PC or rack are at the same voltage potential. Grounding is important to personal safety because consistent grounding minimizes the potential of voltages being applied to places it shouldn't be applied, such as the case. If a piece of equipment is not grounded, someone could receive a shock or be electrocuted simply by touching it.

equipment lock Can be a physical or electronic lock, a special cable that cannot be removed without a tool, or a lock-in device for a port.

Error Checking A Windows tool that checks the drive for file system errors, bad hard drive sectors, and lost clusters.

error message An indication provided by a system or an application that should be noted to help in troubleshooting.

eSATA (External Serial ATA) A port used to connect external SATA devices to a computer.

eSATA bracket A part that installs into an empty expansion slot that has one or more eSATA ports. Each port on the bracket has a SATA cable that attaches to an available motherboard SATA port.

eSATA cable A cable that attaches to an eSATA port located on the outside of a device such as on a motherboard or card. Maximum length is 6 feet (2 meters).

eSATA card An adapter used to add external SATA ports so that external storage devices can be used. May include ports for internal SATA devices.

eSATAp port A port that accepts both eSATA and USB connectors, which can provide power when necessary. Also known as eSATA/USB or power over eSATA.

ESCD (Extended System Configuration Data) A specification that provides the BIOS and operating system a means for communicating with plug-and-play devices. As the computer boots, the BIOS records legacy device configuration information. Plug-and-play devices use this information to configure themselves and avoid conflicts. When an adapter has resources assigned and the resources are saved in ESCD, the resources do not have to be recalculated unless a new device is added to the computer.

ESD (electrostatic discharge) Occurs when stored-up static electricity is discharged in an instantaneous surge of voltage. Cumulative effects of ESD weaken or destroy electronic components.

ESD mat A pad that is placed on a surface to prevent electrostatic discharge events. Such a mat commonly has a place to attach an antistatic wrist strap.

ESD strap An item that fits around a technician's wrist and connects to an electronic component so that the technician and the component are at the same voltage potential, thus preventing an electrostatic discharge event, which can cause damage to electronic components.

eSIM (embedded SIM) A SIM built into cell phones and other devices like smartwatches. eSIMs allow changing network providers without requiring a SIM swap. eSIMs also let you have multiple phone numbers.
Ethernet A network system that carries computer data along with audio and video information. Ethernet adapters are the most common network cards.
Ethernet over Power (EoP) Also called powerline communication. Sends network data to EoP modules that are plugged into power outlets to extend Ethernet networks.
Ethernet port An RJ45 port that connects a device to the wired network.
EULA (end user license agreement) Legal language that specifies what can and cannot be done with a particular software application or operating system.
Event Viewer A Windows tool that monitors various events in the computer.
evil twin A rogue AP broadcasts the same SSID as another AP in the area to intercept wireless traffic.
exabyte (EB) 1 billion times 1 billion bytes, or 2^{60} (1,152,921,504,606,800) bytes.
executable file A file with a `.bat`, `.exe`, or `.com` extension that starts an application, a utility, or a command. A file on which the operating system can take action.
exFAT A file system type that improves upon FAT32 by having a theoretical maximum file size of 16 EB, maximum volume size of 64 ZB (but 512 TB is the current limit), smaller cluster sizes than FAT32, and an increased number of files allowed in a directory. Created for external storage media such as flash drives and hard drives for saving images/video.
expansion slot A motherboard socket into which adapters are connected.
`explorer` A command used on a Windows device to bring up File Explorer.
ext4 (Fourth Extended File System) A file system type used in Linux-based operating systems that supports larger volumes and file sizes than ext3.
extended partition A hard drive division.
extended read/write time An indication a storage device is near full or needing replacement because it takes a longer than normal time to retrieve and/or save data.
extending partition (Disk Management) Increasing the size of a partition by right-clicking on the drive letter and selecting *Extend Volume*.
extensible software Software that is easily upgraded.
extension In operating systems, the three or more characters following the filename and a period (`.`). The extension associates the file with a particular application that executes the file.
external hard drive (boot option) An operating system boot option when a USB or eSATA drive is used.
external interference Wireless devices and other networks can cause problems with wireless network connectivity and reception when using the same unlicensed frequency range.
external shared resources In cloud computing, resources such as servers, applications, hardware such as CPUs and RAM, data storage, and network infrastructure equipment that are shared between organizations through an external vendor.
external storage device A peripheral that attaches to a computer used for saving data.
extremely short battery life In this situation, possibly replace the battery and also close apps and services that are not being used.

F

F-type A type of connector used with coaxial cable that screws onto the cable.
FaceTime Apple's proprietary video and audio calling service, allowing users to connect with other Apple device users via video or audio calls over Wi-Fi or cellular data.
facial recognition lock A type of security lock on a mobile device or computer that uses the integrated camera and stored data to determine whether someone is granted access to the computer.
facial recognition technology (FRT) A security measure used to grant access to someone based on their face being scanned.
factory recovery partition A drive partition that contains files and folders including the operating system, drivers, and preinstalled programs that is used when a system must be rebuilt, restored, or re-created or when troubleshooting Windows problems.
factory reset An option to set a mobile device such as a phone back to original settings.
faded print A condition that arises due to inadequate ribbon, ink level, or toner. Check quality settings. In a thermal printer, reduce the printhead energy or printhead pressure setting.

fail to boot An error condition that occurs when a boot device such as a hard drive is not responding.
failed attempts A Windows feature that locks out a user after a specific number of failed login attempts.
failure to boot A Windows condition that may require operating system repairs or reload.
fake security warning May come through the operating system or a web browser. Do not tap, call, or reply to one of these.
fan A mechanical cooling device attached to or beside the processor or in the case.
fan considerations See fan control.
fan control A BIOS/UEFI Setup option used to control the configuration of case and/or CPU fans, including the ability to place the fans in silent mode and/or control speed.
FAT (File Allocation Table) A method of organizing a computer's file system.
FAT (file system type) A file system type also known as FAT16.
FAT16 A file system supported by DOS and all Windows versions since DOS. DOS and Windows 9x have a 2 GB limit. Newer Windows operating systems have a 4 GB FAT16 partition size limit.
FAT32 A file system that supports hard drives up to 2 TB in size.
FC (Fibre Channel) A standard used to connect the storage area network (SAN) to the other network devices.
feed assembly The part of a computer responsible for taking the paper through the printer.
feeder On a printer, a device that rolls the paper through the paper tray.
fiber cable An expensive network cabling made of plastic or glass fibers that carry data in the form of light pulses. Handles the greatest amount of data with least amount of data loss. Comes in single mode and multi-mode.
fiber network High-speed, high-capacity computer network composed of fiber-optic cables.
File Explorer Options A Windows Control Panel utility used to customize the display of files and folders.
File History A Windows tool that allows backing up a specific user's libraries instead of the entire system and supports scheduling these backups.
file recovery software An application used to recover data from a storage device.
file synchronization An option sometimes available with cloud file storage or a program that you can download that allows you to access files that have been placed in a special folder.
file system Defines how data is stored on a drive. Examples of file systems include FAT16, FAT32, exFAT, and NTFS.
file type A specific type of file based on the application that created it. For example, a `.txt` file created in Word is a different file type than an Acrobat reader `.pdf` file.
fileless Malware that is not stored on a storage device, but is only in RAM making it hard to detect by traditional antimalware software.
filename The name of a file. In older operating systems, the filename was limited to 8 characters plus a 3-character extension. Today's operating systems allow filenames up to 255 characters.
fileshare server A high-end computer configured to store files that can be accessed and managed from a remote location.
FileVault A macOS feature that automatically encrypts the contents of a disk.
Finder Finder is used for navigating and managing files or folders in the file system. It is similar to Microsoft's Windows Explorer/File Explorer.
fingerprint lock A type of security lock on mobile devices and computers that requires a valid and stored fingerprint to be matched with the fingerprint of the person trying to gain access.
fingerprint scanner A biometric security device that requires a finger to be placed on a reader and compared against a stored image.
firewall Software or a hardware device that protects one or more computers from being electronically attacked. It inspects data for security purposes and filters traffic based on network protocols and rules established by a network administrator. Firewalls operate at the application layer of the OSI model.
firmware A combination of hardware and software attributes. An example is a BIOS chip that has instructions (software) written into it.
flash BIOS A type of motherboard memory that allows updates by disk or by downloading internet files.
flash drive A type of memory that holds data even when the power to the device is removed.
flash memory A type of non-volatile memory that holds data when the power is off.

flashing screen A display issue that could be caused by cabling (not being pushed fully in or bent/broken pins.

flatbed scanner A peripheral used to digitize a photo or text.

floating-point number Numbers that can be written in the form $x \div y$, which means they are numbers that include a decimal value, even if that value is 0. For example, the number 7 is an integer, but the number 7.0 is a floating-point number.

folder In Windows-based operating systems, an electronic container that holds files as well as other folders. It is also called a directory.

folder redirection A feature of Microsoft Active Directory that maps a folder on the local machine to a network location such as a server so the user has access to the folder from any device on the network domain.

`for` loop A shorthand way to write a `while` loop.

Force Quit The macOS feature used to stop a program when it stops responding or working correctly.

Force Quit An option used on an Apple device to close an unresponsive app.

form factor The shape and size (height, width, and depth) of motherboards, adapters, memory chips, power supplies, and so on. Before building or upgrading, make sure the device's form factor fits the computer case.

`format` A command that prepares a disk for use.

formatted (disk) A disk that has been prepared to accept data.

forward compatibility A design feature in software that means a system should be able to accept input intended for a later version.

frequency band In wireless networking, a range of specific frequencies used to transmit data. The 3 most common bands used in WLANs are 2.4, 5, and 6 GHz.

frequency response range The range of sounds a speaker can reproduce.

front panel connector A connector found on the motherboard that can have a cable that attaches from the motherboard to the front panel of the computer.

frozen print queue A condition where no print jobs can get through. Clear the print queue by cancelling all print jobs.

FSB (front side bus) Part of the dual independent bus that connects the CPU to the motherboard components.

fsck A Linux command used to check file system consistency and interactively repair issues

FTP (File Transfer Protocol) A standard used when transferring files from one computer to another across a network.

full backup A method of backing up a hard drive in which the archive attribute is used. The backup software backs up all selected files and sets the archive bit to off.

full device encryption A security measure on mobile devices that supports encoding or scrambling all user data.

full format During an installation process to partition a hard drive, this option identifies and marks bad sectors on the drive so they will not be used for data storage. Contrast with quick format.

function key A function (Fn) key that, when used with another key, provides a specific function such as turning up speakers, connecting to an external monitor, or turning on the wireless adapter. This key is commonly found on laptops.

fuser assembly Found in a laser printer; melts the toner onto the paper.

fuzzy image A display issue that can be caused by faulty electronics or broken/bent pins on a cable. The problem could also be a faulty display or video card/port.

G

Gaming A Windows Settings category used to configure the Windows gaming options.

gaming PC A computer design that includes a powerful processor, high-end video or specialized GPU, an SSD, a good sound card, and high-end cooling due to the demands placed on hardware when playing computer-based games.

garbled print A printed output indication that the printer cable is not securely attached or a print driver problem exists.

gateway An IP address assigned to a network device that tells the device where to send a packet that is going to a remote network. Also known as a default gateway or a gateway of last resort.

Gb An abbreviation for gigabit.

GB See *gigabyte*.

GDPR (General Data Protection Regulation) A European Union (EU) security standard developed to protect individuals and firms within the EU.

gestures On a touch device, finger motions (swipe, pinch, tap, spread, and so on) used to manipulate applications or features.

gigabyte Approximately 1 billion bytes of information (exactly 1,073,741,824 bytes); abbreviated GB.

GParted Bundled with Ubuntu, a disk management tool that allows the creation, deletion, and resizing of partitions on a physical disk.

`gpedit.msc` A command that brings up the group policy editor used to control various Windows functions, apps, and what specific groups are allowed to do.

`gpresult` A command that displays Group Policy settings. A Group Policy determines how a computer is configured for both system and user (or a group of users) settings.

GPS (Global Positioning System) A satellite-based navigation system that transmits location information to receivers in mobile devices. Most mobile devices have GPS capability.

GPT (GUID [globally unique identifier] partition table) A type of partition table available in 64-bit Windows editions. GPTs can have up to 128 partitions and volumes up to 18EB.

`gpupdate` A command used to refresh local and Active Directory–based Group Policy settings.

grandfather-father-son backup A backup method where a full backup (grandfather) is done less frequently such as once a month. Then another full backup (father) is done once a week followed by incremental backups (son) daily.

graphic/CAD/CAM design workstation A powerful computer system utilized by design engineers or graphic designers. It usually has multicore processors, high-end video cards with maximum GPU and video RAM, large displays, a large-capacity hard drive and SSD, and maximum system RAM. Uses output devices such as scanner, plotter, or 3D printer.

graphical interface fails to load A Windows startup problem in which startup files are missing or corrupt or there are hardware problems.

`grep` A common Linux utility that searches output for a specified term.

grinding noise The sound that a fan on the motherboard, case fan, hard drive, optical drive or printer could make due to something getting caught in it, lack of oil, improperly inserted disc, or starting to fail. For a printer, check gears, torn paper, paper clips, staples, or labels along paper path.

grounding See equipment grounding.

group policy A type of security policy applied in a network domain environment. The policy dictates what a set of users can do.

group policy editor Used to control various Windows functions, apps, and what specific groups are allowed to do and deploy security settings.

GRUB (Grand Unified Boot Loader) A Linux bootloader that generally replaces the earlier LILO bootloader. It contains all information about how a disk is organized, such as the size and layout of partitions. The latest version is called GRUB2.

guest access A separate wireless network that usually only has access to the internet.

GUI (graphical user interface) In operating systems, an interface in which the user selects files, programs, and commands by clicking pictorial representations (icons) rather than typing commands at a command prompt.

H

hard drive A sealed data storage medium on which information is stored. Also called a hard disk.

hard reset Describes turning a device off and back on or a factory reset of a mobile device.

hardware A tangible, physical item, such as the keyboard or monitor.

hardware token A physical device used to gain access to a resource such as a file or company.

hash Used in security encryption and for file transfers to ensure the file did not get changed during the download.

HDMI (high-definition multimedia interface) An upgraded digital interface that carries audio and video over the same cable.

head crash Occurs when a read/write head touches a platter in a mechanical hard drive, causing damage to the heads or the platter.

header A set of motherboard pins that allows adding a specific function such as USB 2 or 3.x ports, UCB-C ports, SATA/eSATA ports, RGP LEDs, and a Trusted Platform Module (TPM).

headset A mobile wearable device that commonly has a microphone and headphones.

heat sink A metal device for cooling the processor by conducting heat to its fins or bars. Convection then transfers the heat away by flowing air through the case.

heat spreader Aluminum or copper fittings on memory modules used to dissipate heat.
heating element The part on a thermal printer that is part of the printhead.
help A command used to list all of the available commands.
HFS (Hierarchical File System) A type of file system used with Apple computers that has been upgraded to HFS+ and then later upgraded to Apple File System (APFS).
hidden share A share that has a dollar sign ($) added to the share name so that the share is not shown to a remote networked computer.
high-level formatting A process that sets up the file system for use by the computer. It is the third and last step in preparing a hard drive for use.
high latency An undesired network characteristic where packets are dropped frequently and network systems display slow responsiveness to network requests.
high network traffic On a mobile device, try moving to a different location and get closer to the access point or in a different cellular area to get better performance.
high number of ads Can affect a mobile device data plan. Use OS, browser, and app privacy and location settings to block.
high sensitivity of thermal papery Store thermal paper in a cool setting as it is highly sensitive to heat.
hole punch Check if paper that has been hole punched is being misfed or if the chaff from hole-punched paper is causing an issue.
Home A Windows Setting category that contains options for Bluetooth settings, device personalization, and cloud services; not available on devices managed by organizations.
home folder A network folder that allows users to store their files and have access to them from any device that they log onto within the same domain.
home server A server commonly used to act as a web server and print server, control home devices, manage backups, and be accessed from outside the home. A home server commonly includes the capability to stream sound or video, share files, have a Gigabit NIC, or have a RAID hard drive array.
host address A portion of an IP address that represents the specific network device.
host machine In a virtualization environment, the real computer.
hot fix Software that has one or more files that fix a particular software problem. Contrast this to a patch or a service pack.
hotspot A wireless network that has free internet access. Security is a concern because no encryption or authentication is commonly required.
HPA (Host Protected Area) A hidden part of the hard drive that is used to reinstall the operating system. It sometimes contains applications that installed when the computer was sold. Using an HPA reduces the amount of hard drive space available to the operating system.
HSM (hardware security module) Specialized hardware that can be a USB device or a device on the network used for digital key management, storage/protection of cryptographic keys, encryption, and authentication that operates similar to a TPM.
HT See *Hyper-Threading*.
HTTP (Hypertext Transfer Protocol) A standard for internet data communication.
HTTPS (HTTP over SSL) HTTP communication encrypted through an SSL session. With HTTPS, web pages are encrypted and decrypted.
hub A device used with the universal serial bus or in a star network topology that allows multiple device connections. A network hub cannot look at each data frame coming through its ports like a switch does. It forwards data frames (packets) to all ports.
humidity The amount of moisture in the air. The potential for an electrostatic discharge (ESD) event is higher when the humidity is low.
hybrid cloud A type of cloud technology in which the company has some cloud services maintained by internal staff (private cloud) and some cloud services that are outsourced (public cloud).
HyperTransport AMD's I/O architecture in which a serial-link design allows devices to communicate in daisy-chain fashion without interfering with any other communication. Thus, I/O bottleneck is mitigated.
hypervisor In a virtualization environment, the software that creates the virtual machine (VM) and allocates resources to the VM. Also called a virtual machine monitor or virtual machine manager (VMM).

I

I/O address (input/output address) A port address that allows an external device to communicate with the microprocessor. It is analogous to a mailbox number.

I/O shield A part that allows for optimum air flow and grounding for the motherboard ports.

IaaS (Infrastructure as a Service) A type of cloud technology service that describes routers, switches, servers, virtual machines, load balancers, access points, storage, and any other infrastructure device that is provided through the online environment.

iCloud (offsite data storage and email option) An Apple cloud-based service that comes with macOS, offering storage, application support, and syncing of contacts, photos, email, bookmarks, documents, and more between multiple macOS, iOS, and even Windows devices.

ICMP (Internet Control Message Protocol) A Layer 3 protocol used for troubleshooting network connectivity. Commands that use ICMP include `ping`, `pathping`, and `tracert`.

icon An operating system graphic that represents a file, an application, hardware, and shared network resources.

identity access management A framework that outlines policies for managing the user information such as name, phone, title, manager, subordinates, projects, etc. as well as what resources each user or even apps are allowed to access.

identity synchronization Commonly used with corporate customer relationship management (CRM) and enterprise resource planning (ERP) platforms to have a single sign-on allow access to multiple areas.

IDS (intrusion detection system) Software or hardware that is designed to detect potential security issues that could allow an illegal entry to the computer or network. The IDS could log the incident and contact someone in order to prevent invasion.

`ifconfig` In Linux/Unix environments, a command that shows network interface information for Ethernet ports.

iGPU (integrated graphics processing unit) A graphics card built into the motherboard in contrast to having a separate card installed in an expansion slot. An iGPU takes less power and uses motherboard RAM to perform graphics calculations.

image deployment An operating system installation method in which a system image is taken from an external drive, disc, or server and put on a computer.

IMAP (Internet Mail Access Protocol) A protocol used to receive email through the internet. Uses port 143 by default.

iMessage An app tool for sending texts, photos, videos, documents, links, and other media from one Apple device to another Apple device.

impact printer Sometimes called a dot matrix printer. A type of printer that physically impacts a ribbon that places an image on the paper.

impact printhead Holds tiny wires called print wires; found in impact printers.

impersonation A social engineering security threat in which someone pretends to be from your bank or a company such as Microsoft to get you to divulge information or gain access.

improper charging When a phone is inconsistent as to how It charges, inspect the phone connection and clean the battery and pins with compressed air. Check the charger.

in-place overwrite The most common method of recovery data after a failure where backup data is used.

in-place upgrade A method of upgrading Windows when an older Windows version is already installed.

inaccurate system date/time A symptom of the CMOS battery failing or dead.

incident documentation The part of a technician's job to provide details on what has been done about a particular problem.

incineration Destruction of documents or storage devices by fire.

incorrect color A problem caused by bent or broken video pins on a monitor's cable ends.

incorrect data source Check in the input source and ensure it is correct for project output.

incorrect orientation Check the printer page setup when the printed page does not come out the correct way.

incorrect paper size Use the printer properties to select the correct size and orientation of the paper before printing.

incremental backup A method used with a full backup. The incremental backup goes faster because it backs up only files that have changed since the last backup.

identity synchronization The process of synchronizing user attributes (account name, passwords, permissions, etc.) between on-premise networks and cloud networks, as well as across multiple operating systems and applications.

indexing A Microsoft Windows configurable feature that allows quick searches for files and folders.

Indexing Options A Windows Control Panel utility used to change how Windows indexes files and folders to search faster.

ingress Cloud providers may charge for how much data enters the cloud.

inherited permissions A Windows NTFS permission type that is propagated from what Microsoft calls a parent object. For example, if a folder is given the permission Read, then all files within that folder inherit the read-only attribute.

initialization The process in which a variable in a script is given an initial value.

initialize disk A disk option available through the Windows Disk Management tool that enables a disk so that data may be stored on it.

initializing (Disk Management) Making a drive available to be used by right-clicking on a drive > *Initialize Disk.*

ink cartridge A container that holds the ink and the nozzles for an inkjet printer. Also known as a print cartridge.

inkjet printer A type of printer that squirts ink through tiny nozzles to produce print. Inkjet printers produce high-quality, high-resolution, color output.

inkjet printhead Holds the ink reservoir and the spray nozzles; easily replaced.

input A method used to put data into a device or program.

integer A whole number, including zero and negative numbers.

integrated graphics card A video port built into the motherboard that uses motherboard RAM to perform graphics functions.

Intel Corporation The largest processor manufacturer in the world. Intel also makes chipsets, motherboards, network cards, microcontrollers, and other electronic chips and components.

intermittent connectivity A symptom of poor or faulty connections with devices on the same network. Use the `ping` command to check connections all around the network.

intermittent device failure A symptom of a faulty device when sporadic or irregular problems occur with that device.

intermittent projector shutdown A common safety precaution for the projector when it has been used for a long period of time and needs to cool. If this occurs when the projector has only been powered a short period of time, check the filter.

intermittent wireless In this situation, turn off WiFi and turn it back on again. Move the device to see if you get a higher signal strength (display on a laptop).

intermittent wireless connectivity Wireless device connection to the wireless network is affected by obstructions such as walls, trees, concrete columns, rain, snow, fog, other buildings, microwave ovens, and other wireless networks operating in the same unlicensed frequency range.

internal fixed disk (boot option) An operating system boot option that boots from a partition on an internal hard drive.

internal hard drive partition (boot option) An operating system boot option that boots from a bootable partition.

Internet Explorer An older Microsoft browser that is being replaced by Edge.

Internet Options A Windows Control Panel utility used to manage internet connection settings and the appearance of web pages.

Internet-based booting A type of network booting in which the operating system image is retrieved from the internet.

interpreted program Code that is carried out one line at a time.

interrupt See *IRQ*.

inventory list Assets input into an inventory management system or database that can be viewed or printed to see specific details on hardware and/or software maintained by a company.

inverter Converts low DC voltage to high AC voltage for the backlight bulb in an LED display.

IOPS (input/output operations per second) A measurement of hard drive speed for both magnetic drives and SSDs that takes into account sequential reads/writes and random reads/writes.

iOS An Apple operating system for mobile devices.

IoT (Internet of Things) A phrase to describe the technology wave that includes sensors and smart devices to provide data, information, warnings, and control of things like lights, cameras, appliances, thermostats, and locks.

ip a Linux command for managing and configuring network interfaces, routes, and tunnels.

IP (Internet Protocol) A Layer 3 protocol that is part of the TCP/IP protocol suite.

IP address A type of network adapter address used when multiple networks are linked. Known as a Layer 3 address, in IPv4 it is a 32-bit binary number with groups of 8 bits separated by a dot. This numbering

scheme is also known as dotted-decimal notation. Each 8-bit group represents numbers from 0 to 255. An example of an IPv4 IP address is 113.19.12.102. Also see *IPv4* and *IPv6*.

IP addressing scheme A methodical way of setting up network numbers within an organization. Within a company, the IP addressing scheme tends to be private IP addresses.

IP filtering Permits or denies specific network traffic based on websites, users, IP addresses, protocols, or apps.

iPadOS The operating system used on a Macintosh tablet (an iPad).

`ipconfig` A command used from a command prompt in Windows to view the current IP configuration settings.

IPS (intrusion prevention system) A security device that actively monitors and scans network traffic for malicious traffic and violations of security policies as well as takes appropriate action.

IPS (in-plane switching) A type of LCD display that is best to use when viewing from an angle and needing good quality and color.

IPv4 (Internet Protocol version 4) A type of IP address that uses 32 bits (four groups of 8 bits each) shown as decimal numbers in dotted-decimal format. An example of an IPv4 address is 192.168.10.1.

IPv6 (Internet Protocol version 6) A type of IP address that uses 128 bits represented by hexadecimal numbers. An example of an IPv6 IP address is fe80::13e:4586:5807:95f7. Each set of four digits represents 16 bits.

IR (infrared) A technology used for wireless input/output that is useful only over short distances.

IRQ (interrupt request) A microprocessor priority system that assigns a number to each expansion adapter or port to facilitate orderly communication.

iSCSI A fiber standard used to connect the storage area network (SAN) to the other network devices.

ISO file a single file that contains all the files and folders of an optical disk like a CD or DVD.

ISP (internet service provider) A vendor that provides a connection to the internet.

IT automation A method of implementing change where changes to devices or applications can occur without a human doing repetitive changes to multiple systems.

iteration A programming loop that consists of a block of statements that are executed repeatedly for a specific number of times or until a specific condition is met.

ITX (Information Technology eXtended) A motherboard form factor size that is smaller than ATX, the most common form factor. Comes in mini-ITX, nano-ITX, and pico-ITX sizes.

`iwconfig` In Linux/Unix systems, a command that shows network interface information for wireless adapters.

iWork A macOS office productivity suite containing a word processor, a spreadsheet, and presentation applications.

J

`.js` A file extension used with JavaScript files.

jailbreak Compromising the operating system so the user has an increased level of privilege on an iOS mobile device.

JavaScript A programming language that can be run on any operating system. Creating and running JavaScript commands requires installing `Node.js`. The extension that identifies a JavaScript file is .js.

JBOD (just a bunch of disks or just a bunch of drives) A term given to combining more than one drive that is recognized as a single drive letter or a single virtual disk. This is similar in concept to RAID but is not one of the RAID levels.

jitter Irregular receipt of voice packets that is measured in seconds and can cause poor VoIP quality.

join a domain Use the System Control Panel > Change settings > Computer Name tab > Change > Domain. If you are using Azure or another vendor for corporate active directory management, you can use the Accounts Settings link to select Access work or school > Connect.

jumper A plastic cover for two metal pins on a jumper block.

just-in-time (JIT) access Part of a security process called privileged access management (PAM) where a person is allowed access to a system, device, or app for doing something specific and then those rights are revoked.

K

Kb Abbreviation for kilobit.

KB See *kilobyte*.

Kerberos A protocol used in conjunction with an authentication server to prevent transmitted packets from being altered or read.

kernel The heart of an operating system, which acts as the controller and interpreter for nearly everything in a system so that hardware and software can interface and work together. It controls memory management, peripherals, and allocating other system resources to processes.
kernel panic A critical system error that the operating system cannot recover from. When this happens in macOS, the Mac reboots to return to a stable state.
key A physical security measure that can be a physical metal key or an electronic key.
key fob Used for keyless entry.
keyboard Allows users to provide input into the computer.
keyboard port A DIN connector on the motherboard into which only the keyboard cable must connect.
Keychain Access A macOS utility for managing saved passwords securely.
keylogger Software designed to capture keystrokes in an effort to collect user IDs and passwords.
keyword A set of characters that is an instruction in a particular programming or scripting language.
kill A command used through the Terminal application on a Mac or in Linux to halt a program that has frozen or is not responding: `kill -9` (where 9 is the *`process_id`*).
kill task A step to take if an application has frozen or quit responding.
kilobyte Approximately 1,000 bytes of information (exactly 1,024 bytes).
KMS (Key Management Service) A service used in companies that have 25 or more Windows computers to deploy. KMS is a software application installed on a computer. All newly installed computers register with the computer that has KMS installed. Every 180 days, the computer is re-activated for the license. Each KMS key can be used on two computers up to 10 times. Contrast with *MAK*.
knowledge base A collection of documents used to answer commonly asked IT questions or contain IT procedures.

L

/Library A macOS system folder that contains resources that are used throughout macOS, like fonts, internet plugins, and keyboard definitions.
L1 cache Fast memory located inside the processor.
L2 cache Fast memory located inside the processor housing but not inside the processor.
L3 cache Any fast cache memory installed on the motherboard when both L1 and L2 cache are on the processor. Could also be located inside the processor housing.
LAN (local area network) A group of devices sharing resources in a single area, such as a room or a building.
laptop docking station A device used to provide increased connectivity such as one or more displays, wired network connectivity, full-sized keyboard, mouse, and so on.
laptop RAM A memory module that is normally in the SODIMM form factor.
laser printer A type of printer that produces output using an imaging process similar to a copier. Laser printers are the most expensive type of printer.
laser printer maintenance kit A kit that may include a separation pad, pickup roller, transfer roller, charge roller, and fuser assembly, depending on the vendor.
latency The amount of time a packet takes to travel from source to destination. Use the tracert command to see the amount of latency.
launcher A dock-like shortcut bar that allows manipulation of the graphical user interface (GUI) so that multiple apps and/or commands are easily deployed. It has the functionality of being an application launcher shortcut as well as having a universal search feature built-in to it.
Launchpad A macOS application launcher shortcut.
LCD (liquid crystal display) A video technology used with laptops and flat screen monitors. The two basic types of LCD are passive matrix and active matrix.
LDAP (Lightweight Directory Access Protocol) A networking protocol that is used to access, maintain, and distribute directory and database-type information. LDAP uses port 389.
LED (light-emitting diode) A video output technology that is a low-power, low-heat, long-lasting electronic device using liquid crystals.
LED status indicator LEDs on the front of the computer or motherboard can give a clue during the troubleshooting process.
legacy software An older software program that might require an older OS to run or does not run properly under a newer OS.
legacy system An outdated computer system or piece of network equipment that needs to be replaced or updated.

`less` A common macOS and Linux command that shows the contents of a file.

library Windows storage that is similar to a folder but that is automatically indexed for faster searching.

license range A set of wireless frequencies that are managed by the FCC for a specific geographic region.

licensing The legitimacy of using a particular software package through purchasing or registering with the software provider.

lifting technique When lifting equipment, remember to use your legs and not your back.

Lightning port An Apple port/cable used to connect displays and external drives. Commonly used to connect Apple mobile devices like iPhones and iPads to host computers and USB battery chargers.

limited connectivity An error condition in which internet connectivity is lost.

line conditioner A device that protects a computer from overvoltage and undervoltage conditions as well as adverse noise conditions. Also known as a power conditioner.

line down the printed page Lines that appear on printer paper that may be caused by debris on the corona wires or in the developer unit in the laser cartridge. Replace cartridge. Check the drum for debris. On an impact, thermal, or inkjet printer, check the print head and rollers.

link-local address A type of IPv6 address assigned to a NIC. It is used to communicate on a particular network and cannot be used to communicate with devices on a different network.

Linux Released in 1991 by developer Linus Torvalds, a widely used operating system platform that is similar to Unix. It is a free open source operating system that anyone can use, contribute to, and modify. It is widely used in many different areas of technology, such as servers, desktops, embedded systems, and smartphones.

liquid cooling An alternative to a fan or sink for processor cooling. Liquid is circulated through the system, and heat from the processor is transferred to the cooler liquid.

liquid damage A common hazard of mobile devices.

live tile A Windows 8/8.1/10 feature that allows the content within to change, such as a news headline feed.

load alternate third-party driver Part of the Windows installation process that a technician must download drivers for hardware such as a RAID controller before starting the installation process.

load balancer A technology used when you have redundancy such as multiple paths through the network or multiple servers for a particular app or purpose such as DNS.

local security policy Security rules that can be applied to a computer.

local share Something such as a printer, folder, or disc that has been made available across a network.

Local Users and Groups A Windows tool used to create and manage accounts for those who use the computer or computer resources from a remote network computer. These accounts are considered local users or local groups and are managed from the computer being worked on. In contrast, domain or global users and groups are administered by a network administrator on a network server.

`locate` A macOS command that searches for a file in a database of paths. Commonly used subsequently to `update`, which is a command used to update a local database on the system that contains the full pathname of each file.

locator application Software used to pinpoint where a mobile device can be found.

log off when not in use When not using a computer, configure the screen saver to appear after a period of non-use or lock the computer.

logical drive A division of an extended partition into separate units, which appear as separate drive letters.

logical operator Used in scripting to allow for two or more conditions to be tested in one statement. Examples of logical operators include `AND`, `NOT`, and `OR`.

logical partition A division of an extended partition. A logical partition can be assigned a drive letter, formatted, and used for storage.

login script A set of tasks that run when a user logs in when the device is part of a Windows domain.

logon script See *login script*.

LoJack (BIOS option) A BIOS setting option that controls locating the device, remotely locking the device, remotely deleting data, and displaying an "if lost" message.

long-range fixed wireless An internet connectivity option that is used in remote areas.

loop In scripting, a method of repeating something.

loop structure In a loop (or repetition) structure, a loop contains a block of statements that is executed repeatedly.

loopback plug A troubleshooting device that allows port testing.

lost cluster A sector on a disk that the file allocation table cannot associate with any file or directory.

low memory warning A notification from the operating system that a device is running out of RAM (Random Access Memory), especially when running multiple applications or demanding tasks.

low RF signal Caused by a wireless device being too far away from a wireless access point/router or obstructions such as walls.

low-level format A utility that formats a drive; note that this is different from the high-level format done on a newly installed drive or during an operating system installation.

LPCAMM (low-power compression attached memory module) A type of mobile device RAM that takes up less space and power, has faster speeds than SODIMMs, and can be removable.

`ls` A Linux command that lists the contents of a currently working directory.

LTE (Long Term Evolution) A version of 4G that optimized the network for video streaming and online games.

Lucent connector (LC) A type of fiber optic connector that snaps into a connector.

lumens A measure of light output or brightness; how much visible light is coming out of equipment such as lamps, lighting equipment, or projectors.

M

M.2 A type of connector that allows attachment of modules of varying size. First found in mobile devices and used for SSDs but now found on desktop motherboards.

MAC address (Media Access Control address) A unique 48-bit number address shown in hexadecimal assigned to a network adapter. The first half of the number shows the vendor and the second half is the unique number. Also known as a Layer 2 or physical address.

MAC address filtering A security feature on an access point that allows MAC addresses to be entered to limit the number of wireless devices allowed on the wireless network.

macOS A Unix-based operating system that was developed by Apple, Inc., for its Macintosh line of computers, called Mac for short. macOS is the second-most-commonly used desktop operating system behind Windows and is the most-used type of Unix/Linux-based desktop operating systems.

magnetometer Used to scan for firearms/weapons and might also be used for location tracking.

mail server Also known as an email server. Used to maintain a database of email accounts, store email that has been sent and received, and communicate with other mail servers.

maintain a positive attitude A great idea for professionalism and good rapport with customers.

maintenance counter Reset through the laser printer menu to count the number of pages until the message to apply the maintenance kit appears again.

maintenance kit A collection of items commonly used for technical support. Includes a portable vacuum, toner vacuum, compressed air, swaps, monitor wipes, lint-free cloths, general-purpose cloths, general-purpose cleanser, denatured alcohol, antistatic brush, optical drive cleaning kit, gold contact cleaner, safety goggles, and an air filter or mask.

maintenance window A time where planned IT changes occur.

malicious app An illegitimate piece of software that could install a virus, ransomware, be spyware and disrupt normal usage.

malware Software code designed to damage an electronic device (cause lockups, slowness, crash an app, cause the device to not run or boot, and more).

`man` A Linux command, short for *manual*, that can be used with another command to bring up an instruction manual for using the other command.

MAN (metropolitan area network) In a networking environment, a networks that spans a city or town.

man-in-the-middle (MITM) A security attack in which a hacker inserts a device between a sender and a receiver so that this device can receive the intended traffic. APs, DHCP servers, and default gateways (routers or Layer 3 devices) are common devices simulated.

managed switch A type of switched used in a corporate network that has an IP address assigned that can be remotely accessed, configured, and monitored by an administrator.

mATX See microATX.

Mb An abbreviation for megabit.

MB See *megabyte*.

MBR (master boot record) A program that reads the partition table to find the primary partition used to boot the system.

`md` A command issued from a command prompt that creates a directory (folder) or subdirectory.

MDM (mobile device management) The capability to view and manage multiple mobile devices.

MDR (Managed Detection and Response) A security platform used to protect computers, laptops, and servers and provide real-time 24/7 monitoring.

Media Center Can be used to turn a Windows computer into a home entertainment hub but is no longer supported.

megabyte Approximately 1 million bytes of data (exactly 1,048,576 bytes). Abbreviated MB.

memory The part of a computer that temporarily stores applications, user documents, and system operating information.

memory address A unique address for memory chips.

memory card reader A device that accepts varied types of memory cards so that data can be copied or read.

Memory Diagnostic Tool A tool accessed by booting from the Advanced Boot Options menu in Windows to thoroughly test RAM.

menu bar A component of the macOS GUI that is anchored to the top of a screen and is a dynamically changing bar that presents contextual drop-down menu options on the left side, depending on which window is active. On the right side, it provides shortcuts such as connecting to a WiFi network or changing volume. It is also informative, displaying information such as battery life on laptops and the time.

metered connection A type of internet connection that has a data limit imposed by the service provider.

metered service In cloud computing, a company pays an amount based on how much of the service is used on an hourly or monthly basis.

microATX A smaller version of a standard ATX-sized motherboard form factor.

microUSB A standard interface port on mobile devices and smartphones.

microphone An audio input device that can be integrated into a mobile device or that can be added externally, as with a wireless Bluetooth device; controlled with an app.

microprocessor See *processor*.

Microsoft Management Console Holds snap-ins or tools used to maintain the computer. Also known as the Computer Management console.

Microsoft Windows An operating system used on PCs, tablets, and laptops.

MIMO (multiple input/multiple output) Describes 802.11n wireless technology in which multiple antennas operate cooperatively to increase throughput on a wireless network.

miniPCIe A 52-pin expansion slot or card used in mobile devices.

mini-DIN A motherboard connector, sometimes called a PS/2 connector, that connects keyboards and mice.

mini-LED An electronic device used in various technologies including displays. See LED.

miniUSB A port found on mobile devices that is a miniaturized version of the Universal Serial Bus (USB) interface created for connecting smartphones, GPS devices, printers, and digital cameras.

missing drive in OS If the BIOS/UEFI recognizes the storage device, but the OS does not, use the Disk Management tool to initialize and/or partition the drive.

missing files A symptom of malware.

Mission Control A macOS utility that gives an overview for managing all application windows and virtual desktops.

`mkdir` A Linux (and Windows) command used to make a directory.

`mmc` (Microsoft Management Console) A Windows container for management tools. The one already built is known as the Computer Management console. Holds tools such as Device Manager, Disk Management, Local Users and Groups, Event Viewer, Task Scheduler, Performance, Shared Folders, and Services. `mmc` is also the command used from a command prompt to open the Microsoft Management Console.

MNDA (mutual non-disclosure agreement) A security situation where two parties sign a document that says information will not be shared by either party.

mobile digital key A method of allowing physical or digital access using the proximity of a mobile device like a smartphone, tablet, or wearable device. It could also be through an app.

mobile docking station A recharging station that provides a stable environment for mobile devices. Some mobile docking stations can charge more than one device at a time.

modem (modulator/demodulator) A device that connects a computer to a phone line or connects computers and mobile devices to broadband, wireless, WiFi, Bluetooth, or satellite networks.

modular power supply A type of power supply that allows the customization of the number and type of power connections plugged into the power supply.
Molex A type of power connector that extends from a computer's power supply to various devices.
monitor Displays information from the computer to the user.
motherboard The main circuit board of a computer. Also known as the mainboard, planar, or system board.
motherboard LED Motherboards sometimes have LEDs used in troubleshooting. Common ones include the CPU, boot or drive, VGA or video, and RAM or DRAM.
mount A Linux command used to adds new file system (a disk or another directory) to the system's directory tree, or displays currently mounted file systems
mount To make a drive available and recognizable to the operating system through the `diskpart` command utility.
mounting (Disk Management) An options that maps an empty folder on an NTFS volume by right-clicking on a partition or volume > *Change Drive Letter and Paths* > *Add* > *Mount in the Following Empty NTFS Folder* and either type the path or browse to an empty folder > *OK* > *OK*.
mouse A data input device that moves the cursor or selects menus and options.
mouse port A DIN connector on the motherboard that should accept only a mouse cable.
MOV (metal oxide varistor) An electronic component built in to some surge protectors to absorb overvoltage spikes or surges.
mSATA A connector type used for SSDs found on desktop motherboards, laptops, and mobile devices.
`msconfig` A system configuration utility command that allows an administrator to enable or disable services, access control panel links, and control applications.
MSDS (material safety data sheet) A safety-related document that contains information about a product, including its toxicity, storage, and disposal.
`msinfo32` A Windows command used to bring up the System Information window from a command prompt. The System Information window contains details about hardware and hardware configurations as well as software and software drivers.
`mstsc` A Windows command used to control and use a remote computer; brings up the Remote Desktop Connection utility.
MTBF (mean time between failures) The average number of hours before a device fails.
MU-MIMO (multi-user multiple input/multiple output) A wireless technology used with the 802.11ac that allows up to eight simultaneous streams from multiple devices.
multi-mode fiber A type of fiber-optic cabling that allows multiple light signals to be sent along the same cable.
multiboot system A computer system that has two or more bootable operating systems; only one operating system at a time can be run on the system.
multicore A term used to indicate multiple processor cores in the same housing.
multifactor authentication (MFA) Use of two or more factors to provide access. The factors can be something you possess, such as a card, current location, security token–provided code, PIN, fingerprint, facial recognition, palm print, or password.
multifunction device A device that can print, copy, scan, and sometimes act as a facsimile (fax) machine.
multipage misfeed A printer problem that requires checking the rollers through the paper path, crooked paper, or the alignment guides.
multipart paper Special paper designed to withstand the pressure of images struck upon it.
multiple print jobs pending Check for paper, ink/toner, and device error message. Repair the problem and clear the print job or restart the printing.
multisocket A feature on a motherboard that allows more than CPU to be installed.
multitenancy Multiple companies using the same resources located within a particular cloud computing vendor environment.
`mv` A Linux command that moves a file.
MX record (mail exchange record) A type of DNS record that forwards email to a server in another domain.

N

.NET Core Used for the cross-platform version of Windows PowerShell.
`nano` An easy-to-use Linux text editor.
NAS (network-attached storage) See *network-attached storage device*.
NAS drive A drive used in a network-attached storage device that costs more than a drive of the same capacity used in a PC, for example, because a NAS drive is built to run 24/7.

NAT (network address translation) A method of conserving public IP addresses. NAT uses private IP addresses that become translated to public IP addresses.

native resolution The number of pixels going across and down a flat panel monitor. This resolution is the specification for which the monitor was made and is the optimum resolution.

Nautilus The default file manager for the GNOME desktop in Linux systems.

NDA (non-disclosure agreement) A signed document that stipulates that information is not to be shared.

`net` From a prompt, the `net` command manages almost everything on a network. It is followed by other options, each of which has different parameters.

`net use` From a prompt, the `net use` command is used to map a network share to a drive letter or view mapped drives on a Microsoft-based machine.

`net user` From a prompt, the `net user` command is used to create, delete, or make changes to user accounts from a command prompt on a Microsoft-based machine.

NetBT (NetBIOS over TCP/IP) Uses TCP ports 137–139 to support outdated applications that rely on the NetBIOS API to use a TCP/IP-based network. Also known as NBT.

`netdom` From a prompt, a command that can manage workstations in a domain environment.

`netstat` A command that can view current network connections and the local routing table for a PC.

network Two or more devices that can communicate and share resources between them.

Network A macOS System Settings tool that provides settings for Ethernet, the macOS firewall, Thunderbolt, VPN and other network settings.

Network & internet A Windows Settings category that contains configuration options for wire and wireless networks.

Network and Sharing Center A Windows Control Panel utility used to check network status, configure network settings, and set preferences for sharing folders and other resources.

network boot Sometimes called a Preboot Execution Environment (PXE) boot, where the system boots from a server that deploys an operating system image to a computer.

network interface card See *NIC*.

network number The portion of an IP address that represents which network the computer is on.

network path An address that can be used from a command prompt or File Explorer that can be used to go to a shared resource such as a folder.

network port A port that connects a computer to a wired network.

network protocol A data communication language.

network share A folder or network device that has been shared and is accessible from a remote computer.

network tap Captures data from the network.

network topology diagram A type of IT documentation that shows how wired and wireless devices connect.

NFC (near field communication) A technology that connects nearby devices without a cord.

NFS (Network File System) An open standard protocol used for sharing files across a network.

NIC (network interface card) A port on a device that allows connectivity to a network. A NIC can connect to a wired or wireless network.

no Bluetooth connectivity An issue that could be helped by turning the device off and back on, check for interference, ensure that Bluetooth is enabled, and enter passkeys/PINs.

no connectivity An error condition that exists if the self-test issued from a computer fails.

no display With this problem on a mobile device, attach an external display if possible. If attached to a projector, check the output port chosen. Check the lid close detector. Turn the device off and back on. Charge the device fully.

no internet connectivity See no connectivity.

no OS found A situation where the operating system is corrupt, there is a problem with the boot device such as the hard drive, or the BIOS/UEFI settings are incorrect.

no power In this situation, check that power cord is attached, the power button pushed, the surge strip turned on, and the monitor is turned on; could be an indication of a faulty power supply. On a mobile device, check brightness, lid close sensor, and battery. Check for malware.

no wireless connectivity In this situation, check whether WiFi is enabled and ensure that the device is not in Airplane Mode. Turn off WiFi and turn it back on again. Move the device to see if you have a higher signal strength (display on a laptop). Ensure that the correct wireless network is chosen.

non-compliant system A machine that does not meet security policy requirements that could be a potential security threat.
non-ECC RAM A less expensive type of memory chip that does not perform error checking.
normal change A planned change management such as installing a new system or moving the data center.
`NOT` operator Flips the result of an expression so that if an expression is true, it will return false and vice versa; if the expression is false, it will return true.
Notepad An accessory text editor program in Windows.
notepad [command] Opens the Windows Notepad text editor app.
notification area (Windows) The far-right area of the taskbar, which contains information about an application or a tool, such as security, network access, speaker control, or date and time.
notifications Windows notifications can be controlled on a per app basis using the Notifications & actions link through Windows Settings.
`nslookup` A Windows troubleshooting command that displays network domain names and their associated IP addresses.
NPU (neural processing unit) A specialized processor found in computers that perform artificial intelligence tasks.
NTFS (New Technology File System) The file system used with Microsoft operating systems today (starting with Windows NT). Offers encryption, compression, larger file sizes, and longer filenames.
NTFS permissions A security measure that can dictate what a specific user or group can do with a file or folder.
NTLDR is missing A Windows boot error condition in which the operating system needs to be reinstalled.
NTP (Network Time Protocol) A protocol that synchronizes time between network devices.
NTP server Used to synchronize time across network devices.
NVMe (non-volatile memory express) A technology used with SSDs that provides fast performance when accessing NAND flash memory.

O

off site storage Backups kept at a remote location or in the cloud.
ohm A measurement of electrical resistance.
OLED (organic LED) Display screen technology used in many monitors, TV's, and mobile devices today. It does not require a backlight like LCDs but has a film of organic compounds placed in rows and columns that can emit light. It is lightweight and has a fast response time, low power usage, and a wide viewing angle.
omnidirectional antenna A type of antenna that has a radiation pattern in all directions.
on site storage Data and backups kept within the business.
on-path [attack] Threat actor collects and even changes data between a user and the device providing the service (such as a web server).
OneDrive Microsoft's cloud storage solution.
one-time password (OTP) Also known as one-time passcode that is sent via SMS text or email usually that can be used to authenticate access to a site or a transaction.
ONT (Optical Network Terminal) Converts light signals from a fiber connection into electrical for a copper connection.
open source Software that allow vendors to use the core source code and the ability to customize the software, such as, Google Android or Linux.
open-ended question A soft skills technique that results in more information about a problem than questions that have just yes or no answers.
operating system (OS) A piece of software that provides the interface between the user and the various components of the computer (the physical hardware and the digital applications); makes the computer operational.
optical cable See fiber cable.
optical disc (boot option) A boot method that uses a CD, DVD, or Blu-ray disc that has an operating system on it.
optical drive A storage device that accepts optical discs such as CDs, DVDs, or BDs that have data, music, video, or software applications.
Optimize and Defragment A Windows tool accessed with the Defragment button or through the defrag command. It is used to put files in contiguous clusters on the hard drive for better performance.
`OR` operator Returns false if and only if both sides of the expression are false.
order of volatility Preserving the most volatile data first such as what is in RAM, what apps are running, or what websites have been recently visited, etc.

organizational unit (OU) A way to group users, groups, accounts or even other OUs in order to subdivide administrative duties.

orientation The way in which a document or screen is presented: portrait versus landscape.

OS See *operating system*.

OS fails to update [mobile] Be sure device is powered and connected to WiFi or wired network. Free up space. Ensure device is still supported. Turn off Bluetooth. Reset the device, clear cache and storage space. Restart the device or perform a factory reset.

OS not found An issue when the boot order in the BIOS/UEFI is incorrect, the hard drive does not contain an operating system, or there is an issue with the drive that contains the operating system being recognized by the computer.

OS update [mobile] OS updates and upgrades are important on mobile devices and the device should be connected to power if possible during an update.

OS X An older Apple operating system family replaced by macOS.

OSHA (Occupational Safety and Health Administration) A division of the U.S. Department of Labor that promotes safe and healthy working conditions by enforcing standards and providing workplace safety training.

OSI model (Open Systems Interconnect model) A standard for information transfer across a network that was developed by the International Standards Organization. The model has seven layers; each layer uses the layer below it, and each layer provides some function to the one above it.

output In programming or scripting, the result, which could be a screen, a value, a computation, a printed document, and so on.

overclocking Manually changing the front side bus speed and/or multiplier to increase CPU and system speed, but at a cost of increasing the CPU operating temperature. Overclocking a CPU may void the manufacturer's warranty.

overheating On a mobile device, power off the device and let it cool. See if you can determine if a specific spot is getting hotter than other places. Check the battery and replace it, if necessary.

overvoltage A condition when the AC voltage is over the rated amount of voltage.

P

`.pkg` An application packages that contain the software, folders and other files required to install an application, usually in macOS.

`.ps1` A file extension used for a PowerShell script.

`.py` A file extension used with Python scripts.

PaaS (Platform as a Service) A type of cloud service that describes servers, databases, operating system, storage, and development tools provided in an outside environment to relieve the support burden on companies that need an environment to perform high-level programming and develop applications.

paging file A temporary file in hard disk space used by Windows that varies in size depending on the amount of RAM installed, available hard drive space, and the amount of memory needed to run the application. Also known as a swap file.

palm print scanner A biometric security device that is more secure than a fingerprint reader and scans the hand and possibly provide vein analysis.

PAN (personal area network) A network of personal devices such as cell phones, laptop computers, and other mobile devices that can communicate in close proximity through a wired network or wirelessly. A Bluetooth wireless keyboard and mouse form a PAN.

Panel A part of a Linux GUI and similar to macOS, Panel is a menu bar at the top of the screen containing contextual information on the left side with static information on the right side.

paper jam A problem that occurs when paper gets stuck along the printer paper pathway.

paper not feeding A problem that may be due to poor paper quality or to the inefficiency of the rubber rollers that move the paper.

partition A process that can divide a hard drive so that the computer sees more than one drive.

`passwd` A Linux/Unix command to set or change a user password.

password manager Software that could potentially fill in web forms and manages passwords for various websites.

password policy A policy that may be contained within the security policy that defines password requirements (length and types of characters) as well as the password change process.

password security The act of being conscientious about where passwords are written and stored.
passwordless An option like Windows Hello that allows you alternatives to gaining access such as using a face, fingerprint, pin, security key, or picture.
Passwords [BIOS] A BIOS/UEFI settings that provide protection of the BIOS menu option by configuring one or more passwords to access the Setup program.
patch A piece of software that fixes a specific problem in an application or operating system.
patch panel Used with twisted pair cable as a central location to which network cables terminate. It mounts in a network wiring rack, has network ports on the front, and has wiring connected to the back to provide network connectivity.
patch/update management A security best practice in which the operating system, drivers, and BIOS/UEFI are kept up to date so that known security issues are addressed.
patching/OS updates A security best practice for mobile devices in which the operating system (OS) and radio firmware for devices such as cell phones are updated.
path A reference that tells where a file is located among drives and folders (directories).
PATH variable Used in programming and scripting to tell a program where to find the files that it may need.
pathping A command that provides output similar to the ping and tracert commands and includes network latency and loss information between source and destination IP addresses.
PC (personal computer) A common name for a computer, derived from the IBM PC brand.
PCI (Payment Card Industry) A generic term for the entities surrounding business using payment cards, such as debit and credit cards, for transactions.
PCI (payment card information) A type of regulated data related to a credit card, debit card, and the finance industry.
PCI (Peripheral Component Interconnect) An older 32-bit and 64-bit, 66 MHz local bus standard found in computers.
PCIe A point-to-point serial bus used for motherboard adapters. Each bit can travel over a lane, and each lane allows transfers up to 250 MB/s, with a maximum of 32 lanes (which gives a total of an 8 GB/s transfer rate).
PCL (Printer Control Language) Uses printer hardware to do the translation between the printer and the computer.
PD (Power Delivery) A USB standard that allows up to 20 V at 5 A for 100 watts of power. The standard has five levels of power: 10 W, 18 W, 36 W, 60 W, and 100 W.
PDL (Page Description Language) Something unique to a printer that allows communication between the computer and printer and it handles the overall page look of a document.
peer review A part of change management where stakeholders are allowed to provide input to a proposed change.
performance (virtual memory) A computer's performance is affected by the virtual memory settings, which allocate a specific amount of hard drive space that can be used when more applications and data are loaded than the amount of RAM installed.
Performance Monitor A Windows tool that monitors resources such as memory and CPU usage and that allows creation of graphs, bar charts, and text reports.
Performance utility A utility that monitors memory and other hardware parameters usage aspects.
Personalization A Windows Settings category that contains configuration options for the appearance and behavior of the graphical user interface.
PHI (protected health information) The Health Insurance Portability and Accountability Act (HIPAA) developed a U.S. government standard to protect certain types of private health-related information.
phishing (pronounced "fishing") A type of social engineering that attempts to get personal information through email from a company that appears legitimate. Targets obtaining ATM/debit or credit card numbers and PINs, Social Security numbers, bank account numbers, an internet banking login ID and password, an email address, security information such as a mother's maiden name, full name, home address, or phone number.
phone filter A part used with DSL internet connectivity that must be attached to every phone outlet. The traditional analog device connects to this part. The filter allows the DSL signal to be separated from the normal analog traffic.
phone skills An important skill set for technicians when talking to users and supporting them over the phone.

physical address See Mac address.

physical cabling issue [projector] Check all physical connections on both ends if a projector cannot output from a particular source.

physically damaged port Closely inspect a mobile device port if the device will not charge after changing the cable.

PII (personally identifiable information) Any personal data or method of identifying, locating, or contacting a particular person.

PIN (personal identification number) A unique identifier used to access an account or a device such as a mobile tablet.

PIN code A security option commonly available on mobile devices.

`ping` A network troubleshooting command used to test TCP/IP communications and determine whether a network path is available, whether any delays exist along the path, and whether a remote network device is reachable. Use `ping` with the private IP address 127.0.0.1 (IPv4) or ::1 (IPv6) to test a NIC's basic network setup.

pinwheel A spinning wheel, often seen in macOS, generated by the operating system to indicate possible problems such as a nonresponsive application.

pipe symbol A character (|) used at the command prompt that allows control of where or how the output of the command is processed. For example, a command can be "piped" to display only one screen at a time.

piracy The act of copying or distributing copyrighted software.

pixel density The number of pixels per inch (ppi) or pixels per centimeter (ppcm) on a display. The higher the number, the better the quality is.

pixel pitch The distance from the center of one pixel to the center of the adjacent pixel in millimeters. The smaller the pitch, the more pixels there are and the better the quality.

plenum-rated cable A type of cable that is treated with fire-retardant materials so that it is less of a fire risk.

PoE (Power over Ethernet) A method of powering a remote device through an Ethernet switch or a patch panel.

PoE injector A method of providing power to a remote device using an injector when a PoE switch or patch panel is not available.

PoE switch A switch that has the ability to provide power to devices such as access points or IP phones through the Power over Ethernet standard.

policy enforcement In a corporate environment, software and measures are used to ensure the rules of access control, acceptable use of data and company information, remote access, backup, and security are followed.

poor battery health Close any apps and services that are not being used and replace the battery.

poor VoIP quality Results in dropped calls or unintelligible audio that is solved by implementing QoS. Key measurements are latency and jitter.

poor wireless connectivity See intermittent wireless.

POP3 (Post Office Protocol) A protocol used to retrieve email from a mail server. Uses port 110.

pop-up A small window that appears (pops up) to display a message, warning, or advice. Pop-ups often are a nuisance but can be managed through the browser's pop-up blocker feature.

port A connector located on the motherboard or on a separate adapter.

port flapping A port that is continuously going up and down.

port forwarding The process of sending data through a firewall, based on a particular port number or protocol.

port mapping The combination of one public address and a port number that represents one internal company host; also called port address translation (PAT).

port replicator A part that is similar to a docking station that attaches to a laptop computer and allows more devices, such as a monitor, keyboard, and mouse, to be connected.

port security A security feature on a corporate switch that detects whether someone has swapped one corporate device for another one.

port security [firewall] An advanced setting that can allow inbound or outbound traffic based on a specific TCP or UDP port number.

POSIX (Portable Operating System Interface) A designation that meets the specifications of a standardized operating system outlined by the IEEE Computer Society, containing a Bourne shell and other standard programs and services that are found in all POSIX-compliant operating systems. macOS is POSIX compliant.

POST (power-on self-test) Startup software contained in the BIOS/UEFI that tests individual hardware components.

POST beep An indication that a hardware error exists, such as an error in the CPU, motherboard, RAM, power supply, or a stuck key. Look up the code for more information. The number and type of beeps is UEFI/BIOS vendor specific.

POST card A PCI/PCIe adapter or a USB attached card that performs hardware diagnostics and displays the results as a series of codes on an LED display or in LED lights.

PostScript A popular page description language from Adobe Systems Inc.

potentially unwanted program (PUP) A type of software usually installed by adware, but it could be from any malicious website or link.

power A measurement, expressed in watts, that represents how much work is being done.

Power Options A Windows Control Panel utility used to configure power saving modes.

power rating A measurement, expressed in watts per channel, that represents how loud the speaker volume can go without distorting the sound.

PowerShell A Windows technology that helps technicians and network administrators automate support functions through the use of scripts and snippets.

power supply A device that converts AC voltage into DC voltage that the computer can use to power all internal and some external devices.

power supply tester A tool that checks DC voltages sourced from the power supply.

power surge An overvoltage condition that is like a spike but has a longer duration.

prefix notation A method used to describe a subnet mask. It includes a forward slash followed by a number, such as /24. The number is how many consecutive bits are set in the subnet mask.

preventive maintenance Something that is done to prolong the life of a device.

primary partition The first detected drive partition on a hard drive that has been configured with a basic disk.

principle of least privilege A security measure in which a user receives only enough security permissions (on devices, files, network resources, and so on) to do his or her job.

print driver A piece of software that coordinates between the operating system and the printer.

Print Management A Windows administrative tool used to manage printers. Use the Print Management administrative tool from the System and Security Control Panel or use the printmanagement.msc command.

print ribbon A ribbon that is struck by the printhead to leave images on paper in an impact printer.

print server A device (a computer or a separate device) that connects to a printer used by multiple people through a network.

print spooler Also known as a print manager, a software program that intercepts a request to print and sends print information to the hard drive, from which it is then sent to the printer whenever the processor is not busy with other tasks. A print spooler allows multiple print jobs to be queued inside the computer so that other work can be performed.

printer A peripheral used to output text and/or graphics onto paper.

printer firmware Software that can be updated to fix software/app problems, increase security, or update features.

printer sharing Commonly used in a home or small business environment to allow multiple users on the same printer. Contrast with a printer server, used in corporate environments.

Printers & scanners A Windows Settings tool used to view and manage scanners, printers, and print jobs.

Printers & Scanners A macOS System Settings tool that provides settings for adding and removing printers and scanning devices.

printhead The part of the impact printer that holds the print wires and impacts the ribbon.

printing issue A problem when trying to send output to the printer. In Windows, try to print a test page from the printer's *Properties* > *General* tab. Use the Windows Troubleshooting tool.

Privacy & security A Windows Settings category with options for configuring antivirus, firewall, and device tracking settings. Also used to configure Windows permissions and app permissions.

Privacy & Security A macOS System Settings tool that controls which apps can access the user's data, location, camera and microphone. Also manages other safety protections, such as FileVault, which automatically encrypts the contents of a disk.

private AI A corporate use of AI that typically has a focus on data security, controlled data sources, and more control over data privacy than a public AI app.
private browsing Used so that browsing history, cookies, or data collected is not kept.
private cloud Part of a company's network infrastructure located outside the business in a remote location, but the company has responsibility for managing the software and hardware.
private IP address An IP address used inside a home or business that is not allowed to be transmitted across the internet. Contrast to a public IP address.
private network A home or corporate network where the networks use private IP addresses that are not allowed to be routed on the internet, but are translated at the network border into public addresses using a process called NAT.
privileged access management (PAM) An approach to security that uses a combination of technology and processes to define who gains access to resources and provides systems for monitor and control.
proactive A good trait to have as a technician by implementing measure to avoid problems rather than just wait for a problem to occur before implementing the measure.
processing [scripting] One of the three parts of a program (input, processing, and output) and it is the work or task performed.
processor The central 32-bit or 64-bit electronic chip that determines the processing power of a computer. Also known as a microprocessor or central processing unit (CPU).
procurement life cycle The company processes that are performed in order to obtain something.
Program Compatibility Wizard A program that can check for software application compatibility with a newer Windows version.
Programs and Features A Windows Control Panel utility used to uninstall and change programs, as well as enable/disable Windows features such as games, Telnet server, Telnet client, TFTP client, and print services.
project confidence A skill needed in IT personnel.
projector A device that takes input from a device such as a computer, laptop, camera, and so on and sends that image to a screen or wall.
`prompt` A command that changes how the command prompt appears. See also *command prompt*.
proprietary crash screen An error condition on a particular computer or application that is unique to the manufacturer.
proprietary system A type of computer that only allows a particular operating system or has hardware that is incompatible with other vendors. macOS is used only on Apple devices and is a proprietary system.
proxy server A server that acts as a go-between for an application and another server.
`ps` A Linux/Unix command that lists all current processes.
PS/2 port Common name for keyboard and mouse connectors, which are examples of miniDIN-6 connectors.
public AI An app that can be used by the general public that has pre-set training models and datasets. Contrast with private AI.
public cloud A service or an environment operated by an external vendor to provide a service or an application to a company.
public IP address A private IP address that a service provider or company translates to a public IP address that is seen on the internet.
punchdown block A part of the network or phone cabling system that allows a wire to be attached and firmly secured into the block using a punchdown tool.
punchdown tool An implement that terminates cable on a patch panel.
purpose of the change In change management, the part of the planning process that documents why a change is needed.
PVC (polyvinyl chloride) Cable that has a plastic insulation or jacket that is cheaper and easier to install than plenum cable. It can have flame-retardant added.
`pwd` In the Linux environment, a command that identifies the current working path you are in.
PXE (Preboot Execution Environment) boot An option some computers have that can be modified to search for the network device that holds the computer image.
Python A good language for writing scripts because it is easy to learn and Python scripts can be run on most operating systems. The extension.py is used with Python files.

Q

QoS (quality of service) A collection of techniques that ensure that the most important corporate data, voice, and/or video is sent before other noncritical data that may get dropped as a result.

quad-channel A memory type in which a motherboard can access four memory modules simultaneously.
quick format During an installation process, a function used to prepare a hard drive partition but not identify and mark bad sectors so that they will not be used for data storage. A full format, in contrast, does evaluate the drive for bad sectors but takes quite a bit longer to prepare the partition for use.
QR code phishing Information within leads to a malicious website in an attempt to get personal or corporate information.

R

radio A wireless input/output technology that has a longer range than infrared.
RADIUS (Remote Authentication Dial-in User Service) A secure method of authentication using a server.
RAID (redundant array of independent [or inexpensive] disks) Allows writing to multiple hard drives for larger storage areas, better performance, and fault tolerance.
RAID 0 Also called disk striping without parity, a type of RAID that enables data to be alternatively written on two or more hard drives but be seen by the system as one logical drive. RAID level 0 does not protect data if a hard drive fails; it increases only system performance.
RAID 1 Also called disk mirroring or disk duplexing, a type of RAID that protects against hard drive failure. See also *disk mirroring* and *disk duplexing*. Requires two drives at a minimum.
RAID 10 A RAID condition in which a mirrored set and a striped set are combined. Takes four hard drives as a minimum.
RAID 5 Describes putting data on three or more hard drives, with one of the three drives used for parity. See also *RAID*.
RAID 6 Uses an additional drive for parity than RAID 5 so that two failed drives can be recovered. See also *RAID 5*.
RAID failure An error condition that requires using the Windows Disk Management tool to verify the status of the drives used in the RAID.
RAID not found An error condition that sometimes occurs with a power failure or surge, misconfiguration in BIOS/UEFI, system upgrade, application upgrade, or new application installation.
RAM (random-access memory) A volatile type of memory that loses its data when power to the computer is shut off.
RAM limitation The maximum amount of memory that an operating system can recognize. Even if a system has more installed, the operating system will not be able to use that extra memory.
random reboot Could be caused by overheating, a power issue, a particular app, or the OS.
random shutdowns A symptom of an issue with the processor, motherboard, or power supply.
ransomware A security situation in which a hacker has restricted access to a device until the user is pressured to pay money to regain access.
RAW volume A part of a hard drive that has been set aside as a volume but has never been high-level formatted and does not contain a specific type of file system.
RCA A type of connector used with coaxial cable.
rd A Windows command used to remove a directory (folder).
RDP (Remote Desktop Protocol) A Microsoft protocol used for accessing and controlling networked computers and mobile devices. RDP uses port 3389.
read/write failure An error condition that indicates a hard drive has a defective area.
ReadyBoost A utility that can speed up the Windows boot process by caching some startup files to a 256 MB+ flash drive, SD card, or CF card.
reboot A restart of an operating system, also known as a warm start.
rebuild a Windows profile If a message appears that the user profile cannot be loaded, make a copy of the user profile folder, rename the registry key, and have the user log in again.
recovery disc A disc used to boot a system when you don't have an original operating system disc and then restore the computer from a previously saved system image. Sometimes called a system repair disc.
recovery partition An optional partition provided by some vendors that contains the operating system, files, and applications installed on the system when purchased.
Recycle Bin A location in Windows-based operating systems in which user-deleted files and folders are held. This data is not discarded from the computer. The user must empty the Recycle Bin to erase the data completely.

redundant power supply A device that has two or more power supplies that provide power if one power supply fails.

refresh (installation method) A Windows 8/8.1 tool that reinstalls the operating system but keeps user data and settings. Windows 10 uses Reset This PC for this purpose.

refresh rate Measured in hertz (Hz) or milliseconds (ms), the amount of time it takes a screen to be drawn in one second. In LCDs, it is also called temporal resolution. LCD refresh rates are traditionally 60 Hz.

Refresh Your PC A Windows 8/8.1 tool that reinstalls the operating system but keeps user data and settings. Windows 10 uses Reset This PC for this purpose.

ReFS (Resilient File System) A Microsoft file system used with Windows server that has proactive data corruption and support for larger drive capacities.

`regedit` A Windows utility that can modify and back up the registry.

`regedt32` One of two Windows registry editors. See also *registry* and `regedit`.

region code A setting on a DVD or Blu-ray drive or disc that specifies a geographic region. The drive's region code must match the disc's region code.

registry A central Windows database file that holds hardware and software configuration information.

`regsvr32.exe` A command used to register `.dll` files in the Windows registry.

regulatory and compliance policy A policy that is specific to an industry such as health care or manufacturing.

reimage A process of putting a new image (operating system, applications, and settings) on a corporate computer.

relational operator An operator that compares one side of an expression to another and is used in scripts.

Reliability Monitor A tool that provides a visual graph in Windows Vista or 7 of how stable the system is and shows details on events that might have affected system reliability.

reload OS A repair option that installs a new copy of the operating system when other repair options haven't been successful in fixing the problem.

Remote Assistance A Windows tool used to remotely access a Windows device. The remote computer displays a prompt requesting permission for remote access. Contrast with Remote Desktop, which does not request permission.

remote backup An option on a mobile device to allow the device or specific data like personal contacts, videos, pictures, and/or music to be backed up to remote storage.

Remote Desktop Connection A Windows tool used to remotely access a Windows-based device that does not require someone to be at that computer and does not prompt for permission. Contrast with Remote Assistance, which does prompt for permission.

Remote Desktop Services Previously known as Terminal Services, software on a server that can be used to deploy images to computers and to access, control, and manage remote computers and servers.

Remote Disc A feature that allows the use of a Mac computer's optical drive (even from a Windows computer).

remote network installation Pulling an image from a server or network share in order to load an operating system.

Remote Settings (link) A link used from the *System* Control Panel utility to configure Remote Desktop and Remote Assistance.

remote wipe The process of using software to send a command to a mobile device to delete data, perform a factory reset, remove everything from the device so that it cannot be used, and overwrite data storage to prevent forensic data recovery.

remove debris A maintenance process task for a thermal printer.

repair an application Select the application in the *Windows Programs and Features* section of the Control Panel and select *Repair*.

repair installation Used when you have to reload the Windows operating system. Sometimes called an in-place upgrade or a reinstallation.

repeater A network device that boosts the network signal. Network switches are repeaters. Wireless repeaters boost the wireless signal to extend the wireless network.

repetition In a repetition (or loop) structure, a loop contains a block of statements that is executed repeatedly.

repetition structure In scripting, this is a block of statements that are used repeatedly.

replace ink cartridge A maintenance or repair process for an inkjet printer.

replace paper [impact] A maintenance process where paper is inserted into the paper tray, threaded into the printer, or threaded onto a sheet feeder for fan-fold paper.
replace paper [thermal] Ensure the proper size and type of thermal paper is used and thread the paper through the rollers as directed by the manual or an image on/inside the printer.
replace printhead [impact] A maintenance process where the part that holds all the pins used to press against the ribbon is replaced.
replace ribbon A maintenance or repair process for an impact printer.
replace toner cartridge A maintenance or repair process for a laser printer.
Reset This PC A recovery option that reinstalls Windows and deletes users' files, apps, and settings.
resin An alternative to 3-D filament printing that produces better quality objects.
resistance A measurement, in ohms, of how much opposition is applied to an electrical circuit.
resolution The number of pixels shown on a monitor or the output of a printer.
Resource Monitor A Windows graphic tool that shows performance for the main system components.
restart service In Windows, use the *Services* Computer Management tool to restart a service that has stopped responding.
restore (installation method) A Windows installation method that takes the operating system back to a previous point in time.
restore point A snapshot image of the registry and some of the dynamic system files that have been saved previously by the System Restore utility. This is used when a Windows computer has a problem.
restrict login time A security measure where user or group accounts can be restricted to specific days and times through their Windows account management.
retinal scanner A biometric security device that scans the eye for authentication and access.
RFI (radio frequency interference) A specific type of EMI noise that occurs in the radio frequency range. Often results from operation of nearby electrical appliances or devices.
RFID (radio frequency identification) A technology that allows automatic identification of people, objects, or animals.
rights Permissions granted or denied to files, folders, and network resources.
risk analysis A part of change management in which the risks of the proposed changes are weighed against the company benefits.
risk level A rating such as low, medium, or high or a numerical value representing the level of risk an IT change brings if implemented.
RJ11 A type of connector used with analog modems and traditional phone jacks.
RJ45 A type of connector used on Ethernet network cards and ports. Used to connect a device to the wired network.
`rm` Short for remove, a Linux command that deletes a file or directory.
RMM (remote monitoring and management) A networking tool used to share a screen with a user or remotely access a computer to troubleshoot a specific problem, share files, remote image, update apps or OS, inventory control, and deploy security solutions.
`robocopy` A command used to copy files. It has more parameters than `COPY` or `XCOPY`.
rogue antivirus A downloaded application that appears to help someone with a problem, but that is, in reality, a virus.
roll back device driver Use *Device Manager* and right-click on a particular piece of hardware > *Properties* > *Driver* tab > *Roll Back Driver* button to take a device driver back to a previous version.
roll back Windows update If a Windows update causes a system to have issues, roll back the update to at least one previous version and then apply the updates one at a time.
rollback plan A documented business process that outlines what to do and when to do when an IT change isn't going as planned.
roller A printer part that is part of the system used to move paper through a printer.
root In Unix/Linux, the administrator account. The root user has absolute power on a system, including within macOS.
root directory The starting place for all files on a disk. A hard drive is limited to 512 entries. The designation for a hard drive's root directory is `C:\`.
router A network device that determines the best path to send a packet. Works at OSI model Layer 3.
run as administrator A higher level of security access that may be needed to execute specific commands from the command prompt or have access to administrative tools or utilities.

S

/System A macOS system folder contains the actual macOS operating system.

`.sh` An extension used with a shell script or a text file that has a sequence of commands for a Unix-based system.

S/PDIF (Sony/Phillips Digital Interface Format) Defines how audio signals are carried between audio devices and stereo components. It can also be used to connect the output of a DVD player in a PC to a home theater or some other external device.

S-video port A composite video port, coded yellow, that uses a 7-pin mini-DIN connector.

SaaS (Software as a Service) A type of cloud service that describes hosted applications such as a learning management system, enterprise resource planning (ERP), human resources management (HRM), payroll, antivirus, and inventory management that are hosted by another company and accessible from anywhere.

Safe boot A Windows System Configuration option found on the Boot tab.

safe mode (Mac) A way to start a Mac so that the startup disk is checked and repaired if possible. Hold down Í while starting the computer.

Safe Mode (Windows) A Windows option used when the computer stalls, slows down, does not work properly, or has improper video settings or intermittent errors or when a new hardware/software installation causes problems. In Safe Mode, Windows starts with minimum device drivers and services.

safety goggles A personal protection device that should be worn when working on equipment to protect the eyes from debris, chemicals, and liquids.

SAN (storage area network) A collection of storage media that is centrally managed and available to a multitude of network devices, such as servers, network-based applications, virtual machines, and users.

sandbox A method of using virtualization or non-production equipment to test code or app changes before deployment.

sandbox testing Implementing a proposed change in a non-production environment.

SAS (Serial Attached SCSI) SAS devices connect in a point-to-point bus. Used in the enterprise environment in which high reliability and high mean time between failures is important.

SATA (Serial ATA) A point-to-point architecture for IDE devices that provides faster access for attached devices.

SATA cable A cable used to connect one SATA device to a motherboard SATA port.

SATA connector A motherboard connector used to attach a cable between the motherboard and a SATA device. This connector can also be used to connect an adapter that contains one or more additional external SATA ports.

satellite modem A type of modem that can provide internet access at speeds faster than an analog modem but slower than cable or DSL access.

scope of the change As part of the change management planning phase, an IT change plan should include the scope of the project.

screen lock A feature on a mobile device that requires something (a PIN, fingerprint, facial features, security pattern, voice, and so on) to access the device and unlock the screen of the device.

screen resolution The number of pixels on the screen such as 1920 x 1080 (1920 pixels in each row with 1080 rows).

screen sharing A macOS feature that allows one user to view and even control the display of another Apple computer that is on the network.

screened subnet See DMZ.

scribe A plastic tool that helps with prying plastic parts or covers off laptop and mobile devices.

script A small program written in one of several scripting languages that is designed to do a specific task.

SD (Secure Digital) A storage device with non-volatile flash memory used for mobile devices.

SDS (safety data sheet) A document that describes a product, including its toxicity, storage, and disposal procedures. Also contains information regarding health or safety concerns.

secure boot A BIOS/UEFI setting option that prevents unauthorized software from loading during the boot process.

secure connection Websites that use HTTPS and security certificates through a browser.

secure DNS A security measure that encrypts DNS requests in an effort to thwart DNS attacks.

secure management access Configuring a network devices such as an AP or wireless router for SSH for remote connectivity and having a non-default password.

Secure Sockets Layer See *SSL*.
secured print An option available on some printers that requires a passcode in order to send/retrieve a print job.
security certificate verification A way of verifying that the address in the certificate matches the web address and is digitally signed by a "trusted" authority.
security group An Active Directory type that allows applying group policy settings or permissions to any shared resource.
security pattern A security option that requires tracing a specific set of dots to access a mobile device.
security policy One or more documents that provide rules and guidelines related to computer and network security.
security threat An operating system that is no longer supported by a vendor can present a problem in that it becomes a risk to the business due to lack of security updates.
selection A selection (or decision) structure consists of a test condition together with one or more groups (or blocks) of statements. The result of the test condition determines which block of statements will be executed.
self-grounding The act of placing a part of your body in contact with an electronic device to prevent an electrostatic discharge (ESD) event.
sequence One of the three basic programming constructs. It means that code executes one instruction at a time, in the sequence the code is written.
Serial ATA See *SATA*.
serial cable A type of cable that connects to an RS-232 or DB9 port.
server-based network A basic type of LAN in which users log in to a controlling computer, called a server, that knows who is authorized to connect to the LAN and what resources the user is authorized to access. Usually found in businesses that have 10 or more computers.
service A Windows process that provides a specific function to the computer.
service fails to start In this situation, use the *Services* Computer Management tool to investigate and possibly manually start the service.
service pack A group of upgrades or patches provided by Microsoft for an operating system.
service release Software available from a manufacturer to fix a known problem (bug) in its applications program.
Services A tool that can be accessed through Windows Computer Management console or by typing `services.msc` from a command prompt. You can also control it from System Configuration utility > Services tab.
`services.msc` A command that brings up the *Services* snap-in Computer Management tool so that you can start and stop services.
session layer Layer 5 of the OSI model, which manages communication and administrative functions between two network devices.
Setup Software that tells a computer about itself and the hardware it supports, such as the amount of RAM memory, type of hard drive installed, current date and time, and so on.
setup location Ensure an appropriate place is identified for installing a new printer.
`sfc` A command used to start the System File Checker utility, which verifies operating system files.
Shadow Copy A Windows technology used with the System Restore program that uses a block-level image instead of monitoring certain files for file changes.
share A folder that has been set so that others can use it. This can be on a computer, printer, or network resource such as a scanner.
share permissions A security measure that can dictate what a specific user or group can do with a file or folder that can be accessed across a network.
Shared Folders A Windows tool used to view shares, sessions, and open files.
shared resources In cloud computing, resources such as servers, applications, hardware such as CPUs and RAM, data storage, and network infrastructure equipment shared among people within an organization or between organizations.
shell A standardized user interface to interact with the operating system.
shell script A text file that contains a sequence of commands for a Linux/Unix-based system. Shell scripts may not run correctly on a Windows system. A shell script file extension is .sh.
shielded twisted pair (STP) See *STP*.
shortcut An icon with a bent arrow in the lower-left corner. It is a link to a file, a folder, or a program on a disk. If the file is a document, it opens the application used to create the document.
shoulder surfing Someone behind you looking at what you type or what is on the screen to glean unauthorized information.

shredding A method of destroying documents for security reasons.

shrink (partition) The act of making a hard drive section smaller. In the *Disk Management* tool, right-click the drive letter > *Shrink Volume*.

`shutdown` A Linux/Unix and Windows command to shut down or restart the system, depending on the options used.

SIM (subscriber identification module) A small card in mobile devices and phones that stores personal contacts, numbers, and phone services.

simple volume A Windows term for the storage unit that contains the files needed to load the operating system. The system volume and the boot volume can be the same unit.

single-core processor A processor that has only one core CPU.

single-mode fiber A type of fiber-optic cabling that sends one light beam down the cable.

single rank A memory module that has only one set of DRAM chips. Contrast with dual rank that has two.

single sign-on An authentication technique that allows a user to authenticate to multiple systems, servers, printers, and other network devices with a minimum of a user ID and password.

site survey Used in wireless network design to determine the best wireless hardware placement for the optimum coverage area.

sizing issue With displays if the icons/words appear oversized or too little, adjust the display settings (resolution or size of text).

SLA (service-level agreement) An agreement with an external/third-party provider for a specific level of up time. It can also define internal wired and wireless network performance expectations.

sleep-and-charge USB port A computer port that provides power to an attached device (power to charge the device) even when the computer is powered off.

SLI (Scalable Link Interface) A technology used with video cards that allows two cards to work together.

slow boot A situation that could be caused by the operating system, startup applications, services, or too many startup login scripts.

slow network speed The results of network latency, the time measured to transmit data from source to destination. For wireless networks, this is caused by obstructions such as objects, walls, weather, microwave, ovens, and devices/other wireless networks operating in the same unlicensed frequency range. For wired networks, it typically is poor or faulty cabling or security issues

slow performance An indication that a computer system is operating in a less-than-efficient manner. Could be caused by lack of hard drive space, not enough memory, a poorly performing application, malware, or insufficient CPU cores/speed. For mobile devices, check battery power level, close apps that aren't being used, close services that aren't being used, connect to a Wi-Fi network, and move closer to the AP.

slow profile load The company may make use of local or domain policies including user and group profiles. Too many profiles that are required at startup slows the startup/login process.

sluggish performance See slow performance.

S.M.A.R.T. (Self-Monitoring, Analysis, and Reporting Technology) A feature that allows a storage device to send messages about possible failures or data loss. Configuration setting located in the BIOS/UEFI.

smart card A small ID-size card that can store data, be encrypted, and swiped through and/or interact wirelessly with a smart card reader. Examples of smart cards are identification, medical, credit, and access card.

SMB (Server Message Block) A means of providing access to shared network devices and files. SMB uses port 445.

smishing Text (SMS) messages used to tempt people into revealing information or contain a malicious link.

SMS (short message service) A text message that provides a security code used in authentication.

SMTP (Simple Mail Transfer Protocol) A standard used for email or for transferring messages across a network from one device to another. SMTP uses port 25.

snapshot In a virtualization environment, a copy or backup of the virtual machine (VM) at a particular point in time that is used to revert the VM to that point in time. It is similar in concept to a restore point.

SNMP (Simple Network Management Protocol) A standard that supports network monitoring and management. SNMP uses ports 161/162.

SoC (system on a chip) A single chip that contains everything needed to run such as a CPU, RAM, graphics, processor, ports, etc.

social engineering A technique used to trick people into divulging information, including their own personal information or corporate knowledge.
SODIMM (small outline DIMM) A special small DIMM used in laptops and printers.
SOP (standard operating procedure) A documented set of instructions on how to do a specific task.
soft reset Simply restarting a device. Contrast this to a hard reset, which is also called a factory reset.
soft token A security technique in which a code is delivered via text, phone call, or email, and this code is required in addition to the user ID and password.
software An application or operating system consisting of a set of instructions that makes the hardware work.
software firewall A software application or tool provided with a computer or device like an access point that can be configured to permit or block specific types of traffic.
software incompatibility When a new application might not work with an older operating system.
Software Updater An Ubuntu tool used to update Linux operating systems and applications.
Sound A Windows Control Panel utility used to configure audio devices and configure the sound scheme.
sound card An adapter, also known as an audio card, that has several ports that convert digital signals to audible sound and also the reverse. Common devices that connect to the ports include microphones and speakers.
spam Email that is unsolicited and comes from unknown people or businesses.
spam gateway A device that filters inbound and outbound email for spam.
spanned volume A Windows term that describes hard drive space created from multiple hard drives.
SPD (serial presence detect) An extra EEPROM feature that allows the system BIOS to read the EEPROM (which contains memory information such as capacity, voltage, error detection, refresh rates, and data width) and adjusts motherboard timings for best CPU-to-RAM performance.
SPDIF (Sony-Phillips Digital Interface Format) See *S/PDIF*.
speaker A mechanical device that produces acoustic sound and that may be internal or external to a computer or mobile device.
spear phishing Provides someone with specific information (an invoice, a known company, account information, etc.) making you think the email is legit in an attempt to obtain personal or corporate information.
special function key One of the uppermost keys on a keyboard, which activate specific functions. Labeled ¡, ™, and so on, these keys control things like sound on/off, screen brightness dimmer/brighter, and more.
special thermal paper Paper sensitive to heat that is used with thermal printers in retail establishments.
speckling Random spots on a printed paper. Check ink cartridges on an inkjet printer. On a laser printer, rock toner cartridge back and forth and replace if necessary.
speed (NIC property) A network card configuration property. It is normally configured automatically, but manual options include 10 Gb/s, 1 Gb/s, 100 Mb/s, and 10 Mb/s.
SPICE (Simple Protocol for Independent Computer Environments) An open source protocol used to remotely access and control VMs.
spinning pinwheel An error indication that can indicate a lack of response from the hard drive and/or a particular application. Commonly seen in macOS.
splash screen An introductory screen that appears on a device that may be required and state the criteria for accessing the device or a particular service or website.
splitting partition (Disk Management) A way of dividing space on a hard drive or making one partition smaller (right-click the drive > *Shrink Volume*) and then creating a new partition with the relinquished drive space.
spoofing Sending an Ethernet frame with a fake source MAC address to trick other devices into sending traffic to a rogue device.
Spotlight A macOS universal search tool that can locate every file and directory and also search email, contacts, music, and even the web.
SPS (standby power supply) A device that provides power to the computer only after it first detects an AC voltage power-out condition.
spyware Software that collects information without user consent, using keystroke logging, gaining access to saved documents, and recording internet activity. Results in unsolicited pop-ups and identity theft.

SQL (Structured Query Language) injection An attack that targets a database to either collect, delete, display, or modify data.

SRAM (static random-access memory) Memory that is faster but more expensive than DRAM. SRAM is also known as cache memory, or L1, L2, or L3 cache.

SSD (solid-state drive) A drive that uses non-volatile flash memory and no moving parts to store data. It is faster but more expensive than a mechanical hard drive.

SSH (Secure Shell) A means of securing data communication including remote connectivity of devices and file transfers. SSH uses port 22.

SSHD (solid-state hybrid drive) A drive that contains both a mechanical hard drive and flash memory used as an SSD.

SSID (service set identifier) A set of up to 32 alphanumeric characters used in wireless networks to differentiate between networks.

SSID broadcasting Used with wireless network access points to periodically send out a beacon frame that includes the SSID. Wireless devices can automatically detect the SSID from this beacon.

SSID not found If a particular SSID is not found in the list of wireless networks, it could be that the wireless router/AP has been configured to not broadcast the SSID, and it has to be entered. Otherwise, the device might be out of range of the wireless network.

stalkerware Software used to track or monitor someone.

standard change A planned change management such as software update, hardware upgrade, hardware replacement, or system change, that is of low risk to the company and pre-approved within the department/company.

standard format The type of drive formatting done through the drive installation process. Contrast with a low-level format.

standard privileges A security function in Windows that allows people using a Standard user account execute specific commands from a CLI.

Standard user One of the two basic types of Windows user accounts that, by default, cannot install most applications or change system settings. Contrast with an Administrator account that has full control over a system.

standoff A plastic connector on the bottom side of a motherboard.

staple jam Check all along the paper path for a staple including rollers. Gently pry off any found staple.

Start button Located in the lower-left corner of the Windows desktop, a button that is used to access and launch applications, files, utilities, and help, as well as to add/remove hardware and software.

Start screen The standard look of Windows that has tiles instead of icons, like the traditional Windows desktop. Windows can also have a traditional desktop and a Start screen.

static IP address An address is manually input in contrast to being assigned by a DHCP server.

Storage Spaces A Windows technology that allows combining different types of storage devices into one writable space.

STP (shielded twisted pair) Network cable with extra foil to prevent outside noise from interfering with data on the cable.

straight tip (ST) connector A type of fiber connector that attaches like a BNC connector where you have to turn the metal part of the connector in order to make a secure attachment.

straight-through cable A network cable that uses twisted pair copper wires and RJ45 connectors at each end. The cable uses the same pinout and is also known as a patch cable.

streak A paper issue in a printer caused by the drum, toner cartridge, dirty or damaged fusing assembly, or the paper.

string A basic data type that is simply a string of characters.

striped volume A Windows term describing how data is written across 2 to 32 hard drives. It is different from a spanned volume in that each drive is used alternately instead of filling the first hard drive before going to the second hard drive. Other names include striping and RAID 0.

stylus An input device that may be known as a touch pen used to provide input on a mobile device.

stylus does not work Check for worn, dirty, or broken tip. Replace battery if it has one.

`su` A Linux command that switches from one user account to another.

subdirectory A directory contained within another directory. Subdirectories are also called subfolders.

subfolder A folder contained within another folder that might also be called a subdirectory.

subnet A portion of a network number that has been subdivided so that multiple networks can use separate parts of a single network number. Subnets allow more efficient use of IP addresses. Also called a subnetwork or a subnetwork number.

subnet mask A number a computer uses to determine which part of an IP address represents the network and which portion represents the host.

subscriber connector (SC) An older type of fiber-optic connector that is square and doesn't have a push lever as part of the connector like the LC type, but it does snap into a socket.

`sudo` A Linux command that allows a user temporary root privileges.

surge suppressor/protector A device that helps protect power supplies from overvoltage conditions. Also known as a surge strip.

suspend mode Another name for sleep mode, used to conserve power in a computing device.

swap partition Also known as a paging file, acts as a memory overflow and allows secondary storage to let programs exceed the size of available physical memory by using hard drive space as memory.

swipe lock Ability to lock out a mobile device or its screen with a finger sweep movement.

switch In star networks, a Layer 2 central controlling device that looks at each data frame as it comes through each port.

swollen battery A bulging battery requires immediate replacement as it may not hold a charge and could soon leak.

Sync Center A Windows 7 Control Panel area used to synchronize files between computers.

synthetic backup A backup method that uses a full backup and incremental backups.

syntax A set of symbols and rules used to create instructions. Every scripting language has its own syntax.

syslog server A device used to receive information from multiple network devices and used as a historical record of events such as devices losing power, a particular interface going down, or access (login/logout) to the device.

Sysprep A tool used to deploy Windows in a corporate environment. Also known as Windows System Preparation.

System A Windows Settings category that contains most of the hardware configuration options for the computer, such as Display, Sound, Power, Storage, and Remote Desktop.

System Configuration utility A Windows utility that allows boot files and settings to be enabled/disabled for troubleshooting purposes. The command that brings up this utility is `msconfig.exe`.

System Control Panel Used to view details about the computer Including the name, amount of RAM, and processor speed as well as allowing and using remote access/assistance.

system file A file that is needed to allow a computer to boot. A file type that is also known as a startup file.

System File Checker (SFC) A Windows tool used to verify operating system files.

system image Contains a saved copy of the operating system and all user files that can be used to restore a damaged or corrupted computer.

System Information A macOS utility that provides an overview of the Mac, including basic diagnostic information such as installed hardware, software, and network settings.

system lockout A configuration setting to prevent unauthorized access when a security method is not successful. For example, incorrectly entering a password three times.

system log Each operating system has logs that can be viewed when things go wrong. In Windows, Event Viewer is used.

system partition A type of active hard drive partition that contains the hardware-specific files needed to load the operating system.

System Preferences A macOS basic management and troubleshooting tool, equivalent to Control Panel utilities in Windows. It contains most of the system settings, such as desktop backgrounds and screen savers, as well as more advanced settings, such as user accounts and file sharing. Third-party applications can also insert their own preferences menu into the System Preferences menu.

system protection The *System* section of the Control Panel > *System Protection* tab is used to set up and configure System Restore, manage restore points, and manage the amount of disk space used by System Restore.

system requirements (application) The hardware and software required for an application to be installed.
system resources The collective set of interrupt, I/O address, and DMA configuration parameters.
System Restore A utility that makes a snapshot of the registry and backs up certain dynamic system files. When a problem occurs, use this utility to take your system back to a time before the error started.
system volume A Windows term describing the storage space that holds Windows operating system files used to boot the computer.

T

T568A An ANSI/TIA/EIA Ethernet network cabling standard.
T568B An ANSI/TIA/EIA Ethernet network cabling standard.
TACACS (Terminal Access Controller Access-Control System) A secure method of authentication using a server.
tailgating A breach of physical security that occurs when an unauthorized person enters a secure space behind an authorized person. Training and diligence by all employees are the only ways to stop tailgating.
taskbar On a Windows program, the bar that runs across the bottom of the desktop. It holds buttons that represent files and applications currently loaded into RAM. It also holds icons representing direct access to system tools.
`taskkill` A command used to halt a process or task.
Task Manager A Windows-based utility that displays memory and processor usage data and also displays currently loaded applications as well as currently running processes.
Task Scheduler A Windows-based utility that allows applications or tasks to be executed periodically or at a specific date and time. This can include a systemwide message.
Task View A Windows icon that allows the user to create multiple desktops and switch between them.
TCP (Transmission Control Protocol) An OSI model Layer 4 standard that ensures reliable communication between two devices.
TCP printing Also known as TCP/IP printing, the ability to connect to and print to a printer that has been assigned an IP address.
TCP/IP (Transmission Control Protocol/Internet Protocol) The most widely used network protocol stack for connecting to the internet. Developed by the Defense Advanced Research Projects Agency in the 1970s, it is the basis of the internet.
teamwork The ability to work with others toward a common goal.
Telnet A nonsecure application protocol that allows connection to a remote network device. Telnet uses port 23. Commonly replaced by the more secure SSH.
temperature Computers should operate in temperatures between 60 and 75 degrees.
terabyte (TB) Approximately 1 trillion bytes of information, or 2^{40} (1,099,511,627,776) bytes.
Terminal The terminal emulator for macOS and Linux that allows the command-line interface (CLI) access to the operating system. Certain tasks or functions are not GUI-friendly, and CLI commands are required.
test development A safe way to use virtualization or other means when trying out new software without hurting any other device.
tethering Allows sharing of internet connectivity among mobile devices in the area. It is a form of hotspot.
text file A file where each byte represents one character of ASCII code. Scripts are all text files.
thermal pad Applied between a processor and heat sink to provide consistent heat dispersion.
thermal paste Applied between the processor and its heat sink to provide a thermal pad that disperses heat more evenly.
thermal printer A printer commonly used in retail that uses heat and special thermal paper to create the printed image.
thick client See *standard thick client*.
thin client A type of computer that does not have all the ports and components (such as a hard drive) of a traditional PC. It includes basic applications, meets minimum requirements for the selected OS, and has network connectivity.
third-party vendor [security] Commonly used for security measures such as shredding corporate documents or destroying data on storage devices.
This PC A category shown in Microsoft Windows that contains local drives and quick access to the desktop, documents, music, and downloads.

thread A unit of programming code that receives a slice of time from Windows, so it can run concurrently with other units of code or threads.

throttle management The ability to control processor speed by slowing the processor down when it is not used heavily or is running too hot.

Thunderbolt A type of video port on PCIe adapters or on Apple computers.

tile A square block on a Windows Start screen with a picture of the function it performs when activated.

Time & language A Windows Settings category used to configure time, date, language, typing and speech options.

time-based one-time password (TOTP) A security measure used to provide a code to someone via text, voice call, or email that has a time limit applied.

Time Machine A bundled application in macOS that performs full and incremental system backups to an external hard drive. It gets its clever naming from the capability to navigate past backups as if traveling backward through time.

time management How much time you budget and then actually spend on doing each task throughout the workday.

time/date/region/language settings Part of the operating system installation process is to set the regional time, date, and language preferences.

timeout/screen lock A security feature in which, after a period of nonuse, the computer requires a username and password to again access the computer.

TKIP (Temporal Key Integrity Protocol) A method of encryption that is an improvement over WEP because the encryption keys periodically change.

TN (twisted nematic) A technology used with LCDs.

tone generator A tool used with a toner probe to identify cables when they are unlabeled or incorrectly labeled.

toner The combined particles in a laser toner cartridge that produce an image when fused onto paper. Harmful if inhaled. Messy if spilled.

toner probe Used with a tone generator to locate and identify cables.

toner vacuum A vacuum used inside a laser printer that will not damage the vacuum as a result.

top Displays real-time dynamic information about running processes and system resources.

TOSLINK A type of fiber S/PDIF connection.

`touch` A Linux command used to create a file.

touch screen An display type that a finger or a stylus is used to interact with it.

touch screen non-responsive When this occurs, close apps. See if the problem is app specific. Restart the device. Turn off the device, remove the battery, allow the device to dry or cool, reinstall the battery, and turn on the device. Remove the screen protector, calibrate the screen, and do a factory reset.

TPM (Trusted Platform Module) A motherboard chip used for hardware and software authentication. TPM can authenticate hardware devices. Applications can use TPM for file and folder encryption, local passwords, email, VPN/PKI authentication, and wireless authentication.

TPM (Trusted Platform Module) A part that might be on the motherboard or the motherboard might have a connector that allows an APM to be installed. It Is also available on a USB stick. A TPM increases security by generating and storing cryptographic keys, passwords and other authentication information, as well as digital certificates.

traceroute A command that traces the route a packet takes to a destination by sending packets with increasing Time-to-Live (TTL) values and observing the responses from network hops.

`tracert` A Windows network troubleshooting command that displays the path a data packet takes through a network, thus allowing you to see where a fault occurs in larger networks. Compare with `traceroute`, used in macOS and Linux.

trackpad A part of a laptop or keyboard that allows cursor control.

track point A device used for locating important items including mobile devices and wallets. (They are also known as tracker, tracking device, or device tracker.)

tractor feed A part of an impact printer used to move fanfold paper through the printer; the paper has holes on each side.

transfer corona A wire inside a laser printer that applies a positive charge to the back of the paper so that the toner is attracted to the paper as it moves through the printer.

transport layer Layer 4 of the OSI model, which determines the details of how data is sent, supervises the validity of the transmission, and defines the protocol for structuring messages.

tray not recognized Re-insert the printer paper tray securely. Check paper size settings and for any paper jams along the paper path.

tree A Windows command that shows a directory and file structure, depending on the option used.

tri-channel A type of memory execution in which motherboards access three memory modules simultaneously.

Trojan A virus program that appears to be a normal application but that, when executed, changes something. It does not replicate but could gather information that could later be used to hack into someone's computer.

trusted source A security measure that is built in to some browsers and security software that indicates whether a website or downloaded file is a trusted or untrusted software source.

twisted pair cable Network cable made of eight copper wires twisted into four pairs. Can be shielded or unshielded.

TXT record A type of DNS record used for documentation and security.

`type` A command that displays a file's contents on the screen.

Type 1 hypervisor In a virtualization environment, a hypervisor that has the operating system running on top of the hypervisor. Also known as a native hypervisor.

Type 2 hypervisor In a virtualization environment, a hypervisor that runs on top of a host operating system to manage and oversee the virtual machine. Also known as a hosted hypervisor.

Type A-B-C fire extinguisher A fire extinguisher that can be used on either Type A, Type B, or Type C fires.

Type C fire extinguisher A fire extinguisher that can be used only on electrical fires.

U

/Users A macOS system folder that contains a home folder for each account that logs into the computer; also contains the Shared folder, whose contents are available to anyone who uses the computer.

/Users/username/Library A macOS system folder that contains a user's personal settings, preferences, caches, and other application-related files.

UAC (User Account Control) A Windows dialog box that appears and asks permission to do something that might be harmful or change the operating system environment. Some changes require an administrator password to continue.

Ubuntu Software Center A software manager to access Ubuntu's repositories of open source software. It can install new applications and uninstall existing ones, many of which are available for free.

UDP (User Datagram Protocol) A Layer 4 connectionless standard that applications use to communicate with a remote device.

UEFI (Unified Extensible Firmware Interface) The replacement for the traditional BIOS that has a boot manager instead of the BIOS controlling the boot process. The UEFI environment allows for a graphic interface, the use of a mouse, antivirus software to be used before the operating system loads, and internet access.

unattended installation A method of installing Windows in which the remote computer does not have to be touched. Use Microsoft Deployment Toolkit with Configuration Manager or another imaging product.

unauthorized app Software that has not been paid for (pirated or bootleg).

unavailable resources A symptom of a network problem in which the network device cannot access the internet, a network printer, a network share, a particular server, email, and/or other resources.

unbuffered memory Memory that does not delay all data transfers by one clock tick to ensure accuracy as registered memory does. Used in low- to medium-powered computers.

undervoltage A condition that occurs when AC power drops below 100 volts, which may cause the computer's power supply to draw too much current and overheat.

unexpected app behavior Could be caused by a free app, OS version, malicious app, or poorly written software.

unfreeze A change management time frame where IT systems can be modified or installed.

Unity The graphical user interface in Ubuntu. It has some similarities to the user interface of macOS, but it is drastically different from Windows.

unlicensed range Wireless frequencies that any manufacturer can use.

unmanaged switch A type of switch that cannot be remotely accessed and is commonly found in home and small business wired networks.

unprotected system A computer that has no anti-virus/anti-malware software installed and/or firewall disabled.

unshielded twisted pair See *UTP* and see also *twisted pair cable*.

untrusted source A security measure that is built in to some browsers and security software that indicates whether a website or downloaded file is a trusted or untrusted software source.

unusual noise A symptom of a CPU or system fan, hard drive, or power supply problem.

Update & Security In Windows 10, a Settings category with options to configure Windows Update and manage security settings.

update boot order One thing that can cause a Windows computer to not boot is the boot order in the BIOS/UEFI settings.

update network settings A device might need the network settings updated in order to get onto the wired or wireless network. This could involve using the `ipconfig /release` and `ipconfig /renew` commands or changing the IP address to a manually assigned one.

updatedb A Linux command that updates the file database.

UPnP (universal plug and play) An alternative to port forwarding that allows peer-to-peer (P2P) gaming applications to function without further configuration.

UPS (uninterruptible power supply) A device that provides power for a limited time to a computer or device during a power outage.

upstream Describes information that is sent to the internet, such as transmitting email or uploading a file to a server.

upward compatibility A technique used by a software manufacturer when a product is designed in such a way that it can accept input intended for a future version. Another name for forward compatibility.

USB (universal serial bus) A bus that allows 127 devices to be connected to a single computer port.

USB 2.0 A standardized port that supported speeds up to 480 Mb/s, a maximum of 0.5 amps, 5 VDC, as well as Type A and Type B connectors.

USB 3.0 A standardized port that supports speeds up to 5 Gb/s, a maximum of .9 amps, and 5 VDC.

USB 3.1 A standardized port that supports speeds up to 10 Gb/s and supports the Type C connector.

USB expansion card A metal plate that has one or more USB ports and a cable that connects to the motherboard. The metal plate fits in a slot that a normal card in an expansion slot would take.

USB header Pins on the motherboard used to connect to a USB adapter so that more USB ports are available.

USB lock A security device that prevents USB storage devices from being inserted into a USB port.

USB Permissions A BIOS/UEFI Setup option used to modify parameters such as USB speed options and the number of ports to enable/disable.

USB Type-A An upstream male connector on a USB cable that connects to an upstream Type-A port on a host computer or other hub.

USB Type-B A downstream male connector on a USB cable that connects to a Type-B connector on the downstream device.

USB Type-C A reversible plug connector for USB devices and hosts and that will eventually replace USB Type-A/Type-B plugs.

USB-C See *USB Type-C*.

USB-PD A USB power delivery standard that allows up to 20 V at 5 A for 100 watts of power. The standard has five levels of power: 10 W, 18 W, 36 W, 60 W, and 100 W.

USB-to-Ethernet converter A connector cable with a USB plug and an Ethernet end.

User Account Control See *UAC*.

user account management The process of creating a user, adding that user to a group, and managing those functions.

user authentication/strong passwords A security method used to ensure that a person accessing a device, network, or resource is allowed to do so.

user profile All settings associated with a specific user, including desktop settings, network configurations, and applications that the user has access to. It is part of the registry.

User State Migration Tool See *USMT*.

username and password A form of security where the device or an authentication server has a specific unique identifier and associated characters to allow access.

USMT (User State Migration Tool) A Windows tool used when deploying a large number of Windows computers.

UTM (unified threat management) A security device that provides multiple functions, such as content filtering, antivirus, antispyware, anti-malware, firewall, and intrusion detection and prevention.

UTP (unshielded twisted pair) The most common network cable. Comes in different categories for different uses. See also *twisted pair cable*.

V

`.vbs` A file extension for VBScript files.

VA (vertical alignment) An LCD panel technology that provides wide viewing angles, good color, and high contrast.

vacuum A device used to suction dust and debris from computers and wiring closets.

variable In scripting, the name of a storage location in the computer's internal memory. The value of the variable is the contents at that memory location. It Is called a variable because the value can change (vary) as the program runs.

VBScript A scripting language designed specifically for use with Microsoft Internet Explorer. A VBScript file has the extension .vbs.

VDI (virtual desktop infrastructure) An environment in which the PC's operating system and apps reside on a server.

ventilation Computers require good ventilation. Never block air vents, especially on a laptop.

VGA port A type of 15-pin three-row video port that normally has a CRT monitor attached.

`vi` A command-line text editor used by macOS and Linux.

video capture card An adapter that allows bringing in video from an external source such as a video camera.

video card An adapter used to output video to a display. Contrast with onboard video card.

virtual machine A way for an operating system to appear as a separate computer to each application. One computer that has two or more operating systems installed that are unaware of each other due to virtualization software.

virtual printing Printing to somewhere other than to the directly connected printer and to a specific file so that the information can be viewed, saved, emailed, or sent to another printer.

virtual RAM A method of using storage space on the hard drive as if It were memory.

Virtual XP mode A Windows 7 tool that was previously known as Windows XP Mode that can be downloaded and used in Windows 7 Professional and higher versions to allow older applications to run.

virtualization A process that allows a computer to run multiple operating systems without affecting each other, share hardware, and provide a test environment for software that may not be compatible on a specific platform.

virtualization support A BIOS/UEFI option that allows virtualization to be enabled on a computer that has the hardware and an operating system that supports virtualization.

virtualization workstation A computer that has multiple operating systems in a virtual environment in which one operating system has no interaction with the other operating system; they are independent of one another. A virtualization PC has multiple powerful multicore processors, maximum RAM, multiple fast large-capacity hard drives, 1 Gb/s network connection, virtualization software, and a possible NAS.

virus A program designed to change the way a computer originally operated.

vishing A form of phishing that uses a voice call in order to obtain personal information.

VLAN (virtual local area network) A switch technology that allows assignment of ports to a specific VLAN number, thus creating separate networks so that the devices that connect to ports assigned to one VLAN number cannot see devices that connect to switch ports assigned to a different VLAN number.

VM (virtual machine) See *virtual machine*.

VNC (virtual network computing) A situation in which one computer can be controlled from a remote network.

voice recognition technology A security measure that allows access based on someone speaking.

VoIP (Voice over IP) A way of sending phone calls over the internet or over networks that traditionally transmitted only data.

volt The measurement for voltage.

voltage An electronic measurement of the pressure pushing electrons through a circuit. Voltage is measured in volts.

volume A section of a storage device that receives a drive letter and to which data can be written.
VPN (virtual private network) A remote computer connecting to a remote network by "tunneling" over an intermediate network, such as the internet or a LAN.

W

Wake on LAN A BIOS and adapter feature that allows a network administrator to remotely control power to a workstation and allows a computer to come out of the sleep mode.
Wake on Ring A BIOS and adapter feature that allows a computer to come out of sleep mode when the telephone rings, so the computer can accept faxes, emails, and so on when the user is absent.
WAN (wide area network) Two or more LANs communicating, often across large distances. The most famous WAN is the internet.
WAP (wireless access point) See *wireless access point*.
warm boot Restarting a computer by pressing Ctrl+Alt+Del, using the restart function, or by clicking the Windows Restart option. Puts less strain on a computer than a cold boot.
warranty The amount of time a particular piece of hardware is guaranteed by the manufacturer.
watt The electrical measure in which computer power supplies are rated.
wattage rating A measure used to determine whether a power supply is powerful enough to power the devices within a computer.
web server A computer configured to provide web-based content that is accessed through a web browser.
webcam Short for web camera, a small camera used for communicating via video across the internet.
weight limitation Do not lift anything that weighs over 40 pounds by yourself.
WEP (Wired Equivalent Privacy) A type of encryption that is sometimes used in wireless networks.
whaling A form of phishing attack that targets senior executives.
`while` loop In scripting, a type of loop that begins with the keyword `while` along with a test condition. If the condition is true, the loop begins, and the block of statements in the loop repeats until the condition is no longer true.
whoami Displays user, group and privileges information for the user who is currently logged on to the local system.
Wi-Fi (Wireless Fidelity) A type of network in which no wires are needed to connect to the network.
Wi-Fi 5 See 802.11ac.
Wi-Fi 6 See 802.11 ax.
Wi-Fi 7 See 802.11be.
Wi-Fi analyzer A tool used to identify what wireless networks are in the area, determine what frequencies (channels) are used, and find a less crowded channel for any wireless installations, hotspot, or tethering that may be needed in a particular area. Also known as a wireless locator.
Wi-Fi antenna Attaches to a WLAN card to receive or transmit wireless signals.
Wi-Fi antenna connector The screw holes where you attach the wireless antenna cables in a mobile device.
Wi-Fi calling A common mobile device app used to make phone calls using a WiFi connection rather than a cell phone network.
wildcard A special character used at the command prompt when typing commands. The `?` character is used to designate "any" for a single character place, whereas the `*` character denotes any characters from that place forward.
window A specific area of the screen that has contains information.
Windows Defender A Windows application that detects spyware.
Windows Defender Antivirus Security software that is compatible with other antivirus products and is available in Microsoft Windows.
Windows Defender Firewall Security software provided with Microsoft Windows used to allow or block network traffic based on rules.
Windows domain A type of computer network in which all user accounts, computers, printers, and other network devices are registered with a central database located on one or more clusters of central computers known as domain controllers.
Windows Explorer See *Explorer*.
Windows Hello An option that allows you to use a face, fingerprint, pin, security key, password, or picture password to gain access.

Windows Memory Diagnostic tool A tool used to thoroughly test RAM. Accessed from a command prompt using the `mdsched` command or using the *Administrative Tools* section of the Control Panel > *Diagnose Your Computer's Memory Problems* link.
Windows Mobile A Microsoft operating system for phones that has been discontinued.
Windows Recovery Environment See *WinRE*.
Windows Resource Protection See *WRP*.
Windows Storage Spaces A Windows 8/10 technology that allows the combination of different types of storage devices into one writable space.
Windows Tools A Windows Control panel category that contains higher-level utilities that are also found in other categories; known as Administrative Tools in Windows 10.
Windows Update Modified files provided for the current operating system.
Windows Update A Windows Settings tool used to manage Windows Updates.
Windows Upgrade Advisor A Microsoft tool that can be downloaded and executed to determine if a computer can function well with a higher version of Windows installed.
WinRE (Windows Recovery Environment) A tool found on the Windows installation disc and also in Windows that includes multiple tools used to troubleshoot Windows when it does not work properly.
WinRM (Windows Remote Management) A tool used to remotely access and configure/maintain Windows computers.
wireless access point A device that receives and transmits data from multiple computers that have wireless NICs installed. The access point can be a standalone unit or can be integrated into an ADSL router.
wireless broadband A feature available from service providers that allows PC Cards, USB modems, mobile data cards, or integrated laptop connectivity to have the capability to receive, create, and communicate internet information within a specific coverage area.
wireless card Also known as a wireless NIC, an electronic device that allows wireless network connectivity.
wireless extender Another name for a wireless repeater that increases the size of a wireless network.
wireless regulations Wireless frequencies are regulated within a particular company. There are licensed and unlicensed ranges, but even in the unlicensed ranges there are rules that must be followed regarding maximum power, subchannels, etc.
WISP (wireless internet service provider) A vendor that provides internet access.
WLAN (wireless LAN) A wireless network that consists of an access point and some wireless devices, including laptops, tablets, and smartphones.
WMN (wireless mesh network) A type of wireless network that does not require access points. Peer radio devices allow connectivity over distances, which is especially good in emergency situations. Data is passed from one device to another to reach its final destination.
workgroup A term given to a peer-to-peer Windows network. A workgroup does not use a server to authenticate users during the login process.
WPA (Wireless Protected Access) A data encryption program that uses Temporal Key Integrity Protocol (TKIP) or Advanced Encryption Standard (AES) to improve security.
WPA2 (Wireless Protected Access) An improvement over WPA that includes dynamic negotiation between the AP and the client for authentication and encryption algorithms. It is a common choice for securing wireless networks.
WPA3 (Wireless Protected Access A wireless security standard that makes use of simultaneous authentication of equals (SAE) encryption.
WPS (WiFi Protected Settings) A method used to easily configure a wireless device for the SSID and WPA2 security.
written communication An important skill for a person in IT to have, especially when communicating with others and documenting IT issues/processes.
WRP (Windows Resource Protection) A tool that protects system files and registry keys in Windows.
WWAN (wireless wide area network) A wireless network that extends across more than one county, such as when WiMAX is used.

X

x64 A term that refers back to the architecture and commands used originally with the Intel 8086 CPU that have been updated to a 64-bit version.
x86 A term that refers back to the architecture and commands used with the Intel 8086 CPU.

xcopy A command that transfers files from one place to another in the command prompt environment.

XDR (Extended Detection and Response) A security platform used to protect computers, laptops, and servers, provide 24/7 monitoring, and extend the coverage to include the network, cloud environment, and app security.

xDSL Used to describe the various types of digital subscriber lines (DSLs) available for connecting to the internet. Examples include ADSL, CDSL, DSL Lite, HDSL, RADSL, SDSL, VDSL, and x2/DSL.

XFS (Extensible File System) A disk file system type that is suitable for enterprise-level computing (such as data centers) because it efficiently handles extremely large file systems in the petabyte range.

XSS (cross-site) scripting A situation where a threat actor collects and even changes data between a user and the device providing the service (such as a web server).

Z

zero day [attack] A vulnerability in a particular software application that is found by hackers before it is known or fixed by the developer of the application.

zero-touch deployment Sometimes called unattended installation or zero touch installation (ZTI), a method of installing an operating system in which a script or answer file (usually custom-prepared for a specific company) is used to provide configuration options during the installation process.

Zero Trust model A method of IT security design that says nothing and no one are trusted and everything is verified. All IT areas are compartmentalized and access is granted for pre-determined policy-driven reasons and the right credentials are provided. When a breach occurs, it is isolated to that one compartment.

ZIF socket (zero insertion force socket) A common CPU socket that has a lever that provides easy access for CPU removal.

zombie A device that has been hacked and is controlled by someone else or that carries out malicious tasks.

This page intentionally left blank

Index

Symbols

* (asterisks) as wildcards, 664
\ (backslashes)
    \error messages, keyboards, 456
    file structures, 659
: (colons), comments, 704
= = (equal to) operators, 705
>= (greater than or equal to) operators, 705
> (greater than) operators, 705
(hash characters), 492, 703-704
<= (less than or equal to) operators, 705
< (less than) operators, 705
!= (not equal to) operators, 705
. (periods) in commands, 661
.. (two periods) in commands, 661
? (question marks), troubleshooting mobile devices, 426
“ ” (quotation marks), comments, 703
// (slashes), comments, 703

Numbers

1s and Os (bits), 18
2.0 audio subsystems, 450
2.1 audio subsystems, 450
2.4 GHz frequencies
    mobile devices, 375
    wireless networks, 546
2.5GBaseT Ethernet standard, 521
2.5-inch hard drives, 215
3-2-1 backups, 901
3.3V output voltage, 153
3.5-inch hard drives, 215
3-D printers, 303, 308
3G cellular networks, 367, 490
3-pin ATX power supply connectors, 154
4G cellular networks, 367, 490
4GB RAM, 185
4-pin 12V ATX power supply connectors, 154
4-pin Berg power supply connectors, 154
4-pin Molex power supply connectors, 154
5G cellular networks, 367, 490
5GBaseT Ethernet standard, 521
5 GHz frequencies
    mobile devices, 375
    wireless networks, 546
5V output voltage, 153
5,400 RPM (Revolutions Per Minute), magnetic hard drives, 216
6 GHz frequencies
    mobile devices, 375
    wireless networks, 546
6-pin ATX power supply connectors, 154
6-pin PCIe ATX power supply connectors, 154
7,200 RPM (Revolutions Per Minute), magnetic hard drives, 216
8-pin 12V ATX power supply connectors, 154
8-pin PCIe ATX power supply connectors, 154
10BaseT Ethernet standard, 521
10GBaseER Ethernet standard, 521
10GBaseLR Ethernet standard, 521
10GBaseLX4 Ethernet standard, 521
10GBaseSR Ethernet standard, 521
10GBaseT Ethernet standard, 521
12V output voltage, 153
15-pin SATA power ATX power supply connectors, 154
20 + 4 connectors, 142
20-pin motherboard connectors, 155
24-pin main power ATX power supply connectors, 154
24-pin motherboard connectors, 155
24-pin motherboard power connectors, 142
25GBaseER Ethernet standard, 521
25GBaseLR Ethernet standard, 521
32-bit OS, 617
40 Gb Ethernet standard, 521
64-bit OS, 617
80 PLUS efficiency ratings, power supplies, 162
100BaseT Ethernet standard, 521
100 Gb Ethernet standard, 521
110V vs. 220V input voltage, 153
568A/B cabling standard, 51
802.11 wireless standard, mobile devices, 375-376
802.11a wireless standard, 375, 548
802.11ac (Wi-Fi 5) wireless standard, 375, 548
802.11ad (WiGig) wireless standard, 548
802.11ax (Wi-Fi 6) wireless standard, 375, 548
802.11b wireless standard, 375, 548
802.11be (Wi-Fi 7) wireless standard, 375, 548
802.11e wireless standard, 548
802.11g wireless standard, 375, 548
802.11i wireless standard, 548
802.11n wireless standard, 375, 548
1000BaseLX Ethernet standard, 521
1000BaseSX Ethernet standard, 521
1000BaseT Ethernet standard, 521
10,000 RPM (Revolutions Per Minute), magnetic hard drives, 216
15,000 RPM (Revolutions Per Minute), magnetic hard drives, 216

A

A records, DNS, 565
AAA servers, 584
AAAA records, DNS, 565
AAX files, 631
AC (Alternating Current), 150-151, 164
acceptance from end-users, change management, 966
access
    ACL, 871
    attacks, 882
    Bluetooth printers, 336

cloud storage, 805
command prompt, 656
Device Manager, 114
domains, 622
environment variables, 696
File Explorer, Windows, 897
guest access, wireless networks, 927
identity access management, 870
IMAP, 589
JIT access, 873
Keychain Access, macOS, 832-833
LDAP, 589
local access, security, 884-886, 889
network access
security, 884-886, 889
user management, 884
Network Access layer, TCP/IP, 590
network printers, 336
PAM, 873
physical access, security policies, 862
PowerShell, 666
ransomware, 878
remote access, 863, 918
remote networks, 689
root access, unauthorized, 414-415
secure management access, 571
Setup programs, 105
TACACS+, 873
unauthorized account access, 413
wireless networks, guest access, 927
wireless printers, 336
WPA, 568
WPA2, 568, 923
WPA2 with AES, 568
WPA3, 568, 923
access control vestibules (mantraps), physical security, 866-867
"access denied" messages, share permissions, 894
accessories, mobile devices, 362-364
accounts
AD accounts, 886-888
administrator accounts, 763, 884-885
backup operator accounts, 885
child accounts, 884
email accounts
creating, 804
troubleshooting, 910
expiration dates, 890
guest accounts, 884, 890
network configuration operator accounts, 885
offer remote assistance helper accounts, 885
performance log user accounts, 885
recovery, 763-764, 902
remote desktop user accounts, 885
root user accounts, 836
standard accounts, 884
standard user accounts, 763
unauthorized access, 413
user accounts, 885
Credential Manager, 759, 762
Local Users and Groups tool, 762-763
recovery options, 763-764
rights, 762
root user accounts, 836
UAC, 722, 764
UAC, permissions, 897
ACL (Access Control Lists), 738, 871
ACPI (Advanced Configuration and Power Interface), 159
ACPI setting (BIOS/UEFI), 109
action plans (troubleshooting process), establishing, 463
activation clocks, 734
active listening (soft skills), 2, 92-93, 970
Active status messages, 250
ActiveSync, 381
Activity Monitor, macOS, 830
AD (Active Directory)
accounts, 886-888
basic functions, 885-886
corporate OS, 622
folders, 888
login scripts, 888
OU, 886
security groups, 886
adapters
DVI-to-HDMI, 42
flash media, 361
identifying adapter functions, 13
installing, 13-14
integrated motherboard ports, 53
miniPCI/PCIe, 390
motherboards, 13
nonvideo adapters, 161
PCIe, 86
removing, 143
video adapters
installing, 269-270
troubleshooting, 459
Wake on LAN, 159-160
Wake on Ring, 159
adding
arrays, 767
computers to domains, 566-567
devices, Windows, 743
audio devices, 746
clock drift, 750
Device Manager, 743-748
display settings, 746-747
"Not enough USB controller resources" error messages, 749-750
Sound utility, 746
USB endpoints, 749-750
snap-ins, 754
volumes to hard drives, 767
Windows credentials, 760
address bars, web browsers, 6, 493
addressing
ARP, 587
broadcast addressing, 544, 987
dynamic IP addressing, 560
I/O addresses, 114
IP addressing, 985-987
dynamic IP addressing, 560
filtering, 925
static IP addressing, 560
IPv4 addressing, 542
broadcast addressing, 544
CIDR, 546

classes of, 543
examples of, 544
host addresses, 543
network numbers, 543
octets, 542
private IP addresses, 543
public IP addresses, 543
schemes, 544
subnet masks, 545-546
VLAN, 545
link-local addressing, IPv6, 542
MAC addressing, 541, 921
filtering, 924
formats of, 542
memory addresses, 114
NAT, 570, 587, 917
non-IT personnel, 56
PAT, 587, 917
physical addresses, 542
static IP addressing, 560
ADF (Automatic Document Feeders), 17, 288
Administration option, AP configurations, 571
Administrator Password setting (BIOS/UEFI), 108
administrators
accounts, 763
BIOS/UEFI security, 873
default user account passwords, changing, 885
defragmenting hard drives, 769
disk management tools, 767
group accounts, 884
privileges, 656
rootkits, 878
run as administrator permissions, 897
shares, 893
user accounts, 884
Windows
changing update settings, 740
reloading, 738
ads
adware/pop-ups, 497, 880
blocking, 379, 497
high number of ads, 414
ADSL (Asymmetric DSL), 483
Advanced BIOS setting (BIOS), 108
Advanced Boot Options menu, Windows, 776-777
advanced menu, UEFI, 107
Advanced tab (Internet Options Control Panel), 494
adverse power conditions, 951
advertisements
memory, 189
SODIMM, 400
adware/pop-ups, 497, 880
aerosol cans, disposal laws, 149
AES (Advanced Encryption Standard), 568, 903
AGP (Accelerated Graphics Ports), 84
AHCI (Advanced Host Controller Interface) mode, SATA, 228
AI (Artificial Intelligence), 71
file extensions, 631
hallucinations, 961
IT documentation, 961
private AI, 961
public AI, 961
air, compressed, 148-150, 945
air filtration masks, 149, 945
airborne particle pollution, safety, 957
airflow, cases, 157
Airplane mode, 376
alarms
physical security, 866
troubleshooting, 247
alcohol, denatured, 148
alerts
desktop alerts, 880
malware alerts, 880
WEA, 370
all-in-one computers, disassembly, 146
all-in-one (multifunction) devices, 17. *See also* printers
installing, 326
overview, 302
sensitive material, 302
allow lists, 913
alphanumeric characters, 701
alternative IP addresses, configuring, 563
AMD (Advanced Micro Devices)
APU, 72
HyperTransport buses, 70
multicore processors, 71
processors, 66-67, 75-76, 268
sockets, 76
video cards, 268
AMI, BIOS/UEFI audio beeps, 456
amplification, speakers, 281
amps, 151-153
analog signals, video ports, 38
analysis
cell tower analyzers, 387
risk analysis, change management, 965
Wi-Fi analyzers, 386, 558
AND operators, 708
Android OS, 360, 619
APK, 371
apps
deleting, 418
updating, 419
developer mode, 371
email configuration, 380
factory resets, 384
home screens, 364
mobile device backups, 384
mobile device synchronization, 383
Recovery Mode, 416
security, 413
antenna connectors, Wi-Fi, 405
antennas
attenuation, 556
directional antennas, 556
gain, 557
MIMO, 558
MU-MIMO, 558
networks, 541
omnidirectional antennas, 556
path loss, 556
radiation patterns, 556
ranges, 557
signal strength, 558
wireless antennas, laptops, 406
Wi-Fi, 407

anti-malware, 870
mobile devices, 386
reinitializing, 735
security policies, 862
antistatic protection
bags, 138, 949
brushes, 148
gloves, 78, 137
antistatic wrist straps, 78, 136-137
antivirus software, 870
Microsoft Defender Antivirus, 906
mobile devices, 386
reinitializing, 735
rogue antivirus apps, 906
Windows installations, 732
AP (Access Points), 541, 548-549
as wireless repeaters, 552
default settings, 926
firmware, 926
installing, 926-927
passwords, 926
rogue AP, 928
SSID, 551, 926
wireless AP, 570-571
wireless networks, 921
APFS (Apple File Systems), 230
APIPA (Automatic Private IP Addressing), 563
APK (Android Application Packages), 371
app scanners, 386
App Center, Ubuntu, 843
appearance (soft skills), 428-429
.app files, 824
App history tab, Task Manager, 783
App Store, macOS, 823-824
Apple
Apple ID, 823
iCloud, mobile devices, 384-385
iOS, 360, 619
deleting apps, 419
email configuration, 380
mobile devices, 383-384
passcode settings, 413
security, 413
updating apps, 419
iPadOS, 360, 619
iPhones, home screens, 365
iTunes, mobile device synchronization, 384
Lightning ports, 372
macOS, 818
Activity Monitor, 830
.app files, 824
Apple ID, 823
App Store, 823-824
best practices, 854
Boot Camp, 834
cd command, 835-836
chmod command, 835-838
chown command, 835-837
Console, 831
cp command, 835-836
desktop, 819-820
Disk Utility, 833-834
.dmg files, 824
Dock, 819-820
Finder, 819
Force Quit, 826
gestures, 822
grep command, 835-838
GUI, 819-822
iCloud, 822
installing apps, 824
iWork, 822
kernel panic, troubleshooting, 831
Keychain Access, 832-833
kill command, 835
Launchpad, 821
less command, 835, 838
ls command, 835
man command, 835, 839
menu bar, 819
Mission Control, 820
mkdir command, 835
mv command, 835-836
nano command, 835, 838
Notification Center, 820
Passwords app, 832
pinwheels, 830
.pkg files, 824
POSIX, 819
pwd command, 835-836
recovering deleted files, 826
releases, 818-819
rm command, 835-836
root user accounts, 836
Safe mode, 829
screen-sharing, 823-824
Spotlight, 821
su command, 835
sudo command, 835-836
system folders, 823
System Information, 831
System Settings, 827-829
system updates, 824
Terminal, 834
Time Machine, 825-826
touch command, 835-836
troubleshooting, 829
troubleshooting, kernel panic, 831
uninstalling apps, 824
utilities, 830-834
vi command, 835
Widgets, 820
OS X, 818
Application layer
OSI model, 540
TCP/IP model, 541, 590
application logs, troubleshooting, 758
Apply button, Windows, 629
Apps & Features Settings utility, Windows, 752
apps (applications)
antivirus apps, rogue, 906
APK, 371
App Store, macOS, 823-824
authenticator apps, 412, 872
Backups app, Ubuntu, 844
closing failures, troubleshooting, 418
cloud computing, 505
common apps, 369
compatibility with OS, 195, 751
containers, 503
CPU tab, Task Manager, 786
crashes, 195, 757, 782
deleting, 418-419
Details tab, Task Manager, 784
disabling, 780
DRM, 876
email, off-site apps, 505
file types, 621
hanging apps, troubleshooting, 757

installing, 371, 695, 751-752
failures, troubleshooting, 419
macOS apps, 824
launching, 751
Launchpad, macOS, 821
loading failures, troubleshooting, 419
locator apps, 369-370
logs, 757
macOS, installing/uninstalling apps, 824
malicious apps, 411
MAM, 385
Memory tab, Task Manager, 786
Microsoft Store, 722
Mission Control, macOS, 820
"not responding" error messages, troubleshooting, 757
obtaining, 371
older apps, Windows compatibility, 195
opening, 365
OS
app compatibility, 195, 751
OS-specific apps, 615
requirements, 751
update limitations, 620
partitioning, 231
Passwords app, 832
Performance tab, Task Manager, 786
pinning to Windows 11 taskbars, 627
QR codes, 371
quitting, Force Quit (macOS), 826
recovery, Time Machine (macOS), 825-826
removing, 371
repairing, 753
rogue antivirus apps, 906
sandboxes, 411
SDK, 371
Services and Applications, Windows, 769
Services tab, Task Manager, 784
Settings app, Windows 10/11, 640-641
side-by-side apps, Windows, 722
side-loading, 371
spoofing, 411
starting during Windows startup, 784
Startup apps tab, Task Manager, 783
system requirements, 751
Time Machine (macOS), 825-826
troubleshooting, 418-419
unauthorized apps, 411
uninstalling macOS apps, 824
updating
failures, troubleshooting, 419
MDM and, 385
Users tab, Task Manager, 784, 787
virtual apps, streaming, 505
Windows Update Assistant, 725
Apps utility, Windows 11, 752
apt command, Linux, 845, 848-849
APU (Accelerated Processing Units), 72
archival storage, SSD, 217
ARM processors, 66
ARP (Address Resolution Protocol), 587
arrays
adding, 767
RAID
"array missing" error messages, 251
BIOS/UEFI settings, 240
configuring, 238
failures, 251
fault tolerance, 238-240
FCM, 239
hardware RAID, 240
hot swappable RAID drives, 240
levels of, 239, 240
RAID, 239
"RAID not found" error messages, 251
software RAID, 239
troubleshooting, 251
articles/knowledge bases, 961
aspect ratios, displays, 450
assessment phase, change management, 965-966
asset management, 963
asset tags, 963
assigning
default gateways, 565
hard drive letters, 235, 657, 767
assistants (virtual), 370
asterisks (*) as wildcards, 664
ATA, SATA, 219
AHCI mode, 228
BIOS/UEFI settings, 228
cabling, 223
connectivity, 220-221
eSATA, 221, 225-226
installing devices, 223
Legacy mode, 228
mSATA, 220, 225, 228
ports, enabling in BIOS/UEFI, 224
RAID BIOS/UEFI configuration settings, 240
RAID mode, 228
attacks, security
access attacks, 882
adware/pop-ups, 880
backdoor attacks, 882
BEC attacks, 882
boot sector viruses, 878
botnets, 879, 882
brute force attacks, 882
cryptojacking/cryptomining, 879
DDOS attacks, 882
dictionary attacks, 874, 882
DoS attacks, 882
dumpster diving, 869, 881
evil twin attacks, 882
fileless malware, 879
impersonation attacks, 880
inside attacks, 882
keyloggers, 879
malware, 878-880
MITM attacks, 883
password spraying attacks, 883
phishing, 881-882
piggybacking, 881
PUP, 880
QR code phishing, 881
ransomware, 878
reconnaissance attacks, 883
replay attacks, 883
rootkits, 878
shoulder surfing, 866-867, 881

smishing, 881
Smurf attacks, 883
social engineering attacks, 875, 880
spear phishing, 881
spoofing attacks, 883
spyware, 878
SQL injection attacks, 883
stalkerware, 879
supply chain/pipeline attacks, 883
tailgating, 866, 881
TCP/IP hijacking attacks, 883
Trojan malware, 878-879
viruses, 878-880
vishing, 881
vulnerability scanners, 883
whaling, 881
XSS attacks, 883
zero-day attacks, 883
zombie attacks, 883
attenuation, antennas, 556
attitude (soft skills), 3, 200, 292-293, 969
attrib command, 665, 669
attributes, files/folders, 896-897
handling, 665
Windows, 637
ATX (Advanced Technology Extended)
motherboards, 88, 157
power connectors, 157
power supplies, 153-156
audible alarms, troubleshooting, 247
audio
2.0 subsystems, 450
2.1 subsystems, 450
beeps, 456
cards, 43
devices, adding with Sound utility (Windows), 746
displays, troubleshooting, 272
editing workstations, system design, 442
headsets, 362-363
microphones
choosing, 280-281
laptops, 407-410
system design, 450
Windows operations, 280-281
motherboards
ports, 277
speakers, 276
ports, 43, 54, 277-278
POST codes, 455
projectors, 276
sound cards, 277
installing, 278-279
muting, 280
port connectivity, 279
system design, 450
theory of operation, 278
Windows operations, 279
speakers
amplification, 281
choosing, 282
frequency response ranges, 282
mobile devices, 362
motherboards, 276
power ratings, 281
shielding, 282
system design, 449
troubleshooting, 282-283
USB speakers, 282
volume control, 282-283
subsystem design, 449-450
troubleshooting, 276, 282-283
voice recognition, physical security, 868
audit logs, 337, 890
AUP (Acceptable Use Policies), 863, 964
authentication, 864
apps, 872
authenticator apps, 412
defined, 884
digital security certificates, 906
DMARC, 912
failures, 873
identity synchronization, 872
JIT access, 873
Kerberos, 873
multifactor authentication, 872
networks, troubleshooting, 585
OTP, 872
PAM, 873
printers, 337
RADIUS, 873
SAE, 923
SAML, 873
scanners, 337
servers, 584
soft tokens, 872
SSO, 872
TACACS+, 873
TOTP, 872
authorization, 884
autodiscovery, servers, 380
automating
backups, 695
IT, 966
processes, 693-694
updates, 739
automobiles, mobile device synchronization, 381
AutoPlay, disabling, 904
autorotating screens, troubleshooting, 421
AutoRun, disabling, 904
auxiliary fans
cases, 157
power requirements, 161
availability, cloud computing, 507
avoiding distractions (soft skills), 971-972

B

B+M keys, SSD, 218
backdoor attacks, 882
backlights (screens), 407, 421
backslashes (\)
\error messages, keyboards, 456
file structures, 659
backup operators accounts, 885
backups, 452-453
3-2-1 backups, 901
alternative locations, backing up to, 902
automating, 695
batteries, 954
before OS installations, 731
before troubleshooting, 451
credentials, 760
data backups, Windows, 644, 740-741
differential backups, 900

File History backups, 741
full backups, 900
GFS backups, 901
grandfather backups, 901
incremental backups, 900
Linux, 844
mobile devices
Android OS, 384
iCloud, 385
iOS, 384
multiple hard drives as backups, 900
off-site backups, 902
OS security, 899-902
remote backups. *See* synchronizing
restore points, 741
synthetic backups, 900
testing, 899
wbadmin command, 690
Windows
data, 644, 740-741
registry, 644, 740-741
system images, 644-645
Windows Backup, 901
Backups app, Ubuntu, 844
backward compatibility, 621
badge readers, physical security, 865
badging, data privacy, 337
bags, antistatic, 138
balanced power, Windows, 799
bandwidth, 488, 587
barcode scanners, 288
baselines, 785
basic disks, 236, 727
Basic QoS (Quality of Service), wireless networks, 571
basic storage, 236
BAT files, 631, 664, 693
batch scripting, Notepad, 692
batteries
backups, 954
charging, 424
CMOS, 112
cooling, 393
failing batteries, signs of, 111
improper charging, 392
laptop batteries
optimizing performance, 393-394
removing, 392
Li-ion batteries, 393, 947-948
motherboard batteries, 111
poor battery health, 423
recycling, 111, 948
swollen batteries, 423
troubleshooting, 423-424
bauds, 481
bcdedit command, 669-670
be humble (soft skills), 855
BEC (Business Email Compromise) attacks, 882
beeps, POST, 195
being on time (soft skills), 200, 971
being proactive (soft skills), 598
best practices
Linux, 854
macOS, 854
security, 930
binary bits, defined, 18
binary prefixes (bytes), 20
biometric security, 867
activating, 869
fingerprint scanners, 868
FRT, 868-869
mobile devices, 378, 412
palm print scanners, 868
retinal scanners, 868
voice recognition, 868
BIOS (Basic Input/Output Systems)
audio beeps, 456
boot process, 454
configuration settings
ACPI, 109
Administrator Password, 108
Advanced BIOS, 108
Boot Options, 107-108
Boot Password, 108
Built-in Diagnostics, 109
CPU Configuration, 108
Devices, 108
Drive Encryption, 109
Fan Control, 108
fTPM, 109
General Optimization, 107
Hardware Monitoring, 108
iGPU, 109
Integrated Peripherals, 108
Intrusion Detection/Notification, 109
LoJack, 109
Numlock on/off, 108
Onboard Device Configuration, 108
passwords, 108
RAID, 240
SATA Configuration, 108
Secure Boot, 109
System Information, 107
Temperature Monitoring, 108
TPM, 109
USB Permissions, 108
Video options, 108
Virtualization Support, 109
Virus Protection, 108
Flash BIOS, 105
flashing, 112-113
functions, 104
M.2 SSD settings, 228
mSATA settings, 228
NVMe SSD settings, 228
on-board NIC, 569
overview, 104
POST, 104, 456-457
RAID configuration settings, 240
resetting, 112
resource conflicts, 114
ROM checksum error messages, 456
SATA
ports, 224
settings, 228
security, 873-874
Setup programs, 104-105
storage devices, configuring, 228
system boots from the wrong device, troubleshooting, 109
TPM considerations, 110
troubleshooting, 113
upgrading, 105
viruses, 112
BitLocker, 622, 903
BitLocker Drive Encryption, 623
BitLocker Recovery Password Viewer, 623
BitLocker To Go, 623, 903

bits. *See also* bytes
defined, 18
OSI model, 539
blackouts, 951
blank/black screens, troubleshooting, 90, 163, 271, 792-793
blocking ads, 379, 497
Bloom's Taxonomy, 440, 452
blue screens, 758. *See also* BSOD
Bluetooth, 55
Bluetooth cards, replacing, 404
Bluetooth & Devices Settings utility, Windows, 746
connectivity, 426-427, 519
device verification, 594
laptops, 374
M.2 slots, 218-219
mobile device connectivity, 373-374
PAN, 519
printers
access, 336
connectivity, 325
Blu-ray technology
disc drives. *See* optical drives
preventive maintenance, 287
region codes, 285
BMP files, 631
BNC connectors, 48
bollards, physical security, 863
bookmarks, web browsers, 493
Boot Camp, macOS, 834
boot manager, UEFI, 454
Boot Options setting (BIOS/UEFI), 107-108
boot orders, updating, 735
boot partitions, 234, 773
Boot Passsword setting (BIOS/UEFI), 108
boot passwords, 873
boot process, 614
"bootable device not found" error messages, 113, 248
bootloader, Linux, 840
bootrec command, 248, 670
bootrec /fixboot command, 773
bootrec /fixmbr command, 773
bootrec /scanos command, 773
boot sectors, 236
boot sector viruses, 878
boot volumes, 237, 772
bootups
Advanced Boot Options menu, Window, 776-777
Boot Camp, macOS, 834
boot partitions, 773
failures, troubleshooting, 247, 790-791
GRUB, finding, 854
"Invalid Boot Disk" error messages, 773
LILO, 854
multiboots, Windows, 723
network boots/PXE, 772
nonbootable disks/media, 791
preventive maintenance, 148
process, 453-454
PXE, 772
reboots, troubleshooting, 163
Safe Boot, 778
Safe Mode, 736
Secure Boot setting (BIOS/UEFI), 109
security, 873
System Configuration utility, Windows, 777-780
Task Manager, Windows, 782
troubleshooting
blank screen on bootup, 90
failures to boot, 247, 790-791
finding missing bootloaders, 854
graphical interfaces, 791
reboots, 163
resetting PC, 791
slow boot, 795
system boots from the wrong device, 109
warm bootups, 104, 460
Windows boot process
overview, 772
speeding up, 789-790
troubleshooting, 790-791
botnets, 879, 882
bps (bits per second), 481
breakout (network) tabs, 537
Bridged mode, virtual NIC, 570
bridges, wireless, 548
brightness, monitors/projectors, 275
broadband, 490, 587
broadcast addressing, 544, 987
broken screens, laptops, 408
brownouts, 951
browsers
ad blockers, 497
address bars, 6, 493
bookmarks, 493
clearing data, 494
configuration settings, 494-495
default browsers, 494
Edge tile, Windows Start screen, 628
extensions, 493-495
Firefox, 496-497
Google Chrome, 496-497
hashes, 492
history, 493
integrated searches, 493
Microsoft Edge, 496-497
Internet Options Control Panel settings, 494
settings, 493-494
password manager, 492
patching, 495
performance, 497-498
plug-ins, 493-495
pop-ups, 497
private browsing, 494
as proxy servers, 495
redirection, 496
refresh option, 493
rootkits, 496
Secure DNS, 495
security, 492-497
synchronizing, 495
tabs, 493
troubleshooting
basic issues, 496-497
degraded (slow) performance, 497-498
extensions, 495
plug-ins, 495
slow performance, 497-498
tools, 497
trusted sources, 492
untrusted sources, 492

updating, 496
verifying security certificates, 495
brushes, antistatic, 148
brute force attacks, 882
BSB (Back-Side Buses), 69-70
BSOD (Blue Screens of Death), 457, 758
troubleshooting, 247, 272
Windows updates, 793
Btrfs, 843
bubble jet printers. *See* inkjet printers
buffered memory, 181
buffers, data, 241
building customer trust (soft skills), 931
Built-in Diagnostics setting (BIOS/UEFI), 109
bulbs
backlight, 407, 421
CCFL, 407
projectors, 276
burning smells, troubleshooting, 90, 163
burn-in (screens), troubleshooting, 272
buses
BSB, 69-70
defined, 67
external data, 67
FSB, 69-70
HyperTransport, 70
internal data, 67
PCI, 69
PCIe, 69
performance, 68
speeds, 68
business processes, documentation, 964
buying
memory, 189
surge suppressors, 953
BYOD (Bring Your Own Device) policies, 385, 862
bytes, 19-20. *See also* bits

C

.CAB files, 631
cabinets, network, 535
cable connectors, 541
cable locks, security, 410, 865
cable modems, 44, 482-483, 581-582
cable testers, 530, 537
cable (wire) strippers, 529, 537
cabling
568A/B standard, 51
cable (wire) strippers, 529, 537
Cat 5, 49-50
Cat 5e, 49-50, 526
Cat 6, 49-50, 526
Cat 6a, 49-50, 526
Cat 7, 527
Cat 8, 527
coaxial, 48-49, 482
copper, 47, 526
corporate networks, 531-532
crimpers, 529-530, 537
crossover, 528
direct burial, 44, 526
DVI, 39
eSATA, 44
Ethernet, 50-51, 532
external, removing, 140
fiber networks, 51-52, 486-488
IDE, 142
internal, removing, 141-142
labeling, 533
Lightning, 37, 54
loopback plugs, 537
managing, 535, 942
modems, 480
multimeters, 537
multi-mode fiber, 52
network (breakout) taps, 537
network cabinets, 535
network racks, 535
patch cables, 528
patch panels, 531
pin 1, 142
plenum, 50, 527
PoE, 533
power cables, removing, 140
power supplies, 447-448
punchdown blocks, 50, 537-538
punchdown tools, 50, 537-538
PVC, 51, 527
RJ45 wall jacks, 532
SAS, 222
SATA, 223
serial, 44
single-mode fiber, 52
STP, 50, 526-527
straight through, 528
T568A wiring standard, 51, 528
T568B wiring standard, 528
tangs, 527
testers, 530, 537
Thunderbolt, 36-37, 54
tone generators, 537
toner probes, 537
twisted pair, 526-532
USB, 32
UTP, 49-50, 526-530
VGA, 39
video connections, troubleshooting, 271
caches, 241-243
clearing, 494
L1, 69
L2, 69
L3, 69
memory, 69, 178
threads, 71-72
CAD/CAM/graphic workstations, 441
calendars, mobile device synchronization, 381
calibrating
inkjet printers, 320
laser printers, 323
touch, trackpads, 421
cameras
smart cameras, 359
webcams, 17, 290-291, 362, 407-410, 868-869
canned air, 148-150
capacitors, 90, 151
capitalization, commands, 657
CAPS LOCK key, 16
captures, screen, 7
card readers, memory, 199, 361

cards
Bluetooth cards, replacing, 404
cellular cards, laptops, 389
emulation, NFC, 377
expansion cards, laptops, 389-391
M.2 expansion cards, 390
miniPCIe cards, 389
NIC
advanced properties, 568-569
configuring, virtualization, 569-570
duplexing, 569
on-board NIC (BIOS/UEFI), 569
QoS, 569
speed, 569
troubleshooting, 579-581
virtual NIC, 569-570
Wake on LAN, 569
Windows network settings, 592-594
wireless NIC, 548-549, 567-568
NVMe cards, 391
sound cards, system design, 450
vCards (VCF), contact synchronization, 382
wireless cards, 389, 404
carriages, inkjet printers, 306
cars, mobile device synchronization, 381
cartridges (ink), inkjet printers, 320
cases
airflow, 157
fans, 157
form factors, 154
matching motherboard form factors with, 89
opening (disassembly), 141
standoffs, 145
system design, 447-448
types of, 154
ventilation, 157
Cat 5 cables, 49-50
Cat 5e cables, 49-50, 526
Cat 6 cables, 49-50, 526
Cat 6a cables, 49-50, 526
Cat 7 cables, 527
Cat 8 cables, 527
cause, theories of probable, 453
CCFL bulbs, 407
cd command
macOS, 835-836
Windows, 659-660, 671
CD (Compact Discs), preventive maintenance, 287
CD drives. *See* optical drives
CDMA (Code Division Multiple Access), 367
cell phones. *See* smartphones
cell tower analyzers, 387
cellular cards, laptops, 389
cellular data, mobile device connectivity, 379
cellular location services, 369, 370
cellular networks, 366-367, 490
certificate-based credentials, 759
Certificate Manager, 907
certificates
certificates of destruction, 869
digital security certificates, 906
certifications
CompTIA Core 1 (220-1201) A+ certifications, 5
CompTIA Core 2 (220-1202) A+ certifications, 5
CFX12V power supplies, 154
change boards, 964
change management
assessment phase, 965-966
cycle of, 965
design phase, 966
documenting changes, 123, 966
emergency changes, 965
evaluation phase, 966
freezes, 964
implementation phase, 966
normal changes, 965
permissions, 893
purpose of change, 965
risk analysis, 965
risk levels, 965
scope of change, 966
standard changes, 965
changing
default administrator account passwords, 885
documenting changes, 123, 966
hard drive letters, 767
IP addresses, 560
one thing at a time (soft skills), 123
permissions, 891
troubleshooting perspectives (soft skills), 713-714
update settings, Windows, 740
usernames/passwords, 570
channel ID, wireless networks, 553-556, 571
characters (passwords), number of, 874
charging
batteries, troubleshooting, 424
laptops, improper charging, 392
laser printers, imaging process, 310
USB ports, 34
checkboxes, Windows, 630
checking power supply voltages, 163
checkpoints/snapshots, VM, 501
child accounts, 884
child exploitation, security, 929
chipsets, system design, 447
chkdsk command, 246, 671-672
chkntfs command, 672
chmod command, macOS, 835-838
choosing
microphones, 280-281
power supplies, 161-162
speakers, 282
chown command, macOS, 835-837
Chrome, Google, 360, 496-497, 619
CIDR (Classless Inter-Domain Routing), IP addressing, 546
CIFS (Common Internet File System) protocol, 583, 589
cipher command, 672-673
circuit testers, AC, 164
CIS (Continuous Ink Systems), 317
clamping voltage, 952
clarifying customer statements, 2
classes, IPv4 addressing, 543
clean installations, Windows, 723
cleaning
blades, laser printers, 311
discs, 287
displays, 148

gold contact cleaners, 148
heating elements, thermal printers, 324
keyboards, 15
laser printers, 311, 323
lens cleaners, 148
mouse/mice, 15
optical drives, 148
printheads, inkjet printers, 321
scanners, 289
cleaning phase, laser printer imaging process, 310
cleansers, general-purpose, 148
clearing
browser data, 494
caches, 494
CMOS, 113
logs in Event Viewer, 759
paper jams, 339
TPM, 110
clicking sounds, troubleshooting, 247, 286
CLI (Command-Line Interface), Linux, 845, 848-849
client-side DHCP, 562
client-side DNS, 566
clocks
activation clocks, 734
drift, troubleshooting, 750
speeds, 69
cloned partitions in Disks, 852
Close button, Windows, 629
closing
apps, troubleshooting closure failures, 418
command prompt, 676
cloths, cleaning, 148
cloud computing
advantages of, 507-508
apps, 505
availability, 507
collaboration tools, 806-807
community clouds, 507
concept of, 503
corporate focus, 507
DaaS, 504
dedicated resources, 508
deploying services, 506-507
egress data rates, 508
elasticity, 507
email systems, 804-805
file storage, 505
hybrid clouds, 506
IaaS, 504
iCloud, 384-385, 822
ingress data rates, 508
mobile device synchronization, 381
multitenancy, 508
network controllers, 505-506
off-site email apps, 505
OneDrive, 722
PaaS, 504
printing, 337-338
private clouds, 506
productivity tools
collaboration tools, 806-807
email systems, 804-805
storage, 805-806
public clouds, 506
SaaS, 504
scanning, 337-338
services, 337
deploying, 506-507
metered utilization services, 508
service rates, 508
shared resources, 507
storage, 214, 381, 805-806, 900. *See also* synchronizing
streaming virtual apps, 505
CL ratings, 189
cls command, 673
clusters
lost clusters, 243
NTFS file systems, 231
CMDB (Configuration Management Databases), 963
cmdlets, 712
CMOS (Complementary Metal-Oxide Semiconductors)
batteries, 110
clearing, 113
error messages, 456, 457
ESCD, 116
jumpers, 112
memory, 110
CNAME records, DNS, 565
coaxial cables, 48-49, 482
collaboration tools, cloud-based, 806-807
collating pages, 330
collection-controlled loops. *See* for loops
colons (:) in comments, 704
color
appearance (soft skills), 429
audio ports, 278
gamut, displays, 266
incorrect colors (screens), troubleshooting, 271
inkjet printers, 307, 346
COM files, 631
command command, 673
command-line interface, 615
[command name] /? command, 668
command prompts
accessing, 656
appearance of, 657
attrib command, 665, 669
bcdedit command, 669-670
bootrec command, 670
cd command, 659-660, 671
chkdsk command, 671-672
chkntfs command, 672
cipher command, 672-673
closing, 676
cls command, 673
command command, 673
[command name] /? command, 668
copy command, 664-665, 673
defrag command, 673
del command, 663, 674
dir command, 660-662, 669, 674
directories
naming, 657
navigating, 659-663
root directories, 657
subdirectories, 657
disable command, 675
diskpart command, 675
dism command, 675
drive letters, 657
drive navigation inputs, 669
dxdiag command, 675-676
enable command, 676

INDEX

exit command, 676
expand command, 676
explorer command, 677
files
backslashes (\) in file structures, 659
naming, 657
organizing, 657
tree structure, 657-659
formatting commands, 657, 677
full paths in, 663
gpresult command, 677
gpupdate command, 678
help command, 668, 678
hostname command, 678
ipconfig command, 678-679
md command, 662-663, 679
mkdir command, 662-663, 679
mmc command, 679
more command, 680
msconfig command, 680
msinfo32 command, 680
mstsc command, 680
nbtstat command, 681
net command, 681
netdom command, 682
netstat command, 683
net use command, 681
net user command, 682
notepad command, 683
nslookup command, 683
overview, 656
pathping command, 684
ping command, 684-685
PowerShell, opening, 666
rd command, 663, 685
regedit command, 685
regsvr32 command, 685
ren command, 686
rmdir command, 663, 685
robocopy command, 664-665, 686
services.msc command, 686
set command, 687, 698
sfc command, 687
shutdown command, 688
systeminfo command, 688
taskkill command, 689
tasklist command, 689
telnet command, 689
tools, starting with commands, 666
tracert command, 690
type command, 664, 690
wbadmin command, 690
whoami command, 690-691
Windows, 656
winver command, 691
wscript command, 691
xcopy command, 664-665, 691-692
commands
administrative privileges, 656
attrib command, 665, 669
bcdedit command, 669-670
bootrec command, 670
bootrec /fixboot command, 773
bootrec /fixmbr command, 773
bootrec /scanos command, 773
capitalization, 657
cd command, 659-660, 671
chkdsk command, 671-672
chkntfs command, 672
cipher command, 672-673
cls command, 673
command command, 673
[command name] /? command, 668
common commands list, 667-668
convert command, 730
copy command, 664-665, 673
defrag command, 673
del command, 663, 674
dir command, 660-662, 669, 674
disable command, 675
diskpart command, 675
dism command, 675
drive navigation inputs, 669
dxdiag command, 675-676
enable command, 676
exit command, 676
expand command, 676
explorer command, 677
format command, 677
formats of, 657
formatting, 668
gpedit.msc command, 889
gpresult command, 677
gpupdate command, 678
help command, 668, 678
hostname command, 678
ipconfig command, 678-679
learning, 666
Linux commands
apt command, 845, 848-849
dd command, 845, 849-852
df command, 845
fsck command, 845
ifconfig command, 846
ip command, 845-847
iwconfig command, 845
iwlist command, 847
locate command, 845, 853
mount command, 845
passwd command, 845-846
ps command, 845-848
shutdown command, 845-846
su command, 845
sudo command, 846
top command, 845
updatedb command, 845, 853
macOS commands
cd command, 835-836
chmod command, 835-838
chown command, 835-837
cp command, 835-836
grep command, 835, 838
kill command, 835
less command, 835, 838
ls command, 835
man command, 835, 839
mkdir command, 835
mv command, 835-836
nano command, 835, 838
pwd command, 835-836
rm command, 835-836
su command, 835
sudo command, 835-836
touch command, 835-836
vi command, 835
md command, 662-663, 679
mkdir command, 662-663, 679
mmc command, 679
more command, 680
msconfig command, 680
mskinfo32 command, 680
mstsc command, 680, 801
nbtstat command, 681
net command, 681

netdom command, 682
netstat command, 683
net use command, 681
net user command, 682
notepad command, 683
nslookup command, 683
output, multiple pages, 662
pathping command, 684
periods (.) in commands, 661
ping command, 684-685
rd command, 663, 685
reasons for learning, 666
regedit command, 685
regsvr32 command, 685
regsvr32.exe command, 754
ren command, 686
rmdir command, 663, 685
robocopy command, 664-665, 686
services.msc command, 686, 794
set command, 687, 698
sfc command, 687
shutdown command, 688
standard (user) privileges, 656
starting tools with, 666
switches, 661-662
systeminfo command, 688
taskkill command, 689
tasklist command, 689
telnet command, 689
tracert command, 690
two periods (..) in commands, 661
type command, 664, 690
usage considerations, 665
wbadmin command, 690
whoami command, 690-691
wildcards, 664
WinRE limited commands, 662
winver command, 691
writing, 666
wscript command, 691
xcopy command, 664-665, 691-692

comments
colons (:), 704
hash characters (#), 703-704
quotation marks (“ “), 703
slashes (//), 703
within scripts, 703

commercial licenses, 876
commitments (soft skills), making/keeping, 972
common commands list, 667-668
common ports, list of, 53
common scripting languages, 693
communication skills
phone, 252-253
written, 166

community clouds, 507
comparison (equality) operators, 705
compatibility
apps and OS, 751
backward compatibility, 621
device drivers, installing, 749
forward (upward) compatibility, 621
software, 621
Windows, 727
Compatibility mode, 195
hardware/software, 725
older apps, 195

compiled programs, 692
complexity of passwords, 874
compliance
OS, 620
policies, 964
regulatory compliance, security policies, 863

component handling/storage, safety, 949-950
Component/RGB video ports, 274
Component Services, 755
compound conditions, 708
compressed air, 148-150, 945
compression, files/folders (Windows), 639
CompTIA Core 1 (220-1201) A+ certifications, 5
CompTIA Core 2 (220-1202) A+ certifications, 5
Computer Management console, Windows, 754
Disk Management tool, 765-767
Local Users and Groups tool, 762-764
ODBC Data Sources tool, 770
Print Management console, 771
Services and Applications section, 769
Storage Spaces Control Panel, 768
System Tools section
Event Viewer, 756-758
Shared Folders tool, 759
Task Scheduler, 755

User Account Management section, 759

computers
design
audio subsystems, 449-450
audio/video workstations, 442
Bloom’s Taxonomy, 440
cases, 447-448
chipsets, 447
cooling systems, 447
CPU, 447
display subsystems, 450-451
environment concerns, 446
gaming PC, 441
graphic/CAD/CAM workstations, 441
home servers, 445-446
memory, 447
motherboards, 447
NAS devices, 443
overview, 440
power supplies, 447-448
processors, 447
recycling components, 446
storage subsystems, 449
thick client workstations, 445
thin client workstations, 444
virtualization workstations, 443

domains, adding to, 566-567
enclosures, 957
locking, 885
naming, 559
types of, 8
workstations
audio/video workstations, 442
graphic/CAD/CAM workstations, 441
thick client workstations, 445
thin client workstations, 444
virtualization workstations, 443

concurrent users (share permissions), maximum number of, 892
conferencing features, displays, 451
confidence (soft skills), projecting, 200, 969
confidential/private materials (soft skills), dealing with, 974
configuration files, Linux, 840
configuring
  ACPI setting (BIOS/UEFI), 109
  alternative IP addresses, 563
  BIOS
    configuration settings, 107
    Flash BIOS, 105
    flashing, 112-113
    functions, 104
    overview, 104
    POST, 104
    resetting, 112
    resource conflicts, 114
    Setup programs, 104-105
    storage devices, 228
    troubleshooting, 113
    upgrading, 105
    viruses, 112
  browsers, 494-495
  CMDB, 963
  CMOS, 110
  cores, 72
  CPU Configuration setting (BIOS/UEFI), 108
  DHCP, 562
  email, mobile devices, 379-380
  end devices, IP addressing
    alternative IP address configurations, 563
    APIPA, 563
    default gateways, 564-565
    DNS, 565-566
    static configurations, 560-561
  ESCD, 116
  firmware, updating, 112-113
  hardware, 115-116
  I/O addresses, 114
  IP addresses, alternative, 563
  IRQ, 114
  manufacturer's advice, ignoring, 117
  memory addresses, 114
  mobile devices
    email, 379-380
    network configurations, 376
  networks
    ifconfig command, Linux, 846
    mobile device configurations, 376
    troubleshooting, 122
  NIC, virtualization, 569-570
  profiles, 385, 922
  RAID, 238-240
  SATA Configuration setting (BIOS/UEFI), 108
  static IP addresses, 560
  storage devices, 222
  System Configuration utility
    msconfig command, 680
    Windows, 777-780
  system resources, 113-114
  UEFI
    advanced menu, 107
    configuration settings, 107
    flashing, 112-113
    main menu, 106
    resource conflicts, 114
    Setup, 105-106
    storage devices, 228
  USB devices, 117-118
  VPN, 919-920
  Windows, 741-743
  wireless AP, 570
  WWAN, 572
connection-oriented protocols, TCP/IP, 590
connectionless protocols, UDP, 590
Connections tab (Internet Options Control Panel), 494
connectivity
  20 + 4 connectors, 142
  20-pin motherboard connectors, 155
  24-pin motherboard connectors, 142, 155
  adapters
    DVI-to-HDMI, 42
    integrated motherboard ports, 53
  ATX power supply connectors, 154, 157
  audio subsystems, 450
  Bluetooth, 426-427, 519
  cabling, 541
    568A/B standard, 51
    Cat 5, 49-50
    Cat 5e, 49-50
    Cat 6, 49-50
    Cat 6a, 49-50
    coaxial, 48-49
    copper, 47, 526
    direct burial, 50, 526
    DVI, 39
    eSATA, 44
    fiber, 51-52
    Lightning, 37, 54
    multi-mode fiber, 52
    plenum, 50
    punchdown blocks, 50
    punchdown tools, 50
    PVC, 51
    serial, 44
    single-mode fiber, 52
    STP, 50
    T568A standard, 51, 528
    Thunderbolt, 36-37, 54
    USB, 32
    UTP, 49-50
    VGA, 39
  cellular networks, 490
  connectors. *See* individual entry
  converters
    USB-to Ethernet, 35
    USB-to-serial port, 46
  dial-up Internet connectivity, 480-482
  EoP, 534
  hubs, 33
  intermittent connectivity, troubleshooting, 425-426, 558, 574-576
  internal connectors, removing, 141-142
  Internet. *See also* mobile connectivity
    cable modems, 482-483
    dial-up connectivity, 480-482
    fiber networks, 486-488
    modems, cabling, 480
    modems, dial-up connectivity, 480-482
    overview, 480
    satellite modems, 488-489
    troubleshooting, 425, 574-576

VoIP, 484-486
xDSL modems, 483-484
IR, mobile devices, 379
keyboards, 54
limited/intermittent connectivity, troubleshooting, 574-576
local connectivity, 575
metered connections, 591
mobile connectivity *See also* Internet, connectivity
cellular networks, 490
hotspots, 489
licensed ranges, 490
long-range fixed wireless, 490
overview, 489
power requirements, 491-492
synchronization, 382
tethering, 489
unlicensed ranges, 491
WAN, 490
wired connectivity, 371-373
wireless connectivity, 373-379, 490
WISP, 490
motherboards
20-pin motherboard connectors, 155
24-pin motherboard connectors, 155
ATX power supply connectors, 154, 157
front panel connectors, 142
pins, 143
power supplies, 153
netstat command, 588
networks
cable management systems, 535
cabling cabinets, 535
cabling racks, 535
direct burial cables, 526
EoP, 534
netstat command, 588
PoE, 533
twisted pair cables, 526-532
unintentional connections, troubleshooting, 426
ODBC Data Sources tool, 770
PCI expansion slots, 83
PCIe
adapters, 86
expansion slots, 84-85
lanes, 85
pin 1, cables, 142
ping command, 684-685
ports
audio ports, 43, 54
charging USB, 34
common ports list, 53
DB9, 44, 54
defined, 30
DP, 40, 54
DVI ports, 39, 54
DVI-A ports, 54
DVI-D ports, 54
eSATA ports, 43-44, 54
Ethernet, 46-47
HDMI ports, 41, 54
installing extra ports, 36
integrated motherboard, 53
keyboard, 30
Lightning, 37, 54
matching monitors to port type, 40
microUSB, 33
miniUSB, 33
mouse/mice, 30
multipurpose ports, 37-38
network, 46
PS/2 mouse, 5
RJ11, 44, 54
RJ45, 46, 50, 54
RS-232, 44
S/PDIF ports, 43, 54
serial ports, 44
sleep-and-charge USB ports, 34
S-Video ports, 40
Thunderbolt, 36-37, 54
USB, 31-32, 54
USB 2.0, 31
USB 3.0, 31
USB 4.x, 31
USB-C, 37
USB connectors, 32
USB hubs, 33
USB-to-Ethernet converters, 35
USB-to-serial port converters, 46
VGA ports, 39, 54
video ports, 38-42, 54
power connectors, video cards, 267
power supplies, motherboards, 153
printers, 332-333, 344-345
Bluetooth, 325
troubleshooting, 339
USB, 325-326, 342
Windows environments, 342-343
wired networks, 325
wireless networks, 325, 334-335
processors, 70
projectors, 275
RJ11, 54
RJ45, 46, 50, 54
SAN, 524
SATA, 141, 220-221
scanners, 289
snug connectors, 142
sound card ports, 279
sound cards, 277
S/PDIF ports, 43, 54
SSH, 589
troubleshooting, 574-576
twisted pair cables
corporate networks, 531-532
RJ45 connectors, 527
STP cables, 526
terminating, 527-530
UTP cables, 526-527
USB hubs, 33
video cables, troubleshooting, 271
wired connectivity
device connectivity, 559
Ethernet, projectors, 275
mobile devices, 371-373
wireless connectivity
Bluetooth, 55
desktop workstations, 547
device connectivity, 559
IR, 55
mobile devices, 373-379
NFC, 55
presenters, 55
projectors, 275
radio, 55

troubleshooting, 425-426
wireless broadband, 490
connectors
BNC, 48
dual Molex-to-PCIe converters, 156
DVI, 39
front panel, 142
F-type, 48
LC, 51
Molex-to-SATA converters, 156
RJ11 connectors, 527-530
RJ45 connectors, 527-530
SC, 51
ST, 51
USB-C, 32
USB Type-A, 32
USB Type-B, 32
USB Type-C, 32
Wi-Fi antenna connectors, 405
consequences of scripting, mitigating, 695
Console, macOS, 831
constructs, scripting, 704
contact cleaners, gold, 148
contacts, synchronization
mobile devices, 381
vCards (VCF), 382
containers, 503
content filtering, 571, 920
Content tab (Internet Options Control Panel), 494
Content view, Windows File Explorer, 634
context menus, Windows, 630
context-sensitive help, Windows, 630
continuity checks, 152-153
continuous reboots, troubleshooting, 90
contrast ratios, displays, 451
controllers, cloud-based network, 505-506
Control Panel, Windows, 641
control plane, SDN, 586
convergence, 484
convert command, 730
converters
dual Molex-to-PCIe converters, 156
Molex-to-SATA converters, 156
USB-to-Ethernet, 35
USB-to-serial port, 46
converting
MBR to GPT, 235
partitions, 231
cooling
batteries, 393
CPU, 77, 81
fans, 77, 108, 157
heat sinks, 77, 81
laser printers, 323
Li-ion batteries, 393
liquid, 77
overclocking, 80
phase-change, 77
processors, 77-78, 81
system design, 447
thermal pads, 77
thermal paste, 77-78, 81
vapor, 77
copper cables, 47, 526
copy command, 664-665, 673
copying
data, Linux, 849-852
directories, 664-665
files, 664-665, 686
files/directories, 691-692
in NTFS permissions, 895
Shadow Copy technology, 737
Windows files/folders, 640
cores
configuring, 72
Core 3 processors, 74
Core 5 processors, 74
Core 7 processors, 74
Core 9 processors, 74
Core Ultra x processors, 74
multicore processors, 71
number of, determining, 72
corporate focus, cloud computing, 507
corporate networks
cabling, 531-532
disk imaging, 733
Windows deployments, 733-734
corporate OS, 621
AD, 622
domains, 622
encryption, 622-623
RDP, 622
security, 622-623
workgroups, 622
corruption/data loss, troubleshooting, 245
costs
cloud storage, 805
operating costs, OS, 620
covers
levering, 394
slot covers, replacing, 139
cp command, macOS, 835-836
CPU (Central Processing Units). *See also* processors
cooling, 77, 81
CPU Configuration setting (BIOS/UEFI), 108
fans, 82
handling, 79
heat sinks, 81
installing, 79-81
OS requirements, 751
photographing prior to installations/upgrades, 81
retention plates, 78
sockets, 76
speeds, 69
system design, 447
thermal paste, 81
thermal solutions, 81
throttle management, 80
throttling, 69
troubleshooting, 83
upgrading, 80
CPU tab, Task Manager, 786
crashing apps, troubleshooting, 90, 195, 457, 757, 782
Credential Manager, 759-762
credentials
backups, 760
certificate-based credentials, 759
generic credentials, 759
storing, 760
web credentials, 759
Windows credentials, 759
adding, 760
editing, 762
removing, 761

crimpers, 529-530, 537
cross platform virtualization, 498
cross-site scripting (XSS) attacks, 883
crossover cables, 528
cryptojacking/cryptomining, 879
cultural sensitivity (soft skills), 970
current directory (.), 668
current (soft skills), staying, 647
current, voltage, 152-153, 537
cursor drift, troubleshooting, 421
customers (soft skills)
  active listening, 92-93
  difficult customers, dealing with, 467-468, 972-973
  service, 967
  statements, clarifying, 2
  trust, building, 931
Custom mode, virtual NIC, 570

D

DaaS (Desktop as a Service), 499, 504
damaged ports, troubleshooting, 415
dark displays, troubleshooting, 792
dash, Linux, 841
data
  backups, Windows, 644, 740-741
  buffers, 241
  caps, 379-381
  files, partitioning, 231
  gathering, 695
    Internet searches, 6-7
    troubleshooting process, 451
  loss/corruption
    OS update limitations, 620
    troubleshooting, 245
  packets, tracert command, 690
  privacy, 337-338
  at rest, 903
  recovery, in-place/overwrite solutions, 902
  SATA cables, 223
  security
    account recovery, 902
    AES, 903
    AutoPlay, disabling, 904
    AutoRun, disabling, 904
    backups, 899-902
    BitLocker, 903
    BitLocker To Go, 903
    data at rest, 903
    device encryption, 903
    EFS, 904
    EOL, 898
    hard drives, storage, 904
    patch management, 898
    restores, 899-902
    unknown notifications, 898
    unprotected systems, 898
    update management, 898
  transfer speeds, wireless networks, 559
  types, 701
  usage, limit notifications, 414
Data Link layer (OSI model), 540
data plane, SDN, 586
data sources (projectors), troubleshooting, 275
databases
  ODBC Data Sources tool, 770
  servers, 584
dates/times (inaccurate), troubleshooting, 111
DB9 ports, 44, 54
DBR (DOS Boot Records), 236
DC (Direct Current), 150-151, 157
DC jacks, replacing, 406
dd command, Linux, 845, 849-852
DDOS (Distributed DOS) attacks, 882
DDR (Double Data Rates), memory, 179-180
dead pixels (screens), troubleshooting, 271
dealing with difficult customers (soft skills), 467-468
decision (selection) structures, 704-708
declaring variables, 701
dedicated cloud-computing resources, 508
dedicated graphics cards, 751
default browsers, 494
default gateways, 564-565
default printers, 328
defrag command, 673
defragmenting
  hard drives, 244, 769
  SSD, 245
degaussing hard drives, 905
degraded (slow) performance, troubleshooting, 423
  browsers, 497-498
  mobile devices, 411
del command, 663, 674
deleting. *See also* removing
  AD accounts, 888
  apps, 418, 419
  files, 628, 663, 674
    manually, 909
    recovering deleted files, macOS, 826
  partitions, 234
  removable media files, 628
Dell computers, POST audio beeps, 455
denatured alcohol, 148
density control blades, laser printers, 311
density (pixel), displays, 265
deny lists, 913
DEP (Data Execution Prevention), 617
deploying
  images, Windows, 723
  tools, 734
  Windows, 733-734
design, computer
  Bloom's Taxonomy, 440
  overview, 440
  system design, 442-445
    audio subsystems, 449-450
    cases, 447-448
    chipsets, 447
    cooling systems, 447
    CPU, 447
    display subsystems, 450-451
    environment concerns, 446
    gaming PC, 441
    home servers, 445-446
    memory, 447
    motherboards, 447
    NAS devices, 443
    power supplies, 447-448
    processors, 447
    recycling components, 446
    storage subsystems, 449
  wireless networks, 550

workstations
audio/video workstations, 442
graphic/CAD/CAM workstations, 441
thick client workstations, 445
thin client workstations, 444
virtualization workstations, 443
design phase, change management, 966
desk controllers, projectors, 275
desktops
DaaS, 504
icons, sizing, 623-634
macOS. *See* individual entry
malware alerts, 880
mobile device synchronization, 381
RDP, 589
remote desktops
Remote Assistance, 801-803
Remote Desktop Connection, 801-803
RDP, 918
starting, 680
user accounts, 885
virtual desktops, 504
virtualization, 499
Windows 10. *See* individual entry
Windows 11. *See* individual entry
workstations, wireless connectivity, 547
Desktop tile, Windows Start screen, 628
destroying hard drives, 905
destruction, certificates of, 869
Details tab, Task Manager, 784
Details view, Windows File Explorer, 634
developer mode, Android OS, 371
developing phase, laser printer imaging process, 310
device drivers, 8, 743
installing, 745-749
rolling back, 748
signed drivers, 745-746
troubleshooting, 748
device encryption, 414, 903
device failures (random), troubleshooting, 459-460
Device Manager, 743-746
accessing, 114
hardware, verifying, 122
undetected/nonfunctioning devices, troubleshooting, 747-748
Devices setting (BIOS/UEFI), 108
df command, Linux, 845
dGPU (Discrete GPU), 267
DHCP (Dynamic Host Configuration Protocol), 562, 571, 584, 589
diagnostics
Built-in Diagnostics setting (BIOS/UEFI), 109
POST cards, 457
UEFI, 458
diagonal cutters, 139
diagrams, network topology, 960
dialog boxes, Windows, 629-630
dial-up networks, 480-482
dictionary attacks, 874, 882
differential backups, 900
difficult customers (soft skills), dealing with, 467-468, 972-973
digital meters, 152
digital security certificates, 906
digital signals, video ports, 38
digital signatures, 745-746
digitizers, 291
laptops, 407
replacing, 273
dimness, troubleshooting
images, 271
screens, 421
DIMM (Dual In-line Memory Modules)
advertisements, 189
installing, 191
models of, 181
physical packaging, 178-179
removing, 190
SODIMM, 178-179, 400
solutions, 188
dir command, 660-662, 669, 674
direct burial cables, 50, 526
directional antennas, 556
directories
attributes, handling, 665
cd command, 671
copying, 664-665, 691-692
current directory (.), 668
LDAP, 589
making, 662-663
md command, 679
mkdir command, 679
naming, 657, 686
navigating with command prompt
cd command, 659-660
dir command, 660-662
md command, 662-663
mkdir command, 662-663
rd command, 663
rmdir command, 663
parent directory (..), 668
removing, 663, 685
renaming, 686
root directories, 657
services, 870
subdirectories, 657, 663
DirectX optical drives, 287
disable command, 675
disabling
apps, 780
AutoPlay, 904
AutoRun, 904
browser plug-ins/extensions, 495
guest accounts, 890
interfering software from OS installations, 732
motherboards for sound card installations, 279
ports, 871
services, 794
startup programs, Windows, 791
disassembly
adapters, removing, 143
all-in-one computers, 146
cases, opening, 141
EMI, 138
equipment grounding, 136
ESD
antistatic tools, 136-138
self-grounding, 138
SSD, 144

external cables, removing, 140
hard drives, removing, 144
internal cables/connectors, removing, 141-142
motherboards, removing, 145
overview, 136
power cables, removing, 140
power supplies, 164
process (overview), 140
RFI, 138
steps of (overview), 140
storage devices, removing, 144
tools, 136-139
disc drives, mounting, 751
discs, cleaning, 287
Disk Cleanup tool, 244, 768
disk striping (RAID 0), 239
Disk Utility, macOS, 833, 834
diskpart command, 675
diskpart utility, partitioning hard drives, 230-232
disks. *See also* hard drives
caches, 241-243
imaging, 733
maintenance, 244, 768-769
management
basic disks, 236
basic storage, 236
boot volumes, 237
concepts, 237
Disk Management tool, 765-767
Disks, Linux, 842, 852
Disk Utility, macOS, 833-834
dynamic disks, 237
dynamic storage, 236
partitioning hard drives, 230-232
RAW volumes, 237
simple volumes, 237
spanned volumes, 237
striped volumes, 237
system volumes, 237
Windows, 232, 236-237
mirroring (RAID 1), 239
quotas, NTFS, 232
striping (RAID 0), 239
dism command, 675
displaying
.bat files, 664
.txt files, 664
variables, 687, 698
DisplayPort, 389
displays
aspect rations, 450
audio, troubleshooting, 272
autorotating, 421
black/blank screens, troubleshooting, 792-793
brightness, 275
broken screens, 408
BSOD, 457, 758
troubleshooting, 247, 272
Windows updates, 793
cleaning, 148
color gamut, 266
conferencing features, 451
contrast ratios, 451
defined, 9
digitizers, replacing, 273
dim displays, troubleshooting, 421
disposal procedures, 273
energy efficiency, 162
flickering displays, troubleshooting, 422
installing, 40
inverters, 407-409
laptops, 389, 407
LCD, 264-265, 272
LED, 264
lumens, 275
matching to port type, 40
mini-LED, 264
monitor wipes, 148
multi-monitor taskbars, 722
multiple displays, 722, 747
no display, troubleshooting, 421
number of, system design, 450
OLED, 264
orientation, 747
pixel density/pitch, 265
privacy screens, physical security, 866
rearranging, 746
refresh rates, 265, 747
replacing, 408
resolution, 275, 409, 747
screen resolution, 266
screen savers, 162
settings, 746-747
sharing, macOS, 823-824
subsystem design, 450, 451
timeouts/screen locks, 890
touch screens, 266, 273, 407
troubleshooting, 271
audio, 272
autorotation failures, 421
backlight failures, 421
black/blank screens, 792-793
BSOD, 758
digitizers, 273
dim displays, 421
flickering display, 422
no display, 421
touch screens, 273
types of, 450
video adapters, 451
wipes, 148
disposal
aerosol cans, 149
documentation, 869
electronics, 946-948
e-waste, 946
monitors, 273
toner, 948-949
distorted images, troubleshooting, 271
distractions (soft skills), avoiding, 971-972
distros (distributions), Linux, 839
DKIM (Domain Keys Identified Mail), 911
DLL (Dynamic Link Libraries), 631, 754
DLP (Data Loss Prevention) policies, 899
DMARC (Domain-based Message Authentication, Reporting, and Conformance), 912
.dmg files, 824
DMZ (Demilitarized Zones), 571, 913, 924
DNAT (Destination NAT), wireless networks, 571

DNS (Domain Name Systems), 589
A records, 565
AAAA records, 565
client-side DNS, 566
CNAME records, 565
Internet security, 909-910
MX records, 565
name resolution, 566
nslookup command, 683
OpenDNS, 909-910
Secure DNS, 495
secure DNS, 910
servers, 584, 840
TXT messages, 911
TXT records, 565
troubleshooting, 909, 910
.DOC (.DOCX) files, 631
Dock, macOS, 819-820
docking stations, 362-363, 389
document feeders (ADF), 302
documentation
ADF, 17
AI, 961
asset management, 963
AUP, 964
business processes, 964
certificates of destruction, 869
change documentation, 966
changes, 123
digitizers, 291
disposal, 869
documenting outcomes, troubleshooting process, 463
FACTA, 869
FERPA, 869
incident reports, 942, 962
inventory management, 963
knowledge bases/articles, 961
memory, 182, 188
MNDA, 875
motherboards, 182, 188
MSDS, 149, 943
NDA, 875
network topology diagrams, 960
new user/exiting user checklists, 960
operational procedures, 942
password policies, 963
policies, 964
proof of incineration, 869
proof of recycling, 869
regulatory/compliance policies, 964
rollback plans, 966
screen captures, 7
SDS, 149
security, 869, 964
sensitive material, 302
shredding documents, 869
SLA, 960
SOP, 959
SOW, 966
student records, 869
text files, 7
written communication skills, 166
domain controllers, 566-567, 622
domains, 521-523, 733
access, 622
adding computers to domains, 566-567
CompTIA Core 1 (220-1201) A+ certifications, 5
CompTIA Core 2 (220-1202) A+ certifications, 5
corporate OS, 622
joining, 886
dongles, 751
door locks, physical security, 863
DoS (Denial-of-Service) attacks, 882
dot matrix printers. *See* impact printers
double images (printing), troubleshooting, 347
double-sided printing (duplexing), 330
double-tap actions (mobile devices), 365
downloading
software packages, 849
Ubuntu, 840
downstream/upstream data, fiber networks, 487
DP (DisplayPorts), 40, 54
DPI (optimized), inkjet printers, 305-307
draft mode, inkjet printers, 306
DRAM (dynamic RAM), 178-180
drawing pads, 358, 363-364
dress codes (soft skills), 428-429
drift, clock, 750
drifting cursors, troubleshooting, 421
drilling hard drive platters, 905
drive activity LED, 246
drive arrays, RAID
"array missing" error messages, 251
BIOS/UEFI configuration settings, 240
configuring, 238
failures, 251
fault tolerance, 238-240
FCM, 239
hardware RAID, 240
hot swappable RAID drives, 240
levels of, 239-240
RAID 0, 239
RAID 0+1, 239
RAID 1, 239
RAID 5, 239
RAID 6, 239
RAID 10, 239
"RAID not found" error messages, 251
software RAID, 239
troubleshooting, 251
Drive Encryption setting (BIOS/UEFI), 109
drivers, 116
load alternate third-party drivers, 731
OS update limitations, 620
Windows installations, 731
drivers, device, 8, 743
installing, 745-747
in compatibility mode, 749
manually, 748
rolling back, 748
signed drivers, 745-746
troubleshooting, 748
drives
hard drives, 10. *See also* disks
2.5-inch, 215
3.5-inch, 215
arrays, adding, 767
basic disks, 236
BitLocker Drive Encryption, 623
boot sectors, 236

changing drive letters, 767
clusters, 231, 243
DBR, 236
defragmenting, 244, 769
degaussing, 905
destroying, 905
disk caches, 241-243
disk mirroring (RAID 1), 239
disk striping (RAID 0), 239
drive activity LED, 246
"drive not recognized" error messages, 246
dynamic disks, 237
encryption, 109, 903
external hard drives, 389, 402, 772
fault tolerance, 238-240
formatting, 229, 677, 904
form factors, 215
freeing up space, 628
HDI, 216
head crashes, 216
hibernation/sleep mode, 236
high-level formatting, 229, 235-236
HPA, 234
hybrid drives, 402
initializing disks, 767
installing, 403, 456
internal fixed drives, 772
internal laptop drives, 402
JSOD. *See* spanned volumes
laptops, 389, 401-402
letter assignments, 235, 657, 767
logical drives, 233
low-level formatting, 229, 904
magnetic hard drives, 215
managing, 833-834
mechanical hard drives, 402-404
memory, space allocation, 178
mounting, 225, 751, 767
mSATA drives, 402
MTBF, 216
multiple hard drives as backups, 900
navigation inputs, 669
noises, troubleshooting, 247, 404
optimizing, 768-769
OS space requirements, 751
overview, 215
paging files, 192
partitioning. *See* individual entry
PATA IDE hard drives, power requirements, 161
planning drive space, 729
platters, 215, 905
RAID, 238-240, 251
rails, 144
recovery, 645
removing, 144
replacing, 402
SATA hard drives, power requirements, 161
SCSI, SAS drives, 219
security, storage, 904
space, OS requirements, 751
SSD, 769
SSHD, 402
standard formatting, 904
status messages, 250, 766
storage, security, 904
swap files, 242
system images, 215, 243-249, 644-645
troubleshooting, 243-249
types of, 215
volumes, 237-238, 772
wiping, 904
optical drives, 10-11, 772
cleaning kits, 148
connectivity, 285
DirectX, 287
DVD/Blu-ray region codes, 285
features of, 284-285
installing, 286
interfaces, 285
ISO files/images, 285
laptops and external optical drives, 389
overview, 283-284
power requirements, 161
preventive maintenance, 287
reading Blu-ray discs, 284
symbols, 285
testing, 286
troubleshooting, 286-287
writable media, 284
DRM (Digital Rights Management), 876
drop-down menus, Windows, 630
drums (photosensitive), laser printers, 311
DRV files, 632
DSL (Digital Subscriber Lines)
ADSL, 483
modems, troubleshooting, 581-582
phone filters, 484
speeds, 484
xDSL modems, 483-484
dual-alternative structures, 706
dual-channel memory, 185-188
dual Molex-to-PCIe converters, 156
dual-rail power supplies, 160
dual rank memory, 182
dual voltage memory, 182
dual-voltage power supplies, 153
dumpster diving, 869, 881
duplexing
assemblies, printers, 313
inkjet printers, 306
laser printers, 311
NIC, 569
duplexing (double-sided printing), 330
duplicate IP address messages, 563
dust, preventive maintenance, 147, 945, 957
DVD (Digital Versatile Discs)
drives. *See* optical drives
preventive maintenance, 287
region codes, 285
DVI (Digital Video Interfaces), 39, 54
DVI-to-HDMI adapters, 42
dxdiag command, 269, 675-676
dye sublimation printers, 308
dynamic disks, 237, 728
dynamic IP addressing, 560
Dynamic status messages, 250
dynamic storage, 236

E

e-clips, 322
e-readers, 359
e-waste, 946
EB (Exabytes), 20
ECC RAM (Error Correction Code RAM), 181

Edge, Microsoft, 496-497
- Edge tile, Windows Start screen, 628
- Internet Options Control Panel settings, 494
- settings, 493, 494

editing
- environment variables, 697
- Windows
  - credentials, 762
  - registry, 643

editing workstations (audio/video), system design, 442
EDR (Endpoint Detection and Response), 884
educating users, security, 875-876
effective permissions, 896
EFS (Encrypting File Systems), 623, 639, 904
egress data rates, cloud computing, 508
EiB (Exbibytes), 20
EIRP (Equivalent Isotropic Radiated Power), 491
ejecting USB devices, 34
elasticity, cloud computing, 507
electrical fire safety, 943
electricity, static
- antistatic brushes, 148
- EMI, 138
- ESD
  - antistatic tools, 136-138
  - self-grounding, 138
  - SSD, 144
- RFI, 138

electronic key cards, physical security, 864
electronics
- AC, 150-151, 164
- amps, 151-153
- capacitors, 151
- circuit testers, 164
- continuity checks, 152-153
- current, 152-153
- DC, 150-151
- disposal/recycling, 946-948
- multimeters, 151
- ohms, 152-153
- overview, 150
- polarity, 151-153
- resistance, 152-153
- safety, 949
- terminology, 150-153
- voltage, 150-153
- watts, 152-153

email
- BEC attacks, 882
- cloud-based email systems, 804-805
- DKIM, 911
- DMARC, 912
- DNS TXT messages, 911
- ESG, 911
- Exchange Online, 379
- IMAP, 379
- mail servers, 585
- MIME, 379
- mobile device configuration, 379-380
- off-site email apps, 505
- POP3, 379, 589
- security, 910-911
- security policies, 863
- SEG, 911
- S/MIME, 379
- SMTP, 379, 590
- spam, 911
- SPF, 911
- SSL/TLS, 379
- troubleshooting, 910-911

embedded systems, 585
emergencies
- alerts, WEA, 370
- changes. change management, 965
- notifications, 370
- procedures, security policies, 863

EMI (Electromagnetic Interference), 47, 138
emulators
- Terminal, macOS, 834
- virtualization, 501

enable command, 676
enclosures, computer, 957
encryption, 865
- AES, 568, 903
- AutoPlay, disabling, 904
- AutoRun, disabling, 904
- BitLocker, 622, 903
- BitLocker Drive Encryption, 623
- BitLocker To Go, 623, 903
- cipher command, 672-673
- data at rest, 903
- device encryption, 414, 903
- Drive Encryption setting (BIOS/UEFI), 109
- EFS, 623, 639, 904
- files, 639, 904
- full device encryption, 903
- other people's files, 904
- SAE, 923
- TKIP, 567
- unlocking encrypted hard drives, 903
- WEP, 567
- Windows files/folders, 639
- WPA, 568
- WPA2, 568
- WPA2 with AES, 568
- WPA3, 568

end devices, IP addressing, 560
- alternative IP address configurations, 563
- APIPA, 563
- default gateways, 564-565
- DNS, 565-566
- static configurations, 560-561

end-users
- change management, 966
- security, 875-876

endpoint management servers, 584
endpoints, USB, 749-750
energy absorption/dissipation, surge protectors, 952
energy efficiency ratings, power supplies, 162
ENERGY STAR ratings, 446
enlarging screens/images, 365
Enterprise edition, Windows 10/11, 618
environment variables
- accessing, 696
- editing, 697
- system environment variables, 696
- user environment variables, 696
- viewing, 698

environmental concerns in system design, 446
environmental impacts, safety, 945-946
EOL (End of Life), OS, 620, 898
EPEAT rating system, 446
EPS12V power supplies, 154
EPS files, 632
EP (toner) cartridges, laser printers, 311, 322
equal to (= =) operators, 705
equality (comparison) operators, 705
equipment grounding, 136
equipment locks, physical security, 865
Error Checking tool, Windows, 768
error messages, 455
  "array missing", 251
  BIOS ROM checksum, 456
  "Bootable device not found.", 113, 248
  CMOS, 456-457
  "drive not recognized", 246
  hard drive installations, 456
  intruder detection errors, 456
  "Invalid Boot Disk", 773
  keyboards, 456
  memory, 457
  motherboards, 457
  "no OS found", 248, 737
  "Not enough USB controller resources", 749-750
  "not responding", 757
  NTLDR Is Missing, 736
  POST, 191
  "RAID array missing," 251
  "RAID not found", 251
  "tray not recognized", 340
eSATA (external SATA), 221
  brackets, 120
  cables, 44
  drives, troubleshooting, 249
  installing cards, 120-121
  mounting/unmounting drives, 225-226
  partitions, 233
  ports, 43-44, 54
ESCD (Extended System Configuration Data), 116
ESD (Electrostatic Discharge), 13, 949
  antistatic tools, 136-138
  self-grounding, 138
  SSD, 144
ESG (Email Security Gateways), 911
eSIM (embedded SIM), 368
Ethernet
  cabling, 49-51, 532
  EoP, 534
  networks
    EoP, 534
    LAN, 519
    star topologies, 520
  NIC, 121
  PoE, 533
  ports, 46-47
  punchdown blocks, 50
  punchdown tools, 50
  projectors, 275
  standards, 521
  types of, 521
  USB-to-Ethernet converters, 35
ethics (soft skills), 348
EULA (End-User Licensing Agreements), 876
evaluation phase, change management, 966
Event Viewer
  clearing logs, 759
  logs, 756-757
  symbols, 757
  troubleshooting apps, 757
events
  forwarded events, 757
  logging, 890
evil twin attacks, 882
exams, preparing for, 5
Exchange Online, 379
exclusions, DHCP, 562
.EXE files, 632
exFAT (FAT64), 230, 236, 728
exit command, 676
exiting user checklists, 960
expand command, 676
expansion cards
  laptops, 390
  M.2 expansion cards, 390
  miniPCIe cards, 389
  NVMe cards, 391
  USB, 117-118
expansion slots, 13-14
  laptops, 390
  motherboards, 83
  PCI, 83
  retention levers, 86
expectations (soft skills), setting/meeting, 974
expiration dates, accounts/passwords, 890
expired passwords, 875
explorer command, 677
exposing phase, laser printer imaging process, 310
ext3 file systems, 842
ext4 file systems, 230, 729, 843
extended partitions, 233, 728
extended read/write times, troubleshooting, 244
extenders, wireless, 551
extending partitions, 767
extensible software, 621
extensions
    browsers, 493-495
  Windows files, 631-632
external cables, removing, 140
external data buses, 67
external hard drives, 402, 772
external hardware tokens. *See* dongles
external interference, wireless networks, 558-559
external laptop devices, 389
external networks, 502
eye protection, 149

F

facial recognition security, 412, 874
FACTA (Federal Trade Commission Act), 869
factory resets, 384
faded print, troubleshooting, 340
failed login attempts, 413, 875
Failed status messages, 250
  batteries, signs of failure, 111
  boot, troubleshooting, 247, 790-791
  power, 954

INDEX

fake security warnings, mobile devices, 411
fans
auxiliary fans, 157, 161
cases, 157
Fan Control setting (BIOS/UEFI), 108
installing, 81-82
processor cooling, 77
FAT (FAT16) file systems, 230, 236
FAT32 file systems, 230-231, 236, 728
FAT64 file systems, 230, 236, 728
fault tolerance, 238, 239, 240
FC (Fibre Channel), SAN connections, 524
FCM (Flash Cache Modules), RAID, 239
feed assemblies, thermal printers, 312, 324
feeds, paper, 306, 313-315, 318, 339
FERPA (Federal Educational Rights and Privacy Act), 869
fiber cables, 51-52
fiber networks, 486
bandwidth, 488
downstream data, 487
ONT boxes, 487
upstream data, 487
File Explorer, Windows, 615, 630
Content view, 634
copying files, 640
Details view, 634
display options, 634
file attributes, 637
file compression, 639
file encryption, 639
file structures, 658-659
folder options, 897
indexing, 636
List view, 634
moving files, 640
paths, 632-634
searches, 635
starting, 677
Tiles view, 634
troubleshooting, 422
viewing mapped drive paths, 597
View tab options, 897-898
File History backups, 741
file systems
APFS, 230
Btrfs, 843
defined, 230
EFS, 904
exFAT, 230, 236
ext3, 842
ext4, 230, 729, 843
FAT (FAT16), 230, 236
FAT32, 230-231, 236, 728
FAT64, 230, 236, 728
NTFS, 230, 236, 728
boot partitions, 234
clusters, 231
disk quotas, 232
partitioning, volume structures, 235
system partitions, 234
ReFS, 230, 729
types of, 728-729
XFS, 843
ZFS, 843
fileless malware, 879
files, 615
attributes, 637, 665, 896-897
backslashes (\) in file structures, 659
.bat files, 664, 693
cloud file storage services, 505
compression, 639
configuration files, Linux, 840
copying, 640, 664-665, 686, 691-692
deleting, 628, 663, 674, 909
directories, 657, 662-663
EFS, 623
encryption, 639, 904
extensions, viewing, 898
finding, Linux, 853
FTP, 589
hidden files, viewing, 898
image files, Print to image (virtual printing), 316
.inf files, 748
ISO files/images, optical drives, 285
JavaScript (.js), 694
leaked personal files/data, 414
managers, 841
missing files, viruses/malware attacks, 880
moving, 640
naming, 657, 686
organizing, 657
PDF files, Print to PDF (virtual printing), 316
permissions, changing, 891
Python scripts (.py), 694
recovery software, 245
ReFS, 768
removable media files, deleting, 628
renaming, 686
servers, 584
sfc, 738
SFTP, 589
sharing menus/options, 898
shell scripts (.sh), 693
swap files, 242
synchronizing, 505
System File Checker, 249, 687
System File Checker tool, 246
system files, 772-773, 898
text files, 692-694
creating, 7
more command, 680
type command, 690
tree structure, 657-659
.txt files, displaying, 664
types, 621
uncompressing, 676
VBScript (.vbs), 694
Windows files
extensions, 631-632
filenames, 631
paths, 632-634
saving, 632
Windows setup log files, 736-737
XPS files, Print to XPS (virtual printing), 316
fileshare servers, 584
filtering
air filtration masks, 149
content, 571, 920
IP filtering, 571, 625
MAC addresses, 924
spam, 911

Finder, macOS, 819
finding
files, Linux, 853
GRUB, 854
fingerprints, security, 412, 868, 874
fire extinguishers, 459, 943
fire safety, 943
Firefox web browser, 496-497
firewalls, 870, 913
AP configurations, 570
port forwarding, 916
Windows Defender Firewall, 914-917
wireless networks, 922
FireWire ports, troubleshooting, 798
firmware
AP, 926
fTMP setting (BIOS/UEFI), 109
updating, 112-113
wireless networks, 571
fixed wireless connectivity, long-range, 490
flapping, ports, 575
Flash BIOS, 105
Flash Cache Modules (FCM), RAID, 239
flash drives, 197-199
flashing BIOS/UEFI, 112-113
flashing screens, troubleshooting, 271
flash media adapters, 361
flash memory, 197
memory card readers, 361
SD cards, 360-361
SSD, 402-404
SSHD, 218
flatbed scanners, 17, 288-289
FlexATX power supplies, 154
flickering displays, troubleshooting, 422
flick/swipe actions (mobile devices), 366
floating point numbers, 701
flowcharts, troubleshooting, 464-466
folders, 615
attributes, 637, 896-897
compression, 639
copying, 640
encryption, 639
home folders, AD, 888
List Folder Contents permissions, 895
moving, 640
NTFS permissions, 896
Public folders, share permissions, 894
redirecting, 888
security options, 897
shared folders, 594-595
mapping, 596, 597
Shared Folders tool, 759
subfolders, 896
system folders, macOS, 823
Windows folders, 631
for loops, 709-711
Force Quit, macOS, 826
Foreign status messages, 250
form factors
cases, 154
hard drives, 215, 401
laptops, 401
motherboards, 88-89, 154
power supplies, 153-154
SODIMM, 400
formatting
commands, 236, 657, 668, 677
full (standard) formatting, 235
hard drives, 677, 904
high-level formatting, hard drives, 229, 235-236
low-level formatting, 229, 904
passwords, 874
quick formatting, 235
forwarded events, 757
forwarding, port, 517, 916-917
forward (upward) compatibility, 621
frames, OSI model, 539
freeing up disk space, 628
freezes, change, 964
frequencies
channel ID, 553-556
Hz, 20
response ranges, speakers, 282
wireless networks, 546, 550
front panel connectors, 142
frozen print queues, troubleshooting, 343
frozen systems, troubleshooting, 424, 784
FRT (Facial Recognition Technology), physical security, 868-869
FSB (Front Side Buses), speeds, 69-70
fsck command, Linux, 845
FTP (File Transfer Protocol), 589
fTPM (firmware Trusted Platform Module) setting (BIOS/UEFI), 109
F-type connectors, 48
full backups, 900
Full Control permissions, 893-895
full device encryption, 903
full paths, command prompt, 663
full (standard) formatting, 235
full system functionality, verifying, 463
function keys, special, 399
fused toner (printing), troubleshooting, 347
fuser assemblies, laser printers, 310-311
fuser cleaning pads, laser printers, 323
fusing rollers, laser printers, 311, 323
fuzzy images (screens), troubleshooting, 271

G

gain, antennas, 557
gaming
P2P, 571
PC system design, 441
garbled print, troubleshooting, 340
gateways
default, 564-565
spam, 911
gathering information/data, 695
Internet searches, 6-7
troubleshooting process, 451
GB (Gigabytes), 19-20
GDPR (General Data Protection Regulation), 878
General Optimization setting (BIOS/UEFI), 107
general-purpose cleansers, 148
general-purpose cloths, 148
General tab (Internet Options Control Panel), 494
generic credentials, 759
geotracking, 369-370

gestures, macOS, 822
GFS (Grandfather Father Son) backups, 901
GHz (Gigahertz), 67
GiB (Gibibytes), 20
.GIF files, 632
gloves, antistatic, 137
glue, thermal paste as, 78
goggles, safety, 149, 944
gold contact cleaners, 148
Google
  Android OS, 619
  Chrome OS, 360, 496-497, 619
  mobile device synchronization, 383
government regulations, workplace safety, 942
gpedit.msc command, 889
GPGPU (general-purpose GPU), 72
gpresult command, 677
GPS (Global Positioning Systems), 358, 369
  tracking, 411
  troubleshooting, 426
GPT (GUID Partition Tables), 234-235, 728
GPU (Graphics Processing Units), 72
  dGPU, 267
  iGPU, 109, 266
gpupdate command, 678
grandfather backups, 901
graphic/CAD/CAM design workstations, 441
graphical interfaces, troubleshooting, 791
graphics
  cards
    dedicated vs integrated, 751
    integrated graphics cards, 266
  dGPU, 267
  iGPU, 266
greater than (>) operators, 705
greater than or equal to (>=) operators, 705
grep command, macOS, 835, 838
grinding noises, troubleshooting, 247, 286, 339
grooming (soft skills), 968
grounding, electronic safety, 136, 949
group policies, 677-678, 889-890
groups
  administrator accounts, 884
  backup operators accounts, 885
  guests accounts, 884
  Local Users and Groups tool, Windows, 762-763
  network configuration operators accounts, 885
  offer remote assistance helper accounts, 885
  performance log user accounts, 885
  remote desktop user accounts, 885
  security groups, 886
GRUB (Grand Unified Boot Loader), 854
GSM (Global System for Mobile Communications), 367
guards, physical security, 865
guests
  access, wireless networks, 927
  accounts, 884, 890
GUI (Graphical User Interfaces), 615
  Linux, 841
  macOS, 819-821
GUID (Globally Unique Identifiers), 234, 728
gun slinger technicians, 123

H

hallucinations, AI, 961
handheld scanners, 288
handling
  CPU, 79
  discs, 287
hanging apps, troubleshooting, 757
hard drives, 10. *See also* disks
  2.5-inch, 215
  3.5-inch, 215
  arrays, adding, 767
  basic disks, 236
  BitLocker Drive Encryption, 623
  boot sectors, 236
  changing drive letters, 767
  clusters
    lost clusters, 243
    NTFS file systems, 231
  DBR, 236
  defragmenting, 244, 769
  degaussing, 905
  destroying, 905
  disks
    caches, 241-243
    mirroring (RAID 1), 239
    striping (RAID 0), 239
  drive activity LED, 246
  dynamic disks, 237
  encrypted hard drives, unlocking, 903
  external hard drives, 389, 402, 772
  fault tolerance, 238-240
  formatting, 229, 677, 904
  form factors, 215
  freeing up space, 628
  HDI, 216
  head crashes, 216
  hibernation/sleep mode, 236
  high-level formatting, 229, 235-236
  HPA, 234
  hybrid drives, 402
  initializing disks, 767
  installing, 403, 456
  internal fixed drives, 772
  internal laptop drives, 402
  JSOD. *See* spanned volumes
  laptops, 389, 401-402
  letter assignments, 235, 767
  logical drives, 233
  low-level formatting, 229, 904
  magnetic hard drives, 215
  managing
    Disks, Linux, 842
    Disk Utility, macOS, 833-834
  mechanical hard drives, 402-404
  memory, space allocation, 178
  mounting, 225, 767
  mSATA drives, 402
  MTBF, 216
  multiple hard drives as backups, 900
  noises, troubleshooting, 247, 404
  optimizing, 768-769
  OS space requirements, 751
  overview, 215
  paging files, 192

partitioning, 229-230
basic disks, 727
boot partitions, 234, 773
converting, 231, 730
deleting, 234
disk part command, 675
drive partitions (volumes), 729
dynamic disks, 728
extended partitions, 233, 728, 767
FAT32 file systems, 231
GPT, 234-235, 728
internal hard drive partitions, 772
logical partitions, 728
MBR, 234-235, 728
planning drive space, 729
primary partitions, 233, 727
system partitions, 234
partitions, 727
basic disks, 727
boot partitions, 773
convert command, 730
disk part command, 675
drive partitions (volumes), 729
dynamic disks, 728
extended partitions, 728
extending, 767
GPT, 728
internal hard drive partitions, 772
logical partitions, 728
MBR partition tables, 728
primary partitions, 727
shrinking, 767
splitting, 767
swap partitions, 728
PATA IDE hard drives, power requirements, 161
planning drive space, 729
platters, 215, 905
RAID
"array missing" error messages, 251
BIOS/UEFI settings, 240
configuring, 238
failures, 251
fault tolerance, 238-240
FCM, 239
hardware RAID, 240
hot swappable RAID drives, 240
levels of, 239-240
RAID 0, 239
RAID 0+1, 239
RAID 1, 239
RAID 5, 239
RAID 6, 239
RAID 10, 239
"RAID not found" error messages, 251
software RAID, 239
troubleshooting, 251
rails, 144
removing, 144
replacing, 402
SATA hard drives, power requirements, 161
SCSI, SAS drives, 219
security, storage, 904
SSHD, 402
standard formatting, 904
status messages, 250, 766
storage, security, 904
swap files, 242
system images, 644-645
troubleshooting
bootup failures, 247
data loss/corruption, 245
extended read/write times, 244
fragmented drives, 244
noises, 247
performance, 243-244, 249
read/write failures, 249
sticky hard drives, 248
types of, 215
volumes
adding, 767
boot volumes, 237-772
RAW volumes, 237
resizing partitions, 238
simple volumes, 237
spanned volumes, 237
striped volumes, 237
system volumes, 237, 772
wiping, 904
hard resets, 416-417
hardware
configuring, 115-116
defined, 8
drivers, installing/updating, 116
installing, 461
laptops, 387
OS update limitations, 620
RAID, 240
reinstalling, 461
troubleshooting, 459
verifying with Device Manager, 122
Windows
compatibility, 725
installations, 730
Hardware Monitoring setting (BIOS/UEFI), 108
hardware tokens, physical security, 865-866
hash characters (#), 492, 703-704
HDI (Head-to-Disk Interference), 216
HDMI (High-Definition Multimedia Interface) ports, 41, 54
head crashes, 216
headers
defined, 36
OSI model, 539
USB, 117
headsets, 17, 362-363
health of batteries, 423
Healthy status messages, 250
heat sinks, 77, 81
heating elements, thermal printers, 312, 324
Hello, Windows, 412
help command, 668, 678
help desks, ticket systems, 962
help (Windows), context-sensitive, 630
HEPA vacuum bags, laser printers, 323
hibernation/sleep mode
hard drives, 236
PC, 799
power supplies, 159
hidden files, viewing, 898
hidden shares, 894
high latency, 577
high-level formatting, hard drives, 229, 235-236
high network traffic, 425
high number of ads, 414

high performance plans, Windows, 799
hijacking attacks, TCP/IP, 883
HIPAA (Health Insurance Portability and Accountability Act), 878
history, web browsers, 493
Hkey_Classes_Root subtree, Windows registry, 643
Hkey_Current_Config subtree, Windows registry, 643
Hkey_Current_User subtree, Windows registry, 643
Hkey_Local_Machine subtree, Windows registry, 643
Hkey_Users subtree, Windows registry, 643
.HLP files, 632
hole punched paper, 341
Home edition, Windows 10/11, 618
home folders, AD, 888
home screens
  Android, 364
  iPhones, 365
home servers, system design, 445-446
host addresses, IPv4 addressing, 543
host machines, 501
hosted (Type 2) hypervisors, 501
hostname command, 678
Host-only mode, virtual NIC, 570
hotfixes, 736
hotspots, 377, 489
hot swappable RAID drives, 240
HPA (Host Protected Areas), 234
HSM (Hardware Security Modules), 88, 865
HTTP (Hypertext Transfer Protocol), 589
HTTPS (HTTP over SSL/TLS), 589
HTTPS (Hypertext Transfer Protocol Secure), 492
hubs, 33, 519-520, 541
humidity
  ESD, 949
  paper, 313
  safety, 958
humility (soft skills), 855
hybrid clouds, 506
hybrid drives, 402
hyperthreading, 502
HyperTransport buses, 70
Hyper-V, 73, 502, 722, 727
hypervisors, 501
Hz (hertz), 20, 67

I

IaaS (Infrastructure as a Service), 504
iCloud, 384-385, 822
ICMP (Internet Control Message Protocol), 587
icons
  moving on mobile devices, 365
  removing from notification area, 749
  sizing, Windows desktop, 634
  Windows 10/11, 623
IDE (Internal Drive Electronics) cables, 142
identification
  access management, 870
  Apple ID, 823
  channel ID, wireless networks, 553-556, 571
  GDPR, 878
  passwordless security, 874
  PCI DSS, 877
  PID, listing, 689
  PII, 877
  PIN, 874
  RFID, physical security, 865
  SSID, 571, 926
  synchronization, 872
  Windows Hello, 874
identifying
  adapter function, 13
  problems, troubleshooting process, 452-453
IDS (Intrusion Detection Systems), 920
IEEE 802.11 wireless standard, mobile devices, 375-376
IEEE 802.11a wireless standard, 375, 548
IEEE 802.11ac (Wi-Fi 5) wireless standard, 375, 548
IEEE 802.11ad (WiGig) wireless standard, 548
IEEE 802.11ax (Wi-Fi 6) wireless standard, 375, 548
IEEE 802.11b wireless standard, 375, 548
IEEE 802.11be (Wi-Fi 7) wireless standard, 375, 548
IEEE 802.11e wireless standard, 548
IEEE 802.11g wireless standard, 375, 548
IEEE 802.11i wireless standard, 548
IEEE 802.11n wireless standard, 375, 548
IEEE 1394 FireWire ports, troubleshooting shutdowns, 798
ifconfig command, 576, 846
ignoring manufacturer's advice, 117
iGPU (integrated GPU), 72, 109, 266
images
  burn-in(screens), troubleshooting, 272
  deployments, Windows, 723
  dim images (screens), troubleshooting, 271
  disk imaging, 733
  double images (printing), troubleshooting, 347
  enlarging, 365
  fuzzy images (screens), troubleshooting, 271
  ISO files/images, 285, 751
  moving through, 366
  Print to image (virtual printing), 316
  system images, 644-645, 791
  Windows deployments, 723
imaging
  laser printers
    drums, 311
    process, 309-310
  reimaging computers, 733-734s
  SIM, 734
IMAP (Internet Message Access Protocol), 379, 589
IMEI (International Mobile Equipment Identities), 367
impact printers
  maintenance, 318-319
  paper, 305, 319
  printheads, 303-304, 319
  print ribbons, 304, 318-319
  troubleshooting, 345
impersonation attacks, 880

implementation phase, change management, 966
improper charging, troubleshooting, 392, 424
IMSI (International Mobile Subscriber Identities), 368
inaccurate system dates/times, troubleshooting, 111
incidents
  documentation, 962
  reports, 942
  response, security, 928-929
incineration, proof of, 869
incompatibility, software and OS (Operating Systems), 620
incorrect colors (screens), troubleshooting, 271
incorrect data sources (projectors), troubleshooting, 275
incremental backups, 900
indexing, Windows, 636
indicator lights, printers, 338
.inf files, 632, 748
infinity, digital meters, 152
information/data, gathering, 695
  Internet searches, 6-7
  troubleshooting process, 451
infrastructures, IaaS, 504
inherited permissions, 895
.INI files, 632
initializing
  disks, 250, 767
  variables, 701
initiating updates, 695
ink cartridges
  CIS, 317
  inkjet printers, 305-306, 320
  recycling, 317
  refilling, 317
inkjet printers, 303
  calibrating, 320
  carriage belts, 306
  carriages, 306
  cleaning, 321
  color, 307, 346
  draft mode, 306
  duplexing assemblies, 306
  ink cartridges, 305-306, 320
  maintenance, 319-321
  NLQ mode, 306
  optimized DPI, 305-307
  paper trays/feeders, 306
  power supplies, 306
  printheads, 305-306, 321
  rollers, 306
  stepper motors, 306
  troubleshooting, 345-346
in-place/overwrite solutions, 902
in-place upgrades, Windows, 723-724
input/output
    cameras/webcams, 17
  defined, 17
  flatbed scanners, 17
  headsets, 17
  keyboards, 14-16, 30, 54
  microphones, 17
  mouse/mice, 14-16, 30, 54
  printers, 17
  programming, 699
  voltage selectors, 156
insider attacks, 882
instability (Windows systems), troubleshooting, 797
Installation Assistant, 725
installation media, 726
installing
  adapter function, 13-14
  antistatic tools, 78
  apps, 371, 695, 751-752
    failures, troubleshooting, 419
    macOS, 824
  CPU, 79-81
  device drivers, 745-746
    compatibility mode, 749
    manual installations, 748
    troubleshooting, 748
  DIMM, 191
  drivers, 116
  eSATA cards, 120-121
  fans, 81, 82
  hard drives, 403, 456
  hardware, 461
  heat sinks, 81
  manufacturer's advice, ignoring, 117
  memory, 191
    laptops, 401
    overview, 190
    planning installations, 179-190
  miniPCI/PCIe adapters, 390
  monitors, 40
  motherboards, 89-90
  mSATA, 225
  multifunction (all-in-one) devices, 326
  NIC, 121
  optical drives, 286
  OS, verifying installations, 735
  printers
    connectivity, 325-326
    overview, 324
    setup locations, 324
  processors, 78, 81
  routers, wireless, 926-927
  SATA devices, 223
  scanners, 289
  software, 461, 750-752
  sound cards, 278-279
  SSD, 226-227, 404
  storage devices, troubleshooting, 246-249
  thermal paste, 81
  tools, antistatic, 78
  USB devices, 117
    expansion cards, 117-118
    ports, 36
  video adapters/cards, 269-270
  Windows
    antivirus software, 732
    backups before OS installations, 731
    clean installations, 723
    compatibility mode, 727
    corporate deployments, 733-734
    disabling interfering software, 732
    drivers, 731
    file systems, 728-729
    hardware, 730
    image deployments, 723
    in-place upgrades, 723-724
    installation media, 726
    licenses, 734
    multiboots, 723

PCmover Express, 726
phases of, 732
recovery partitions, 723
remote network installations, 723
repair installations, 723, 738
resets/restores, 723
security scans, 731
selecting networks, 732-733
types of, 722
unattended installations, 723
USMT, 726
ZTI, 723
wireless AP, 926-927
wireless routers, 926-927
"insufficient disk space" error messages, 249
integers, 701
integrated graphics cards, 266, 751
integrated motherboard port adapters, 53
Integrated Peripherals setting (BIOS/UEFI), 108
integrated searches, web browsers, 493
Intel
multicore processors, 71
processors, 66-67, 74-75
sockets, 76
interfaces
ACPI, 109, 159
AHCI mode, SATA, 228
optical drives, 285
interference
EMI, 138
RFI, 138
wireless networks, 558-559
interfering software, disabling from OS installations, 732
intermittent shutdowns
memory, 195
projectors, 276
intermittent wireless connectivity, 425-426, 558, 574-576
internal cables/connectors, removing, 141-142
internal data buses, 67
internal fixed disks, 772
internal hard drive partitions, 772
internal laptop drives, 402
internal networks, VM, 502
Internet
appliances
content filtering, 920
IDS, 920
IPS, 921
load balancers, 920
UTM systems, 920
calling, 370
connectivity. *See also* mobile connectivity
cable modems, 482-483
dial-up connectivity, 480-482
fiber networks, 486-488
overview, 480
satellite modems, 488-489
tethering, 489
troubleshooting, 425, 574-576
VoIP, 484-486
xDSL modems, 483-484
IoT, 572-573
ISP, 489
metered connections, 591
search skills, 6-7
security, 906
allow lists, 913
deny lists, 913
digital security certificates, 906
DMZ, 913, 924
DNS, 909-910
email, 910-911
firewalls, 913
malware removal, 907-908
Microsoft Defender Antivirus, 906
NAT, 917
PAT, 917
proxy servers, 912
rogue antivirus apps, 906
screened subnets, 571, 913, 924
UPnP, 914
VPN, 919-920
Windows Defender Firewall, 914-917
subscribers, data caps, 379
WISP, 490
Internet layer (TCP/IP model), 541, 590
Internet Options Control Panel settings, Microsoft Edge, 494
interpreted programs, 692
intrusions
intruder detection error messages, 456
Intrusion Detection/Notification setting (BIOS/UEFI), 109
preventing with IDS/IPS, 920
"Invalid Boot Disk" error messages, 773
Invalid status messages, 250
inventories
lists, 963
management, 963
inverters, 407-409
I/O (Input/Output) addresses, 114
IOPS (Input/Output Operations per Second), 244
iOS, 360, 619
apps, updating/deleting, 419
email configuration, 380
mobile devices
backups, 384
synchronization, 383-384
passcode settings, 413
security, 413
I/O shields, 145
IoT (Internet of Things), 572-573, 928
IP (Internet Protocol)
addressing, 541
alternative IP addresses, configuring, 563
APIPA, 563
multiple devices, assigning the same address, 560-561
changing addresses, 560
default gateways, 564-565
DNS, 565-566
duplicate messages, 563
dynamic IP addressing, 560
filtering, 925
IPv4 addressing, 542-546
IPv6 addressing, 542
same address, assigning to multiple devices, 560-561
static IP addressing, 560-561
subnet masks, 985-987
filtering, wireless networks, 57
VoIP, 484-486

ip command, Linux, 845-847
iPadOS, 360, 619
ipconfig command, 576, 678-679
iPhones, home screens, 365
IPS (Intrusion Prevention Systems), 921
IPS LED (In-Plane Switching LED), 265
IR (Infrared) connectivity, 55, 379
IRQ (Interrupt Requests), 114
iSCSI (Internet Small Computer Systems Interface), SAN connections, 524
ISO images
  optical drives, 285
  software installations, 751
isolating
  PC, 498
  problems, troubleshooting process, 461-462
  servers, 498
ISP (Internet Service Providers), 489-490
IT (Information Technology)
  automation, 966
  documentation
    AI, 961
    asset management, 963
    AUP, 964
    examples of, 959
    incident documentation, 962
    knowledge bases/articles, 961
    network topology diagrams, 960
    new user/exiting user checklists, 960
    password policies, 963
    regulatory/compliance policies, 964
    security policies, 964
    SLA, 960
    SOP, 959
  job requirements, preparing for, 3
  roles, 2
iteration, loops, 709
iTunes, mobile device synchronization, 384
ITX (Information Technology eXtended), motherboards, 88
iwconfig command, Linux, 845
iwlist command, Linux, 847
iWork, macOS, 822

J

jailbreaking/unauthorized root access, 414-415
jams, paper, 339
JavaScript (.js), 694
JBOD (Just a Bunch Of Disks). *See* spanned volumes
JIT (Just-In-Time) access, 873
jitter, VoIP, 485
jobs in IT, 2-3
joining domains, 886
.JPG (.JPEG) files, 631
jumpers, 112

K

kB (kilobytes), 19-20
keeping commitments (soft skills), 972
Kerberos authentication servers, 873
kernels, 9
  Linux, 839
  panic, troubleshooting, 831
key cards, physical security, 864
key fobs, physical security, 865
keyboards, 14
  CAPS LOCK key, 16
  error messages, 456
  lights (common), 16
  NUM LOCK key, 16
  ports, 30
  preventive maintenance, 15
  PS/2 keyboards, 54
  PS2 keyboard ports, 54
  repairing, 397-398
  scroll lock key, 16
  special function keys, 399
  troubleshooting, 16
Keychain Access, macOS, 832-833
keyloggers, 879
keys
  B+M, SSD, 218
  M.2 devices, 218
  mobile digital keys, 865
  physical security, 863
keywords, variable names, 700
KiB (Kibibytes), 20
kill command, macOS, 835
kill tasks (stop), 782
kiosks, 957
KMS (Key Management Service), 734
knowledge bases/articles, 961

L

L1 caches, 69
L2 caches, 69
L3 caches, 69
labeling cables, 533
ladder racks, 535
lanes, PCIe, 85
languages, printers, 330
LAN (Local Area Networks), 520
  Ethernet LAN, 519
  VLAN, 545
  Wake on LAN, 159-160
  Wake on LAN, NIC, 569
  WLAN, 518, 523, 921
  workgroups, 521-523
laptops
  apps, troubleshooting, 418-419
  backlight bulbs, 407
  batteries, 393
  Bluetooth, 374, 404
  cable locks, 410
  CCFL bulbs, 407
  cellular cards, 389
  DC jacks, replacing, 406
  digitizers, 407
  DisplayPort, 389
  displays, 407-409, 421-422
  docking stations, 389
  expansion cards, 389-391
  expansion slots, 390
  external devices
    hard drives, 389
    monitors, 389
    optical drives, 389
  hard drives, 389, 401-403
  hardware, 387
  input voltage selectors, 156
  internal drives, 402
  inverters, 407-409
  keyboards, 397-399, 420

levering covers, scribes, 394
M.2 expansion cards, 390
memory, 400-401
microphones, 407-410
miniPCIe cards, 389
miniPCI/PCIe adapters, 390
monitors, 389
motherboards, repairing, 395-396
NVMe cards, 391
optical drives, 389
overview, 387
performance, troubleshooting, 423
port replicators, 389
power supplies
  options, 800
  optimizing battery performance, 393-394
  removing batteries, 392
  settings, 394
  temperature changes, 392
processors, removing, 396
RAM, 360
removing
  hard drives, 402
  keyboards, 397-398
  touchpads, 397
repairing
  keyboards, 397-398
  motherboards, 395-396
  overview, 394
  processors, 396
  touchpads, 397
screens
  replacing, 408
  resolution, 409
  troubleshooting, 421-422
  Wi-Fi antennas, 407
SD card slots, 361
security
  data-usage limit notifications, 414
  failed login attempts, 413
  jailbreaking, 414-415
  leaked personal files/data, 414
  system lockouts, 413
  unauthorized account access, 413
  unauthorized location tracking, 414
  unauthorized root access, 414-415
SSD, 391, 403-404
storage, 401-402
touchpads, 397
touch screen displays, 407
trackpads, 421
troubleshooting
  app closure failures, 418
  app installation failures, 419
  app load failures, 419
  app update failures, 419
  autorotating screens, 421
  backlight failures, 421
  batteries, 423-424
  Bluetooth connectivity, 426-427
  damaged ports, 415
  dim displays, 421
  frozen systems, 424
  GPS, 426
  hard resets, 416-417
  keyboards, 420
  liquid damage, 415
  network issues, 425-426
  NFC, 427
  no display, 421-422
  no power, 424
  OS update failures, 417
  overheating, 424
  performance, 423
  random reboots, 415
  soft resets, 416
  trackpads, 421
  unexpected app behavior, 418
  Wi-Fi connectivity, 425-426
WAN connectivity, 490
webcams, 407-410
Wi-Fi antennas, 407
wireless antennas, 406
wireless cards, 389, 404
wireless connectivity
  cellular networks, 490
  hotspots, 489
  long-range fixed wireless, 490
  power requirements, 491-492
  tethering, 489
  wireless broadband, 490
large-format inkjet printers, 308
laser printers, 303
  calibrating, 323
  cleaning, 323
  cleaning blades, 311
  cleaning pads, 311
  cooling, 323
  density control blades, 311
  duplexing assemblies, 311
  e-clips, 322
  fuser assemblies, 310-311
  fusing rollers, 311, 323
  imaging drums, 311
  imaging process, 309-310
  maintenance, 321-323
  noises, 311
  parts of, 311
  power supplies, 311
  safety, 309
  toner, 311, 322-323, 948-949
  transfer corona, 323
  troubleshooting, 346-347
  UPS, 955
latency
  networks, 577
  VoIP, 486
launcher, Linux, 841
launching apps, 751
Launchpad, macOS, 821
lb (pounds), paper, 313
LC connectors, 51
LCD (Liquid Crystal Displays), 264-265, 272
LDAP (Lightweight Directory Access Protocol), 589
leaked personal files/data, 414
learning commands, 666
lease time, DHCP, 562
least privilege
  logical security, principle of, 871
  share permissions, 893
LED (Light-Emitting Diodes)
  displays, 264
  drive activity LED, 246
  motherboard LED, drive/boot failures, 246
  motherboards, 458
  status indicators, 246
Legacy mode, SATA, 228

legacy software, 498
legacy systems, 586
lens cleaners, 148
less command, macOS, 835, 838
less than (<) operators, 705
less than or equal to (<=) operators, 705
letter assignments, hard drives, 235
levels of risk, change management, 965
levering covers, scribes, 394
LFX12V power supplies, 154
libraries, Windows, 631
licensed ranges, wireless connectivity, 490
licenses
    asset management, 963
    commercial licensing, 876
    DRM, 876
    EULA, 876
    KMS, 734
    OS licenses, virtualization, 501
    perpetual licenses, 876
    personal licenses, 876
    piracy, 876, 877
    regulated data, 877
    security, 876
    valid licenses, 876
life cycles, procurement, 963
lifting techniques, safety, 20, 945
lighting, physical security, 865
Lightning cables, 37, 54
Lightning ports, 37, 54, 372
light printing, troubleshooting, 345
lights (common), keyboards, 16
Li-ion batteries, 393, 947-948
LILO (Linux Loader), 854
limited/intermittent connectivity, troubleshooting, 425, 574-576
limits, data-usage limit notifications, 414
line conditioners, 953
LINE jacks, modem connectivity, 480
line speed. *See* bandwidth
lines down printed pages, troubleshooting, 339
link-local addressing, IPv6, 542
lint-free cloths, 148
Linux, 617. *See also* Ubuntu
    apt command, 845-849
    backups, 844
    best practices, 854
    bootloader, 840
    Btrfs, 843
    CLI, 845, 848-849
    configuration files, 840
    copying data, 849-852
    dash, 841
    dd command, 845, 849-852
    df command, 845
    Disks, 842, 852
    distros (distributions), 839
    DNS servers, 840
    ext3 file systems, 842
    ext4 file systems, 843
    file managers, 841
    finding
        files, 853
        GRUB/LILO, 854
    fsck command, 845
    GRUB, 854
    ifconfig command, 846
    ip command, 845-847
    iwconfig command, 845
    iwlist command, 847
    kernels, 839
    launcher, 841
    LILO, 854
    locate command, 845, 853
    memory recommendations, 183
    mount command, 845
    network configurations, 846
    passwd command, 845-846
    passwords, 846
    processes, viewing, 847-848
    ps command, 845-848
    shutdown command, 845-846
    software
        obtaining, 848-849
        pre-downloading software packages, 849
        Software Updater, 843
    su command, 845
    sudo command, 846
    systemd, 840
    System menu, 841
    top command, 845
    Ubuntu, downloading, 840
    updatedb command, 845, 853
    user forums, 854
    XFS, 843
    zeroing out devices, 852
    ZFS, 843
liquid cooling, 77
liquid damage, troubleshooting, 16, 415
listening (soft skills), active, 2, 92-93, 970
List Folder Contents permissions, 895
List view, Windows File Explorer, 634
lists
    inventory lists, 963
    moving through, 366
    PID, 689
load alternate third-party drivers, 731
load balancers, 920
loading apps, troubleshooting, 419
local access, security
        AD functions, 885-886
        group policies, 889
        local security policies, 889
        user management, 884
local connectivity, 575
local security policies, 889
local shares, 893
Local Users and Groups tool, Windows, 762-763
locate command, Linux, 845, 853
location tracking, unauthorized, 414
locator apps, 369-370
locked/frozen systems, troubleshooting, 784
locking computers, 885
lockouts, system, 413
locks
    cable locks, 865
    equipment locks, 865
    facial recognition locks, 412
    fingerprint locks, 412
    mobile devices, 412
    physical security, 863-865
    screen locks, 412
    swipe locks, 412
    timeout/screen locks, 890
    USB locks, 865

INDEX

logging off when not in use, 875
logging servers, 585
logical drives, 233
logical operators, testing conditions, 708
logical partitions, 728
logical security
ACL, 871
anti-malware, 870
antivirus software, 870
authentication, 872-873
BIOS/UEFI, 873-874
directory services, 870
firewalls, 870
identity access management, 870
login OS security, 874-875
ports, 871
principle of least privilege, 871
trusted/untrusted sources, 871
unused ports, disabling, 871
VPN, 871
Zero Trust models, 870
logins
Apple ID, 823
failed attempts, 413
failed login attempts, 875
OS security, 874-875
restricting login times, 890
scripts, 888
logistics, audio subsystems, 450
logs
application logs, 757-758
auditing, 890
event logs, 890
Event Viewer, 756-759
security logs, 757-758
service logs, 757
setup logs, 757
system logs, 757-758
vendor specific logs, 757
LoJacks
BIOS/UEFI, 109
physical security, 873
long-range fixed wireless connectivity, 490
long touch/touch and hold actions (mobile devices), 365
loopback plugs, 459, 537
loops, 708
for loops, 709-711
iteration, 709
structures, 704
while loops, 709, 710
loss of data/corruption
OS update limitations, 620
troubleshooting, 245
lost clusters, 243
low-level formatting, 229, 904
low RF signals, 559
LPCAMM (Low-Power Compression Attached Memory Modules), 400
ls command, macOS, 835
LTE (Long Term Evolution), 367, 490
lumens, monitors/projectors, 275

M

M.2 devices, 218-219
BIOS/UEFI settings, 228
expansion cards, 390
MAC addresses, 921
filtering, 924
formats of, 542
macOS, 616, 818
Activity Monitor, 830
.app files, 824
Apple ID, 823
apps, installing, 824
App Store, 823-824
best practices, 854
Boot Camp, 834
cd command, 835-836
chmod command, 835-838
chown command, 835-837
Console, 831
cp command, 835-836
deleted files, recovering, 826
desktop, 819-820
Disk Utility, 833-834
.dmg files, 824
Dock, 819-821
Finder, 819
Force Quit, 826
gestures, 822
grep command, 835, 838
GUI, 819-821
iCloud, 822
iWork, 822
kernel panic, troubleshooting, 831
Keychain Access, 832-833
kill command, 835
Launchpad, 821
less command, 835, 838
ls command, 835
man command, 835, 839
memory recommendations, 183
menu bar, 819
Mission Control, 820
mkdir command, 835
mv command, 835-836
nano command, 835, 838
Notification Center, 820
Passwords app, 832
pinwheels, 830
.pkg files, 824
POSIX, 819
pwd command, 835-836
releases, 818-819
rm command, 835-836
root user accounts, 836
Safe mode, 829
screen-sharing, 823-824
screenshots, 7
Spotlight, 821
su command, 835
sudo command, 835-836
system folders, 823
System Information, 831
System Settings, 827-829
system updates, 824
Terminal, 834
Time Machine, 825-826
touch command, 835-836
troubleshooting, 829-831
utilities
Activity Monitor, 830
Boot Camp, 834
Console, 831
Disk Utility, 833-834
Keychain Access, 832-833
System Information, 831
Terminal, 834
vi command, 835
Widgets, 820

magnetic hard drives, 215
magnetic screwdrivers, 139
magnetometers, physical security, 866
mail servers, 585
main menu, UEFI, 106
maintenance. *See also* troubleshooting
  aerosol cans, disposal laws, 149
  air filtration masks, 149
  antistatic brushes, 148
  antistatic wristbands/gloves, 78
  bootups, 148
  CD, 287
  compressed air, 148-150
  CPU, 79
  disks, 768-769
  displays, 148
  dust, preventive maintenance, 147, 945, 957
  DVD, 287
  general-purpose cleansers, 148
  general-purpose cloths, 148
  gold contact cleaners, 148
  inkjet printers, 319-321
  kits, 148
  laser printers, 321-323
  lens cleaners, 148
  lint-free cloths, 148
  monitor wipes, 148
  mouse/mice, 15
  MSDS, 149
  optical drives, 148, 287
  OS, 803-804
  portable vacuums, 148
  printers, 318-319, 324
  projectors, 275
  safety, 20
  safety goggles, 149
  scanners, 289
  SDS, 149
  thermal paste, 78
  thermal printers, 324
  toner vacuums, 148
  urethane swabs, 148
  vacuum bags, 148
  vacuuming, 150
maintenance counters, resetting, 323
Maintenance option, AP configurations, 571
maintenance windows, 964
making/keeping commitments (soft skills), 972
malfunctioning keys (keyboard), troubleshooting, 16
malicious apps, 411
malware, 880
  anti-malware, 870
    initializing, 735
    mobile devices, 386
    security policies, 862
  fileless malware, 879
  mobile devices, 386
  removing, 907-908
  Trojan malware, 878-879
MAM (Mobile Application Management), 385
man command, macOS, 835, 839
MAN (Metropolitan Area Networks), 518
managed/unmanaged switches, 520
managing
  assets, 963
  cable management, 535, 942
  Certificate Manager, 907
  change management, 964-966
  CMDB, 963
  Computer Management console, Windows, 754
    Disk Management tool, 765-767
    Local Users and Groups tool, 762-764
    ODBC Data Sources tool, 770
    Print Management console, 771
    Services and Applications section, 769
    Storage Spaces Control Panel, 768
    System Tools section, 755-759
    User Account Management section, 759
  Device Manager, 743-748
  Disk Management tool, 765-767
  DRM, 876
  files
    File Explorer (Windows 11), 630
    Linux, 841
    Nautilus file manager, Ubuntu, 841
  hard drives
    Disks, Linux, 842
    Disk Utility, macOS, 833-834
  identity access, 870
  inventory, 963
  macOS, 827-829
  MDM, 385, 922
  PAM, 873
  passwords, 875
  patches, 898
  power, USB ports, 119-120
  Print Management console, Windows, 771
  risk, levels of, 965
  secure management access, 571
  storage, Disk Management tool, 765-767
  Task Manager, Windows, 782
  throttle management, 80
  time (soft skills), 971
  updates, 898
  user accounts
    Credential Manager, 759, 762
    editing credentials, 762-764
    Local Users and Groups tool, 762-763
    recovering accounts, 763-764
    rights, 762
    UAC, 764
  users, 884
  UTM systems, 920
mantraps (access control vestibules), physical security, 866-867
manually deleting files, 909
manually installing device drivers, 748
manual paper feeds, 315
manufacturer's advice, ignoring, 117
mapping
  network shares, 596-597
  ports, 571, 917
masks, air filtration, 149

INDEX

matching
cases with motherboard form factors, 89
monitors to port type, 40
motherboard form factors with cases, 89
mATX (microATX), motherboards, 88
MB (Megabytes), 19-20
MBR (Master Boot Records)
converting to GPT, 235
features of, 234-235
partition tables, 728
md command, 662-663, 679
MDM (Mobile Device Management), 385, 922
MDR (Managed Detection and Response), 884
MDT (Microsoft Deployment Toolkit), 734
mechanical hard drives, 402-404
meeting expectations (soft skills), 974
memory, 14
addresses, 114
advertisements, 189
app crashes, 195
"BIOS ROM checksum" error messages, 456
buffered memory, 181
buying, 189
cache memory, 178
caches, 69
card readers, 199, 361
cards, 198
CL ratings, 189
CMOS, 110
crashes, 195
DDR memory, 179-180
DIMM
advertisements, 189
installing, 191
models of, 181
physical packaging, 178-179
removing, 190
solutions, 188
DRAM, 178
dual-channel memory, 185-188
dual rank, 182
dual voltage memory, 182
ECC RAM, 181
error messages, 457
flash drives, 197-198
flash memory, 197
memory card readers, 361
SD cards, 360-361
SSD, 402-404
SSHD, 218
hard drives, space allocation, 178
installing, 191
laptops, 401
overview, 190
safety, 190
viewing amount of installed memory, 184
intermittent shutdowns, 195
laptops, 400-401
limitations
motherboards, 184
Windows, 183-184
LPCAMM, laptops, 400
Memory Diagnostic tool (Windows), 196
module pairs, 187
monitoring usage, 193-194
motherboards
documentation, 182, 188
limitations, 184
slots, 187-188
Non-ECC RAM, 181
non-parity, 189
NVMe
cards, 391
SSD, 218
OS recommendations, 183
"out of memory" error messages, 195
pages, 243
performance, 189
physical packaging, 178-179
planning installations
how many of each memory type, 185-188
how much memory to install, 182
memory features, 181
memory modules, 179-184
researching/buying memory, 189
POST
beeps, 195
error messages, 191
upgrading memory, 196
printers, 341
quad-channel memory, 188
RAM, 12, 178
4GB, 185
disk caches, 243
ECC RAM, 181
laptops, 360, 400
limitations, 617
Non-ECC RAM, 181
OS requirements, 751
power requirements, 161
virtual memory, 241
VRAM, 268, 751
registered memory, 181
removable storage, 198-199
removing, 190, 401
researching, 189
ROM, "BIOS ROM checksum" error messages, 456
SDRAM, 180
shared system memory, 268
single rank, 182
sluggish performance, 195
SODIMM, 178-179, 400
SPD, 182
speeds, 189
SRAM, 178
system design, 447
triple-channel memory, 188
troubleshooting, 195-196
performance, 785
POST error messages, 191
unbuffered memory, 181
upgrading, 183, 196, 400
video memory, 178, 268-269
virtual memory, 241, 786
VRAM, 192-193, 751
Windows performance, 785
XMP, 182
Memory tab, Task Manager, 786
mentoring (soft skills), 509
menu bar, macOS, 819
menus
files, sharing, 898
UEFI, 106-107

messages
Console messages (macOS), 831
error messages, 455
"array missing", 251
BIOS ROM checksum, 456
"Bootable device not found.", 113, 248
CMOS, 456-457
"drive not recognized", 246
hard drive installations, 456
intruder detection errors, 456
"Invalid Boot Disk", 773
keyboards, 456
memory, 457
motherboards, 457
"no OS found", 248, 737
"Not enough USB controller resources", 749-750
"not responding", 757
NTLDR Is Missing, 736
POST, 191
"RAID array missing," 251
"RAID not found", 251
"tray not recognized", 340
metered connections, 591
metered utilization services, 508
meters, digital, 152
MiB (Mebibytes), 20
mice/mouse
defined, 14
ports, 30, 54
preventive maintenance, 15
troubleshooting, 16
microATX
motherboards, 88
power supplies, 154
microphones, 17
choosing, 280-281
headsets, 362-363
laptops, 407-410
system design, 450
Windows operations, 280-281
microSD cards, 361
Microsoft
Defender Antivirus, 906
Edge, 493-497
OneDrive, 381
Store, 722
Windows. *See* individual entry
microUSB ports, 33, 371-372
migrating USMT, 726
MIME (Multipurpose Internet Mail Extensions), 379
MIMO (Multiple Input/Multiple Output) antennas, 558
mini-DIN ports, 30
mini DisplayPort, 389
mini-LED displays, 264
miniPCIe cards, 389
miniPCI/PCIe adapters, installing, 390
miniUSB ports, 33, 371-372
mirroring (RAID 1), disk, 239
misfeeds, troubleshooting, 339
missing
bootloaders, troubleshooting, 854
drives in the OS, 246
files, viruses/malware attacks, 880
Task Manager tabs, trouble-shooting, 782
Mission Control, macOS, 820
MITM (Man-In-The-Middle) attacks, 883
mITX (mini-ITX), 88
mkdir command, 662-663, 679, 835
MMC (Microsoft Management Console)
mmc command, 679
Services window, 686
MNDA (Mutual Non-Disclosure Agreements), 875
mobile connectivity. *See also* Internet, connectivity
cellular networks, 490
hotspots, 489
licensed ranges, 490
long-range fixed wireless, 490
overview, 489
power requirements, 491-492
tethering, 489
unlicensed ranges, 491
WAN, 490
wireless broadband, 490
WISP, 490
mobile devices
accessories, 362-364
Android OS, 360, 380, 619
anti-malware, 386
antivirus software, 386
apps
APK, 371
common apps, 369
deleting, 418-419
installing, 371
locator apps, 369-370
MAM, 385
obtaining, 371
removing, 371
SDK, 371
side-loading, 371
troubleshooting, 418-419
app scanners, 386
backups, 384-385
blocking ads, 379
cell tower analyzers, 387
cellular location services, 369-370
cellular networks, 366-367
Chrome OS, 360, 619
connectivity, synchronization, 382
degraded response times, 411
disposal/recycling, 946
double-tap actions, 365
drawing pads, 358
email configuration, 379-380
e-readers, 359
geotracking, 369-370
GPS, 358, 369
interacting with, 365-366
iOS, 360, 380, 619
iPadOS, 360, 619
keyboards, troubleshooting, 420
long touch/touch and hold actions, 365
malicious apps, 411
malware, 386
MAM, 385
MDM, 385, 922
mobile OS
Android, 371
Android OS, 383-384
emergency notifications, 370
features of, 370-371
Internet calling, 370
iOS, 383-384
mobile payment services, 370-371

INDEX

Recovery Mode, 416
updating, 411
virtual assistants, 370
Wi-Fi calling, 370
moving, 365-366
multitouch techniques, 365-366
network configurations, 376
performance, troubleshooting, 423
phablets, 358
pinch open/close actions, 366
remote wipes, 411
screens, troubleshooting, 421-422
scrolling actions, 366
security, 410, 923, 927-928
authenticator apps, 412
biometric security, 412
data-usage limit notifications, 414
DMZ, 924
facial recognition locks, 412
failed login attempts, 413
fake security warning, 411
fingerprint locks, 412
IP address filtering, 925
jailbreaking, 414-415
leaked personal files/data, 414
MAC address filtering, 924
malicious apps, 411
patterns, 412
PIN codes, 412
screen locks, 412
spoofing apps, 411
swipe locks, 412
system lockouts, 413
TKIP, 923
unauthorized account access, 413
unauthorized apps, 411
unauthorized location tracking, 414
unauthorized root access, 414-415
USS, 410
WEP, 923
Windows Hello, 412
WPA, 923
WPA2, 923
WPA3, 923
WPS, 925
sleep mode, 366
sluggish response times, 411
smart cameras, 359
smartphones, 358
cellular networks, 366-367
eSIM cards, 368
IMEI, 367
IMSI, 368
SIM cards, 368
spoofing apps, 411
spreading/pinching open actions, 366
storage
flash memory, 360
memory card readers, 361
RAM, laptops, 360
SD cards, 360-361
swipe/flick actions, 366
synchronization, 381-384
tablets, 358
touch/tap actions, 365
trackpads, troubleshooting, 421
troubleshooting
app closure failures, 418
app installation failures, 419
app load failures, 419
app update failures, 419
autorotating screens, 421
backlight failures, 421
battery failures, 423-424
Bluetooth connectivity, 426-427
damaged ports, 415
dim displays, 421
flickering displays, 422
frozen systems, 424
GPS, 426
hard resets, 416-417
keyboards, 420
liquid damage, 415
network issues, 425-426
NFC, 427
no display, 421
no power, 424
OS update failures, 417
overheating, 424
performance, 423
question marks (?), 426
random reboots, 415
soft resets, 416
touch screens, 422
trackpads, 421
unexpected app behavior, 418
Wi-Fi connectivity, 425-426
unauthorized apps, 411
unlocking, 366
using, 364-366
viruses, 386
WAN connectivity, 490
Wi-Fi analyzers, 386
wired connectivity, 373
Lightning ports, 372
microUSB ports, 371-372
miniUSB ports, 371-372
proprietary vendor specific ports, 371
USB-C ports, 371-372
wireless connectivity
802.11 wireless standard, 375-376
Airplane mode, 376
biometric security, 378
Bluetooth, 373-374
cellular data, 379
cellular networks, 490
hotspots, 377, 489
IR, 379
long-range fixed wireless, 490
NFC, 377-378
power requirements, 491-492
tethering, 377, 489
wireless broadband, 490
zooming in/out of objects, 366
mobile digital keys, 865
mobile docking stations, 362-363
mobile hotspots, 489
mobile motherboards (system boards), 395
mobile OS
Android OS
APK, 371
backups, 384
developer mode, 371
factory resets, 384
Recovery Mode, 416
synchronization, 383
emergency notifications, 370
features of, 370-371
Internet calling, 370
iOS, 383-384
payment services, 370-371
updating, 411

virtual assistants, 370
Wi-Fi calling, 370
mobile payment services, 370-371
mobile wallets, 371
modems
cable modems, 44, 482-483, 581-582
cabling, 480
dial-up connectivity, 480-482
DSL modems, troubleshooting, 581-582
Internet connectivity, 480-482
ports, 480
RJ11 ports, 44
satellite modems, 488-489
serial transmissions, 480-481
xDSL modems, 483-484
Modify permissions, 895
modular power supplies, 162
module pairs, memory, 187
Molex-to-SATA converters, 156
monitoring
memory usage, 193-194
RMM, 919
Windows performance, 784
baselines, 785
Performance Monitor, 787-788
Reliability Monitor, 789
Resource Monitor, 788
Task Manager, 785-787
monitors. *See* displays
more command, 680
motherboards
24-pin power connectors, 142
adapters
identifying function, 13
installing, 13-14
ATX, 88
audio ports, 277
batteries, 111
BIOS, 104
caches, 69-72
cases, matching with, 89
clock speeds, 69
connectivity
20-pin motherboard connectors, 155
24-pin motherboard connectors, 155
ATX power supply connectors, 154-157
front panel connectors, 142
pins, 143
CPU
cooling, 77, 81
fans, 81-82
handling, 79
heat sinks, 81
installing, 79-81
photographing prior to installations/upgrades, 81
thermal paste, 81
thermal solutions, 81
throttle management, 80
troubleshooting, unusual noises, 83
unusual noises, 83
upgrading, 80
CPU sockets, 76
defined, 12
disabling, 279
ED, boot/driver failures, 246
error messages, 457
expansion slots, 13-14, 83
form factors, 88-89, 154
headers, 36
HSM, 88
installing, 89-90
integrated ports, adapters, 53
I/O shields, 145
ITX, 88
LED, 458
memory, 12-14
documentation, 182, 188
limitations, 184
slots, 187-188
microATX, 88
mITX, 88
mobile motherboards (system boards), 395
multisocket, 76
performance, 68-69
power supply connectivity, 153
processors
AMD, 66-67, 75-76
APU, 72
ARM, 66
buses, 67-70
connectivity, 70
cooling, 77, 81
Core 3, 74
Core 5, 74
Core 7, 74
Core 9, 74
cores, 72
Core Ultra x, 74
CPU, 69
defined, 66
fans, 81-82
GPGPU, 72
GPU, 72
heat sinks, 81
iGPU, 72
installing, 78, 81
Intel, 66-67, 74-75
multicore, 71
overclocking, 80
performance, 67-68
power requirements, 161
Ryzen 3, 75
Ryzen 5, 75
Ryzen 7, 75
Ryzen 9, 75
Ryzen AI, 75
Ryzen Threadripper, 75
SoC, 66
speeds, 67-68
thermal solutions, 81
threads, 71-72
throttle management, 80
troubleshooting, unusual noises, 83
unusual noises, 83
upgrading, 80
virtualization, 73-74
x64, 66
x86, 66
Xeon, 74
reassembling computers, 147
reinstalling, 147
removing, 145
replacing, 89-90
security, 87
sockets, 76
sound card installation, 279
speakers, 276
speeds, 68
standoffs, 145
switches, 458
system design, 447

TPM, 87
troubleshooting, 90-91
types of, 88, 154
upgrading, 89-90
ZIF sockets, 76
motion sensors, physical security, 866
mount command, Linux, 845
mounting
eSATA drives, 225-226
hard drives, 767
mouse/mice
optical mouse/mice, 14-16
ports, 30, 54
preventive maintenance, 15
troubleshooting, 16
moving
between screens, mobile devices, 366
icons on mobile devices, 365
in NTFS permissions, 895
through lists/images, 366
Windows files/folders, 640
MOV (Metal Oxide Varistors), 952
.MPG (.MPEG) files, 631
mSATA, 220
BIOS/UEFI settings, 228
drives, 402
installing, 225
msconfig command, 680
MSDS (Material Safety Data Sheets), 149, 943
msinfo32 command, 680
mstsc command, 680, 801
MTBF (Mean Time Between Failures), 216
multiboots, Windows, 723
multi-card readers, 361
multicore processors, 71
multifactor authentication, 872
multifunction (all-in-one) devices. *See also* printers
installing, 326
overview, 302
sensitive material, 302
sharing, 582, 583
troubleshooting, 583
wireless networks, 548
multimedia devices
audio
microphones, 280-281
motherboard audio ports, 277
motherboard speakers, 276
ports, 278
sound cards, 277-280
speakers, 281-283
troubleshooting, 282-283
cameras, 290-291
digitizers, 291
displays, 264-266
integrated graphics cards, 266
optical drives, 284-287
projectors, 274-276
scanners, 288-289
video
adapter installations, 269-270
memory, 268-269
overview, 264
subsystems, 264
systems, 270
troubleshooting, 270-271
video cards, 269-270
video cards
AMD processors, 268
capture cards, 268
dGPU, 267
iGPU, 266
power connectors, 267
webcams, 290-291
multimeters, 151, 537
multi-mode fiber cables, 52
multi-monitor taskbars, 722
multipage misfeeds, troubleshooting, 339
multipart paper, 305
multiple alternative structures, 706-707
multiple-device ports, IRQ, 114
multiple displays, 747
multiple hard drives as backups, 900
multiple pending print jobs, 343
multipurpose ports, 37-38
multisocket motherboards, 76
multitenancy, 508
multitouch techniques, 365-366
MU-MIMO (Multi-User MIMO) antennas, 558
muting sound cards, 280
mv command, macOS, 835-836
MX records, DNS, 565

N

N versions, Windows 10/11, 618
name resolution, DNS, 566
naming
computers, 559
directories, 657, 686
files, 631, 657, 686
folders, 631
variables, 700-701
nano command, macOS, 835, 838
NAS (Network-Attached Storage)
drives, 219
system design, 443
NAT (Network Address Translation), 587, 917
DNAT, 571
virtual NIC, 570
wireless networks, 571
native (Type 1) hypervisors, 501
Nautilus file manager, Ubuntu, 841
navigating
directories
cd command, 659-660
dir command, 660-662
md command, 662-663
mkdir command, 662-663
rd command, 663
rmdir command, 663
drive navigation inputs, 669
macOS GUI
Dock, 819-820
Finder, 819
gestures, 822
Launchpad, 821
menu bar, 819
Mission Control, 820
Spotlight, 821
NBT (NetBIOS over TCP/IP), 589
nbtstat command, 681
NDA (Non-Disclosure Agreements), 875
needle-nose pliers, 139
net command, 578, 681
.NET Core, 712
net use command, 681
net user command, 682

netdom command, 579, 682
netstat command, 588, 683
Network Access layer, TCP/IP, 541, 590
network (breakout) taps, 537
Network layer (OSI model), 540
Network tile, Windows Start screen, 628
networks
  access
    attacks, 882
    security, 884-886, 889
    remote access, 918
    user management, 884
  adapters, ipconfig command, 678-679
  adding computers to domains, 566-567
  antennas, 541, 556-558
  AP, 541, 548-549
    DMZ, 571
    SSID, 551
    wireless AP, 570
    as wireless repeaters, 552
  ARP, 587
  authentication, troubleshooting, 585
  backdoor attacks, 882
  bandwidth, 587
  Bluetooth
    device verification, 594
    PAN, 519
  botnets, 882
  boots/PXE, 772
  bridges, wireless, 548
  broadband, 587
  brute force attacks, 882
  cabinets, 535
  cable modems, troubleshooting, 581-582
  cabling
    cabinets, 535
    connectors, 541
    copper, 526
    management systems, 535
    racks, 535
    twisted pair cables, 526-532
  cellular networks, 366
    3G networks, 367, 490
    4G networks, 367, 490
    5G networks, 367, 490
    CDMA, 367
    connectivity, 490
    GSM, 367
    LTE networks, 490
  cloud-based network controllers, 505-506
  configuration operators accounts, 885
  configuring, ifconfig command (Linux), 846
  connectivity
    cable management systems, 535
    cabling cabinets, 535
    cabling racks, 535
    direct burial cables, 526
    EoP, 534
    local connectivity, 575
    PoE, 533
    twisted pair cables, 526-532
    unintentional connections, troubleshooting, 426
  corporate networks
    cabling, 531-532
    disk imaging, 733
    Windows deployments, 733-734
  DDOS attacks, 882
  DHCP, 562
  dial-up networks, 480-482
  dictionary attacks, 882
  domains, 521-523, 566-567, 733
  DoS attacks, 882
  DSL modems, troubleshooting, 581-582
  embedded systems, 585
  end devices, IP addressing, 560
    alternative IP address configurations, 563
    APIPA, 563
    default gateways, 564-565
    DNS, 565-566
    static configurations, 560-561
  Ethernet networks
    EoP, 534
    LAN, 519
    PoE, 533
    star topologies, 520
  evil twin attacks, 882
  examples of, 518
  extenders, wireless, 551
  external networks, VM, 502
  fiber networks, 486-488
  high network traffic, 425
  hubs, 519-520, 541
  ICMP, 587
  insider attacks, 882
  internal networks, VM, 502
  IPv4 addressing, 542-546
  IPv6 addressing, 542
  ladder racks, 535
  LAN, 520
    Ethernet LAN, 519
    VLAN, 545
    Wake on LAN, NIC, 569
    WLAN, 518-523, 921
    workgroups, 521-523
  latency, 486, 577
  legacy systems, 586
  MAC addressing, 541-542
  MAN, 518
  MITM attacks, 883
  mobile device configurations, 376
  multifunction devices
    sharing, 582-583
    troubleshooting, 583
  naming computers, 559
  NAS devices, system design, 443
  NAT, 587, 917
  NIC, 548-549, 567-570
  NOC, 523
  numbers, IPv4 addressing, 543
  OSI model, 538-541
  PAN, 518-519
  password spraying attacks, 883
  PAT, 587
  patch panels, 531
  paths, 595
  PCs without switches or hubs, 529
  phone networks, RJ11 ports, 44
  physical addresses, 542
  PoE, 533
  ports, 46
  printers, 332-333, 344-345
    accessing, 336
    sharing, 582-583

troubleshooting, 583
wireless printers, 548
private networks, 523, 732
protocols, 540
public networks, 523, 732-733
racks, 535
reconnaissance attacks, 883
remapping drives, 695
remote access, 918
remote networks
accessing, 689
ping command, 684-685
Windows installations, 723
repeaters, wireless, 552
replay attacks, 883
RJ45 wall jacks, 532
routers, 540-541
DMZ, 571
wireless routers, 548-549, 570
SAN, 518, 524
SCADA systems, 585
scanners, 583
SDN, 586
selecting during OS installations, 732-733
servers, 584-585
shares (shared folders), 594-597
slow speeds, 559
Smurf attacks, 883
SNMP, 590
spoofing attacks, 883
SQL injection attacks, 883
SSL, 587
star topologies, 520
status, troubleshooting, 573-574
subnet masks, 545-546, 985-987
switches, 519-520, 541
TCP, 588
TCP/IP, 540
Application layer, 541
devices, 541
example of, 588-590
hijacking attacks, 883
Internet layer, 541
Network Access layer, 541
Transport layer, 541
TLS, 587
topology diagrams, 960
troubleshooting
authentication issues, 585
Bluetooth connectivity, 426-427
GPS, 426
high traffic, 425
ifconfig command, 576
ipconfig command, 576
net command, 578
netdom command, 579
NFC, 427
nslookup command, 578
pathping command, 577
ping command, 574-576
status, 573-574
tracert command, 577
unavailable resources, 575-576
Wi-Fi connectivity, 425-426
twisted pair cables
corporate networks, 531-532
RJ11 connectors, 527-530
RJ45 connectors, 527-530
STP cables, 526-527
terminating, 527-530
UTP cables, 526-530
types of, 518, 733
UDP, 588
virtual networks, VNC, 918
VLAN, 545
VPN, 871, 919-920
vulnerability scanners, 883
WAN, 518
wireless broadband connectivity, 490
WWAN, 572
WAP, 541
Windows network settings, 590-594, 796-797
wired networks
device connectivity, 559
printer connectivity, 325
wireless networks
802.11ac (Wi-Fi 5) wireless standard, 548
802.11ad (WiGig) wireless standard, 548
802.11a wireless standard, 548
802.11ax (Wi-Fi 6) wireless standard, 548
802.11be (Wi-Fi 7) wireless standard, 548
802.11b wireless standard, 548
802.11e wireless standard, 548
802.11g wireless standard, 548
802.11i wireless standard, 548
802.11n wireless standard, 548
antennas, 541, 556-558
AP, 548-552, 921, 926-927
Basic QoS, 571
bridges, 548
channel ID, 553, 554-556, 571
configuration profiles, 922
content filtering, 571
data transfer speeds, 559
design, 550
desktop workstations, 547
device connectivity, 559
DHCP, 571
DMZ, 571
DNAT, 571
extenders, 551
external interference, 558-559
firewalls, 922
firmware, 571
frequencies, 546, 550
guest access, 927
intermittent wireless connectivity, 558
IoT, 572-573
IP filtering, 571
Mac addresses, 921
MDM, 922
multifunction devices, 548
NAT, 571
NIC, 548-549
overview, 546
port forwarding/mapping, 571
printer connectivity, 325, 334-335
reducing transmit power, 926
regulations, 556
repeaters, 552
routers, 541, 548-549, 926-927
security, 923-928
signal strength, 426
site surveys, 557

SSID, 571
troubleshooting, 928
UPNP, 571
Wi-Fi analyzers, 558
WLAN, 518, 523, 921
WMN, 518
WWAN, 518, 572
WLAN, 518, 523, 921
WMN, 518
workgroups, 521-523, 733
WWAN, 518, 572
XSS attacks, 883
zero-day attacks, 883
zombie attacks, 883
new user/exiting user checklists, 960
NFC (Near Field Communication), 55, 377-378, 427
NIC (Network Interface Cards), 46
advanced properties, 568-569
configuring, 569-570
duplexing, 569
installing, 121
on-board NIC (BIOS/UEFI), 569
QoS, 569
speed, 569
static IP addressing, 560
TCP/IP protocol stacks, checking, 576
troubleshooting, 579-581
virtual NIC, 504, 569-570
Wake on LAN, 569
Windows network settings, 592-594
wireless NIC, 376, 548-549, 567-568
NLQ mode, inkjet printers, 306
no Bluetooth connectivity, troubleshooting, 426-427
no connectivity, troubleshooting, 425-427, 574-576
no display, troubleshooting, 421
"no OS found" error messages, 248, 737
no power, troubleshooting, 163, 424
NOC (Network Operations Centers), 523
noises, troubleshooting, 83, 163
hard drives, 404
printers, 311, 339
troubleshooting, 163
nonbootable disks/media, 791
non-compliant systems, security, 862
Non-ECC RAM (Non-Error Correction Code RAM), 181
nonfunctioning/undetected devices, troubleshooting, 747-748
non-IT personnel, addressing, 56
nonoverlapping channel ID, 553
non-parity memory, 189
nonvideo adapters, power requirements, 161
normal changes. change management, 965
"Not enough USB controller resources" error messages, 749-750
not equal to (!=) operators, 705
"Not Initialized" status messages, 250
NOT operators, 708
"not responding" error messages, troubleshooting, 757
Notepad, 683
batch scripting, 692
printing from, 342
notification area
removing icons from, 749
Windows 11, 627
Notification Center, macOS, 820
notifications
data-usage limit notifications, 414
emergency notifications, 370
fake security warnings, mobile devices, 411
Intrusion Detection/Notification setting (BIOS/UEFI), 109
unknown notifications, OS security, 898
NPU (Neural Processing Units), 71
nslookup command, 578, 683
NTFS (New Technology File Systems), 230, 236, 728
benefits of, 232
boot partitions, 234
clusters, 231
disk quotas, 232
partitioning, volume structures, 235
permissions, 891, 894-896
system partitions, 234
"NTLDR Is Missing" error messages, 736
NTP (Network Time Protocol), 585, 589
NUM LOCK key, 16
number of characters, passwords, 874
Numlock on/off setting (BIOS/UEFI), 108
NVMe (Non-Volatile Memory Express)
BIOS/UEFI settings, 228
cards, 391
SSD, 218

O

objectives, exam, 5
octets, IPv4 addressing, 542
ODBC (Open Database Connectivity), Data Sources tool, 770
ODD. *See* optical drives
OEM (Original Equipment Manufacturer) versions of Windows, 725
offer remote assistance helper accounts, 885
office productivity, iWork (macOS), 822
Offline status messages, 250
off-site backups, 902
off-site email apps, 505
off-site storage, 214, 900
ohms, 152, 153
older apps, Windows compatibility, 195
OLED displays, 264
omnidirectional antennas, 556
on-board NIC (BIOS/UEFI), 569
on-site storage, 900
Onboard Device Configuration setting (BIOS/UEFI), 108
ONE files, 631
OneDrive, 381, 722
Online (errors) status messages, 250
online resources, exam preparation, 5
ONT (Optical Network Terminal) boxes, 487
OOBE (Out-of-Box Experience), Windows, 623, 732
OpenDNS, 909-910
open-ended questions, 2
open source software, 818, 876

opening
apps, 365
cases (disassembly), 141
MMC, 686
PowerShell, 666
System Information window, 680
operating costs, OS, 620
operational procedures
business process documentation, 964
cable management, 942
change management, 964-965
component handling/storage, 949-950
documentation, 942
dust cleanup, 957
electronic disposal/recycling, 946-948
IT documentation
AI, 961
asset management, 963
AUP, 964
examples of, 959
incident documentation, 962
knowledge bases/articles, 961
network topology diagrams, 960
new user/exiting user checklists, 960
password policies, 963
regulatory/compliance policies, 964
security policies, 964
SLA, 960
SOP, 959
overview, 942
PM/airborne particle pollution, 957
power handling
adverse power conditions, 951
battery backups, 954
line conditioners, 953
MOV, 952
SPS, 956
surge suppressors, 951-953
UPS, 954-956
temperature/humidity control, 958
toner safety/disposal, 948-949
ventilation, 959
workplace safety
environmental impacts, 945-946
equipment, 944
fire safety, 943
government regulations, 942
lifting techniques, 945
MSDS, 943
OSHA, 943
personal safety, 945
optical cables. *See* fiber cables
optical drives, 10-11, 772
cleaning kits, 148
connectivity, 285
DirectX, 287
DVD/Blu-ray region codes, 285
features of, 284-285
installing, 286
interfaces, 285
ISO files/images, 285
laptops and external optical drives, 389
overview, 283-284
power requirements, 161
preventive maintenance, 287
reading Blu-ray discs, 284
symbols, 285
testing, 286
troubleshooting, 286-287
writable media, 284
optical mouse/mice, 14-16
optimizing
battery performance, laptops, 393-394
DPI, inkjet printers, 305-307
General Optimization setting (BIOS/UEFI), 107
Optimize Drives tools, Windows, 768-769
Options button, File Explorer (Windows 11), 635
order of volatility, 929
organizing
desktops, Windows 11, 627
files, 657
laptop repairs, 394
soft skills, 968
orientation
displays, 747
pages, printers, 329-330, 344
OR operators, 708
OSHA (Occupational Safety and Health Administration), 943
OSI (Open Systems Interconnect) model, 538-541
OTP (One-Time Passwords/Passcodes), 872
OU (Organizational Units), 886
out of memory error messages, 195
output. *See* input/output
overclocking, 80
overheating
printers, 305
troubleshooting, 90, 163, 424
overvoltage, 951

P

P2P (Peer-to-Peer) gaming, 571
PaaS (Platform as a Service), 504
paaswd command, Linux, 845
packages
memory, 178-179
software, pre-downloading, 849
packets
OSI model, 539
tracert command, 690
pages
memory, 243
orientation, 329-330, 344
paging files, 192
palm print scanners, physical security, 868
PAM (Privileged Access Management), 873
PAN (Personal Area Networks), 518-519
paper
collating pages, 330
feeds, 313-315, 318, 339
hole punched paper, 341
humidity, 313
impact printers, 319
incorrect paper sizes, troubleshooting, 340
jams, 339

lines down printed pages, troubleshooting, 339
multipage misfeeds, troubleshooting, 339
multipart, 305
orientation, 329-330, 344
pounds (lb), 313
printer trays, 313-315, 318
properties, printing, 315
ratings, 313
sources (printing), 330
speckling, troubleshooting
inkjet printers, 345
laser printers, 346
staple jams, troubleshooting, 341
thermal paper, 312, 324
tractor feeds, 313
trays, 330
two-sided printing, 313
paper trays/feeders, inkjet printers, 306
parent directory (..), 668
parental controls, 929
partitioning
apps, 231
basic disks, 727
boot partitions, 234, 773
cloned partitions, 852
convert command, 730
converting, 231
data files, 231
deleting, 234
diskpart command, 675
Disks, Linux, 852
cloned partitions, 852
unusable partitions, 852
drive partitions (volumes), 729
dynamic disks, 728
eSATA drives, 233
extended partitions, 233, 728, 767
FAT32 file systems, 231
GPT
features of, 234-235
MBR conversions to GPT, 235
hard drives, 229-231, 772
internal hard drive partitions, 772
logical partitions, 728
MBR
converting to GPT, 235
features of, 234-235
partition tables, 728
planning drive space, 729
primary partitions, 233, 727
recovery partitions, 646, 723
resizing, 238
shrinking, 767
splitting, 767
swap partitions, 728
system partitions, 234
unusable partitions, 852
PASS method, fire extinguishers, 459
passwd command, Linux, 846
passwordless security, 874
passwords, 412
administrator accounts, changing default passwords, 885
AP, 926
BIOS/UEFI settings, 108
BitLocker Recovery Password Viewer, 623
boot passwords, 873
complexity, 874
expiration dates, 890
expired passwords, 875
failed login attacks, 875
formatting, 874
Keychain Access, macOS, 832-833
logging off when not in use, 875
managing, 492, 875
mobile device synchronization, 381
number of characters, 874
OTP, 872
passwd command, Linux, 846
policies, 963
power-on passwords, 873
rainbow tables, 883
reminders, 874
requiring, 890
security policies, 863
social engineering attacks, 875, 880
special characters, 874
spraying attacks, 883
TOTP, 872
uniqueness, 874
usernames, 874
wireless AP, 570
wireless routers, 570
Passwords app, macOS, 832
PAT (Port Address Translation), 587, 917
PATA IDE hard drives, power requirements, 161
patch panels, 531
patch (straight-through) cabling, 528
patches
browsers, 495
managing, 898
software, 460
path loss, antennas, 556
PATH variables, 696
pathping command, 577, 684
paths
files, Windows, 632-634
full paths, command prompt, 663
networks, 595
shortcuts, 627
patterns (mobile devices), security, 412
payment services, mobile, 370-371
PB (Petabytes), 20
PC (Personal Computers), 8
adapters, 13-14
components of, 9
expansion slots, 13-14
gaming PC, system design, 441
hard drives, 10
hibernation mode, 799
isolation, 498
keyboards, 14-16
memory, 12-14
motherboards, 12-14
mouse/mice, 14-16
networks without switches and hubs, 529
optical drives, 10-11
power supplies, 9-11
resetting, 791, 795
This PC tile, Windows Start screen, 628
tower cases, 10-11
virtualization, 498

PCI (Peripheral Component Interconnect)
adapters, 86
buses, speeds, 69
expansion slots, 83-85
lanes, 85
miniPCIe cards, 389
PCI DSS (Payment Card Industry Data Security Standard), 877
PCIe (PCI Express)
6-pin PCIe ATX power supply connectors, 154
8-pin PCIe ATX power supply connectors, 154
buses, speeds, 69
cards, M.2 devices, 219
dual Molex-to-PCIe converters, 156
video cards, power requirements, 161
expansion slots, 84
PCL (Printer Control Language), 330
PCmover Express, 726
.PCX files, 631
PD (Power Delivery), USB ports, 32
.PDF files, 316, 631
PDL (Page Description Language), 330
peer communication, OSI model, 539
peer reviews, 695, 964
peer-to-peer, NFC, 377
pending print jobs, 343
performance
baselines, 785
browsers, 497-498
buses, 68-70
clock speeds, 69
CPU, 69
defrag command, 673
Disk Cleanup, 244
laptop batteries, optimizing, 393-394
memory, 189
sluggish performance, 195
virtual memory, 786
motherboards, 68-69
NIC, 569
OS, 620
overclocking, 80
performance log user accounts, 885
Performance Monitor, measuring Windows performance, 787-788
Performance utility (Windows, Task Manager), monitoring memory usage, 193-194
processor speeds, 67-68
slow performance, troubleshooting, 423
boots, 795
browsers, 497-498
network speeds, 559
profile loads, troubleshooting, 795-796
storage devices, 243-244
systems, 784
Windows, 784
storage devices, 249
Disk Cleanup, 244
IOPS, 244
lost clusters, 243
system performance, troubleshooting, 784
throttle management, 80
troubleshooting, 423
boots, 795
browsers, 497-498
network speeds, 559
profile loads, 795-796
storage devices, 243-244
systems, 784
Windows, 784
virtual memory, 786
Windows
memory, 785
monitoring, 784-789
wireless networks, 559
performance-based questions, 5
Performance tab, Task Manager, 193-194, 782, 785-787
periods (.) in commands, 661
periods (..) in commands, 661
permanently deleting files, 628
permissions
Change permissions, 893
effective permissions, 896
Full Control permissions, 893-895
inherited permissions, 895
List Folder Contents permissions, 895
Modify permissions, 895
Read & Execute permissions, 895
Read permissions, 893-895
security permissions
changing, 891
NTFS permissions, 891, 894-896
running as administrators, 897
share permissions, 891-894
UAC, 897
USB Permissions setting (BIOS/UEFI), 108
user permissions, restricting, 890
Write permissions, 895
perpetual licenses, 876
personal appearance (soft skills), 428-429
personal files/data, leaked, 414
personal grooming (soft skills), 968
personal licenses, 876
personal safety, 945
perspectives on troubleshooting (soft skills), changing, 713-714
phase-change cooling, 77
PHI (Protected Health Information), 878
phishing, 881-882, 929
Phoenix, audio beeps, 456
phone filters, DSL lines, 484
phone networks
PHONE jacks, modem connectivity, 480
RJ11 ports, 44
VoIP, 484-486
phones. *See* smartphones
photographing CPU prior to installations/upgrades, 81
physical access, security policies, 862
physical addresses, 542
Physical layer (OSI model), 540
physical security
access control vestibules (mantraps), 866-867
alarm systems, 866
badge readers, 865
biometrics, 867-869
bollards, 863

cable locks, 865
documentation, 869
door locks, 863
equipment locks, 865
fingerprint scanners, 868
FRT, 868-869
guards, 865
hardware tokens, 865-866
HSM, 865
key cards, 864
key fobs, 865
keys, 863
lighting, 865
magnetometers, 866
mobile digital keys, 865
motion sensors, 866
palm print scanners, 868
privacy screens, 866
retinal scanners, 868
RFID, 865
smart cards, 865-866
tokens, 865
TPM, 865
USB locks, 865
video surveillance, 866
voice recognition, 868
physically damaged ports, troubleshooting, 415
PiB (Pebibytes), 20
picture passwords, 412
PID (Process ID), listing, 689
piggybacking, 881
PII (Personally Identifiable Information), 877
pin 1, cables, 142
PIN (Personal Identification Numbers), 412, 874
pinch open/close actions (mobile devices), 366
ping command, 574-576, 684-685
pinning apps to Windows 11 taskbars, 627
pins, motherboard connectivity, 143
pinwheels
macOS, 830
spinning, troubleshooting, 195, 250, 457
pipeline/supply chain attacks, 883
piracy, 876-877, 929
pixels (screens)
dead pixels, troubleshooting, 271
density, 265
pitch, 265
resolution, 275
.pkg files, 824
planning
hard drive space, 729
memory installations
how many of each memory type, 185-188
how much memory to install, 182
memory features, 181
memory modules, 179-184
researching/buying memory, 189
plans of action (troubleshooting process), establishing, 463
plate glass, scanners, 289
platforms, PaaS, 504
platters, 215, 905
plenum cables, 50, 527
plug-ins, browsers, 493-495
plugs, loopback, 537
PM (Particulate Matter) pollution, safety, 957
.PNG files, 631
PoE (Power over Ethernet), 533
polarity, voltage, 151-153
policies
AI, 961
AUP, 964
DLP policies, 899
enforcing, MDM, 385
group policies, 889-890
local security policies, 889
password policies, 963
regulatory/compliance policies, 964
security policies, 964
anti-malware, 862
AUP, 863
BYOD, 862
email, 863
emergency procedures, 863
password policies, 863
physical access, 862
regulatory compliance, 863
remote access, 863
user profiles, 863
pools, storage, 241
poor battery health, 423
poor VoIP quality, 485
POP3 (Post Office Protocol version 3), 379, 589
pop-ups/adware, 497, 880
portable vacuums, 148
port replicators, 389
ports
AGP, 84
audio ports, 43, 54, 277
audio subsystems, 450
charging USB ports, 34
common ports list, 53
Component/RGB video ports, 274
damaged ports, troubleshooting, 415
DB9, 44, 54
disabling, 871
DisplayPort, 389
DP, 40, 54
DVI ports, 39, 54
DVI-A ports, 54
DVI-D ports, 54
eSATA ports, 43, 54
eSATAp ports, 44, 54
Ethernet, 46-47
FireWire ports, troubleshooting, 798
flapping, 575
forwarding, 571, 916-917
HDMI ports, 41, 54
integrated motherboards, adapters, 53
keyboard, 30
Lightning ports, 37,54, 372
mapping, 571, 917
matching monitors to port type, 40
microUSB ports, 371-372
mini-DIN, 30
miniUSB ports, 371-372
modem ports, 480
mouse/mice, 30
multiple-device ports, IRQ, 114

multipurpose ports, comparing, 37-38
network, 46
PAT, 587, 917
projectors, 274
proprietary vendor specific ports, 371
PS/2 mouse, 54
RJ11 ports, 44, 54
RJ45 ports, 46, 50, 54
RS-232 ports, 44
SATA ports, enabling in BIOS/UEFI, 224
security, 871, 916
serial ports, 44
sleep-and-charge USB ports, 34
sound cards, connectivity, 279
S/PDIF ports, 43, 54
S-Video ports, 40
Thunderbolt ports, 36-37, 54
triggering, 916
troubleshooting
damaged ports, 415
FireWire ports, 798
unused ports, disabling, 871
USB 2.0 ports, 31
USB 3.0 ports, 31
USB 4.x ports, 31
USB-C ports, 37, 371-372
USB ports, 31, 54
connectors, 32
installing extra, 36
microUSB, 33
miniUSB, 33
PD, 32
power management, 119-120
summary, 35
troubleshooting shutdowns, 798
USB cables, 32
USB hubs, 33
USB-to-Ethernet converters, 35
USB-to-serial port converters, 46
VGA ports, 39, 54
video ports, 38, 42
positive attitude (soft skills), maintaining, 3, 200, 292-293 969
POSIX (Portable Operating System Interface), 819
POST (Power-On Self-Tests), 104
audio POST codes, 455
beeps, 90, 163, 195, 455
BIOS/UEFI POST error messages, 456-457
cards, 457
error messages, 191
memory, upgrading, 196
troubleshooting, 111, 163
PostScript, 330
pounds (lb), paper, 313
power supplies, 9-11
3.3V output voltage, 153
5V output voltage, 153
12V output voltage, 153
80 PLUS efficiency ratings, 162
110V vs. 220V input voltage, 153
AC circuit testers, 164
ACPI, 109, 159
adverse power conditions, 951
ATX, 153-156
batteries
backups, 954
charging, 424
CMOS batteries, 110-112
laptop batteries, 392-394
Li-ion batteries, 393, 947-948
poor battery health, 423
recycling, 111, 948
swollen batteries, 423
troubleshooting, 423-424
blackouts, 951
brownouts, 951
cabling, 140, 447-448
CFX12V, 154
choosing, 161-162
component requirements, 161
connectors, video cards, 267
damaging, 153
DC
jacks, replacing, 406
voltage, 157
disassembly, 164
dual-rail power supplies, 160
dual-voltage, 153
energy efficiency ratings, 162
EPS12V, 154
failures, troubleshooting, 954-956
FlexATX, 154
form factors, 153-154
frozen systems, troubleshooting, 424
hibernate mode, 159
improper charging, 392
inkjet printers, 306
input voltage selectors, 156
laptops, 391-394
laser printers, 311
LFX12V, 154
line conditioners, 953
micro-ATX, 154
modular power supplies, 162
motherboard connectivity, 153
MOV, 952
no power, troubleshooting, 424
overheating, troubleshooting, 424
overview, 153
overvoltage, 951
powering on, 153
purposes of, 156
ratings, speakers, 281
redundant power supplies, 161
replacing, 160
sags, 951
saver plans, Windows, 799
SFX12V, 154
signal checks, 165
speaker ratings, 281
spikes, 951
SPS, 956
standby mode, 159
surge protectors, 162
surge suppressors, 951, 952-953
surges, 951
system design, 447-448
testing, 164
TFX12V, 154
troubleshooting, 163-165, 954-956
types of, 153-154
undervoltage, 951
upgrading, 160
UPS, 162, 954-956

USDB power management, 119-120
video card connectors, 267
voltage, checking, 163
Wake on LAN, 159-160
Wake on Ring, 159
watts, 152-153, 160
WFX12V, 154
Windows power options, 799-800
wireless requirements, 491-492
PowerShell (.psl), 694
cmdlets, 712
.NET Core, 712
opening, 666
.PPT (.PPTX) files, 631
pre-downloading packages, 849
prefix notation, subnet masks, 986
preinstalling. *See* installing
preparing for
exams, online resources, 5
job requirements, 3
Presentation layer (OSI model), 540
presenters, wireless, 55
preventive maintenance. *See also* troubleshooting
aerosol cans, disposal laws, 149
air filtration masks, 149
antistatic brushes, 148
BD, 287
bootups, 148
CD, 287
compressed air, 148-150
denatured alcohol, 148
displays, cleaning, 148
dust, 147, 945, 957
DVD, 287
general-purpose cleansers, 148
general-purpose cloths, 148
gold contact cleaners, 148
kits, 148
lens cleaners, 148
lint-free cloths, 148
monitor wipes, 148
mouse/mice, 15
MSDS, 149
optical drives, 148, 287
OS, 803-804
portable vacuums, 148
printers, 324
impact printers, 318-319
inkjet printers, 319-321
laser printers, 321-323
thermal printers, 324
safety goggles, 149
scanners, 289
SDS, 149
toner vacuums, 148
urethane swabs, 148
vacuum bags, 148
vacuuming, 150
preventive measures, troubleshooting process, 463
primary partitions, 233, 727
principle of least privilege
logical security, 871
share permissions, 893
print drivers, 329-330
Print Management console, Windows, 771
print ribbons, 318
impact printers, 304
replacing, 319
print servers, 335-336, 582, 585
print spoolers, 331, 343
Print to File (virtual printing), 316
Print to image (virtual printing), 316
Print to PDF (virtual printing), 316
Print to XPS (virtual printing), 316
printers, 17. *See also* multifunction (all-in-one) devices
3-D printers, 303, 308
ADF, 302
all-in-one (multifunction) printers, 17
Bluetooth printers
access, 336
connectivity, 325
bubble jet printers. *See* inkjet printers
categories of, 302-303
CIS, 317
cloud printing, 337-338
collating pages, 330
connectivity, 332-333, 344-345
Bluetooth, 325
troubleshooting, 339
USB, 325-326, 342
Windows environments, 342-343
wired networks, 325
wireless networks, 325, 334-335
data privacy, 337
default printers, 328
dot matrix printers. *See* impact printers
duplexing assemblies, 313
duplexing (double-sided printing), 330
dye sublimation printers, 308
feeds, 313-315, 318
firmware, troubleshooting, 338
impact printers
maintenance, 318-319
multipart paper, 305
paper, 319
printheads, 303-304, 319
print ribbons, 304, 318-319
troubleshooting, 345
indicator lights, troubleshooting, 338
ink cartridges, 317
inkjet printers, 303
calibrating, 320
carriage belts, 306
carriages, 306
cleaning, 321
color, 307, 346
draft mode, 306
duplexing assemblies, 306
ink cartridges, 305-306, 320
large-format inkjet printers, 308
maintenance, 319-321
NLQ mode, 306
optimized DPI, 305-307
paper trays/feeders, 306
power supplies, 306
printheads, 305-306, 321
rollers, 306
stepper motors, 306
troubleshooting, 345-346
installing
connectivity, 325-326
setup locations, 324
languages, 330

laser printers, 303
calibrating, 323
cleaning, 311, 323
cooling, 323
density control blades, 311
duplexing assemblies, 311
e-clips, 322
fuser assemblies, 310-311
fusing rollers, 311, 323
imaging drums, 311
imaging process, 309-310
maintenance, 321-323
noises, 311
parts of, 311
power supplies, 311
safety, 309
toner, 311, 323
toner (EP) cartridges, 311, 322
toner safety/disposal, 948-949
transfer corona, 323
troubleshooting, 346-347
UPS, 955
maintenance, 324
memory, 341
networks, 332-333, 336, 344-345
Notepad, printing from, 342
orientation (page), 329-330, 344
overheating, 305
overview, 302
paper
feeds, 339
jams, 339
properties, 315
sources, 330
PCL, 330
PDL, 330
pending print jobs, 343
PostScript, 330
print drivers, 329-330
printheads, troubleshooting, 339
print preferences, 329-330, 344
print queues, 329
print spoolers, 331, 343
print trays, 330
quality, print, 330
resolution, 330
rollers, troubleshooting, 341
secure print, 338
security, 302
self-tests, 338
sensitive material, 302
sharing, 344-345, 582-583
print servers, 335-336
Windows environments, 332-333
wireless printers, 334-335
SMB protocol, 332
solid ink printers, 308
testing, 329
thermal printers, 303, 311
debris removal, 324
feed assemblies, 312, 324
heating elements, 312, 324
maintenance, 324
printheads, 312-313
thermal paper, 312, 324
thermal wax transfer printers, 308
toner
handling, 317
spills, 311
toner vacuums, 148
tractor feeds, 313
trays, 313-315, 318, 340
troubleshooting, 341, 583, 771-772
connectivity, 339
faded print, 340
firmware, 338
garbled print, 340
grinding noises, 339
incorrect paper size, 340
indicator lights, 338
light printing, 345
lines down printed pages, 339
paper feeds, 339
paper jams, 339
printheads, 339
slick rollers, 341
“tray not recognized” error messages, 340
USB-attached printers, 342
Windows environments, 342-343
two-sided printing, 313
unboxing, 325
upgrading, 318
user authentication, 337
virtual printing, 316
Windows environments, 327-328, 331
print drivers, 329-330
print queues, 329
sharing printers, 332-333
testing, 329
wireless printers, 334-336, 548
printheads
impact printers, 303-304, 319
inkjet printers, 305-306, 321
thermal printers, 312-313
troubleshooting, 339
privacy
AI, 961
browsing, 494
clouds, 506
confidential/private materials (soft skills), dealing with, 974
data, 337-338
GDPR, 878
HIPAA, 878
impersonation attacks, 880
IP addresses, 543
networks, 523, 732
PCI DSS, 877
PHI, 878
PII, 877
screens, physical security, 866
WEP, 923
Privacy tab (Internet Options Control Panel), 494
privileges
administrative privileges, 656
principle of least privilege
logical security, 871
share permissions, 893
standard (user) privileges, 656
Pro and Pro Education editions, Windows 10/11, 618
Pro for Workstations edition, Windows, 618-619
proactive technicians (soft skills), 598
probable cause (troubleshooting process), theories of
BIOS/UEFI POST error messages, 456-457
bootup process, 453-454
error messages, 455-457
hardware errors, 459
POST codes, 455

random device failures, 459-460
software errors, 460
testing, 461-462
UEFI diagnostics, 458
probes, toner, 537
problems, troubleshooting process
identifying, 452-453
isolating, 461-462
resolving, 463
procedures, operational
component handling/storage, 949
documentation, 942
power handling, 954-956
workplace safety, 943
processes (Linux), viewing, 847-848
processing phase, laser printer imaging process, 310
processing, programming, 699
processors
AMD, 66-67, 75-76, 268
APU, 72
ARM, 66
buses, 67-70
caches, 69-72
connectivity, 70
cooling, 77-78, 81
cores, 72-74
CPU
sockets, 76
speeds, 69
throttling, 69
fans, installing, 81-82
GPGPU, 72
GPU, 72
heat sinks, installing, 81
iGPU, 72
installing, 78-82
Intel, 66-67, 74-75
laptops, removing from, 396
multicore processors, 71
overclocking, 80
performance speeds, 67-68
power requirements, 161
Ryzen 3, 75
Ryzen 5, 75
Ryzen 7, 75
Ryzen 9, 75
Ryzen AI, 75
Ryzen Threadripper, 75
SoC, 66
sockets, 66
speeds, 67-68
system design, 447
thermal solutions, 81
threads, 71-72
throttle management, 80
troubleshooting, 83
upgrading, 80
virtualization, 73-74
x64, 66
x86, 66
Xeon, 74
ZIF sockets, 76
procurement life cycles, 963
productivity tools, cloud-based
collaboration tools, 806-807
email systems, 804-805
storage, 805-806
profile loads, troubleshooting, 795-796
profiles
configuration profiles, 922
Window profiles, 795-796
Program Compatibility Troubleshooter, 727
programming, 699
Programs tab (Internet Options Control Panel), 494
projecting confidence (soft skills), 200, 969
projectors, 275-276
promptness (soft skills), 971
prompts, mapping from, 597
proper language (soft skills), using, 968-969
property sheets, 691
proprietary crash screens, 457
proprietary OS (Operating Systems), 616
proprietary vendor specific ports, 371
protocols
network protocols, 540
TCP/IP model, 540-541
proxy servers, 495, 912
ps command, Linux, 845-848
PS/2 ports, 54
public AI (Artificial Intelligence), 961
public clouds, 506
Public folders, share permissions, 894
public IP addresses, 543
public networks, 523, 732-733
punchdown blocks, 50, 537-538
punchdown tools, 50, 537-538
punctuality (soft skills), 200, 971
PUP (Potentially Unwanted Programs), 880
purpose of change, change management, 965
PVC cables, 51, 527
pwd command, macOS, 835-836
PXE (Pre-Boot Execution Environment), 772
Python scripts (.py), 694

Q

QoS (Quality of Service), 485
Basic QoS, wireless networks, 571
NIC, 569
QR (Quick Response) codes, 371, 881
quad-channel memory, 188
quality, print, 330
question marks (?), troubleshooting mobile devices, 426
questions
open-ended, 2
performance-based, 5
technical, 2
queues (print), 329, 343
Quick Assist, 918
quick formatting, 235
quitting apps, Force Quit (macOS), 826
quotas, disk, 232
quotation marks (“ “), comments, 703

R

racks, network, 535
radiation patterns, antennas, 556
radio buttons, Windows, 630
radio, wireless connectivity, 55
RADIUS (Remote Authentication Dial-In User Service), 873

RAID (Redundant Array of Independent Disks)
"array missing" error messages, 251
BIOS/UEFI configuration settings, 240
configuring, 238
failures, 251
fault tolerance, 238-240
FCM, 239
hardware RAID, 240
hot swappable RAID drives, 240
levels of, 239, 240
RAID 0, 239
RAID 0+1, 239
RAID 1, 239
RAID 5, 239
RAID 6, 239
RAID 10, 239
"RAID not found" error messages, 251
software RAID, 239
troubleshooting, 251
RAID mode, SATA, 228
rainbow tables, 883
RAM (Random Access Memory), 12
4GB RAM and above, 185
disk caches, 243
DRAM, 178
ECC RAM, 181
laptops, 360, 400
limitations, 617
Non-ECC RAM, 181
power requirements, 161
SRAM, 178
virtual memory, 241
VRAM, 192-193, 268, 751
Windows requirements, 751
random device failures, troubleshooting, 459-460
random reboots, troubleshooting, 415
random shutdowns, troubleshooting, 90, 163
ranges
antennas, 557
wireless connectivity, licensed/unlicensed, 490-491
ransomware, 878
RAW volumes, 237
rd command, 663, 685
RDP (Remote Desktop Protocol), 589, 622, 918
Read & Execute permissions, 895
Read permissions, 893-895
read/write failures, troubleshooting, 249
read/write times, troubleshooting, 244
readers/writers, NFC, 377
reading devices. *See* e-readers
ReadyBoost, Windows, 790
rearranging displays, 746
reassembling computers, 147
reboots
continuous reboots, troubleshooting, 90
random reboots, troubleshooting, 415
troubleshooting, 163
Windows, 748, 797
rebuilding Windows profiles, 795
reconnaissance attacks, 883
recovery. *See also* troubleshooting
accounts, 763-764, 902
deleted files, macOS, 826
file recovery software, 245
in-place/overwrite, 902
partitions, Windows, 723
System Image Recovery, 791
Time Machine, macOS, 825-826
user accounts, 763-764
Windows, 645-646
WinRE, 249, 645, 662, 722, 773-776
Recovery Mode (Android OS), 416
Recycle Bin, Windows 11, 628
recycling
batteries, 111, 948
components, 446
e-waste, 946
electronics, 946-948
ink cartridges, 317
proof of, 869
redirecting
browsers, 496
folders, 888
reducing transmit power, wireless networks, 926
redundant power supplies, 161
refilling ink cartridges, 317
refresh option, web browsers, 493
refresh rates, displays, 265, 747
ReFS (Resilient File Systems), 230, 729, 768
regedit command, 685
regedit program (.reg), 741
regedt32.exe command prompt, 643
regedit.exe command prompt, 643
region codes, DVD/Blu-ray discs, 285
registered memory, 181
registries
troubleshooting, 793
Windows, 116
backups, 644, 740-741
editing, 643
regedit command, 685
regedit program (.reg), 741
regedit.exe command prompt, 643
regedt32.exe command prompt, 643
regsvr32 command, 685
subtrees, 643
user profiles, 643
regsvr32 command, 685
regsvr32.exe command, 754
regulated data, licensing, 877
regulations, wireless networks, 556
regulatory/compliance policies, 863, 964
reimaging computers, 733-734
reinitializing
anti-malware, 735
antivirus software, 735
re-inking print ribbons, 318
reinstalling
hardware/software, 461
motherboards, 147
Windows, 738
relational operators, 705
reliability, OS, 620
reloading Windows, 645, 737-738
remapping network drives, 695
remediating malware-infected systems, 907-908
reminders, passwords, 874
remote access, 863, 918

remote backups. *See* synchronizing
remote control, projectors, 275
remote desktops
RDP, 918
starting, 680
user accounts, 885
Windows
Remote Assistance, 801-803
Remote Desktop Connection, 801-803
remote networks
accessing, 689
installations, Windows, 723
ping command, 684, 685
remote wipes, mobile devices, 411
removable
drives, BitLocker To Go, 623
media files, deleting, 628
storage, 198-199
removing. *See also* deleting
adapters, 86, 143
apps, 371, 418-419
batteries, laptops, 392
browser plug-ins/extensions, 495
DIMM, 190
directories, 663, 685
external cables, 140
hard drives, 144, 402
icons from notification area, 749
internal cables, 141-142
keyboards, laptops, 397-398
malware, 907-908
memory, 190, 401
motherboards, 145
power cables, 140
processors, laptops, 396
snap-ins, 754
software, 750-751
storage devices, 144
subdirectories, 663
touchpads, 397
touch screens, 273
USB devices, 34
Windows credentials, 761
ren command, 686
renaming files/directories, 686
repairing. *See also* troubleshooting
apps, 753
keyboards, 397-398
laptops, 394-398
motherboards, 395-396
overview, 394
processors, 396
touchpads, 397
Windows installations, 723, 738
repeaters, wireless, 552
repetition, programming, 699
repetition structures. *See* loops
replacing
Bluetooth cards, 404
DC jacks, laptops, 406
digitizers, 273
displays, 408
hard drives, 402
ink cartridges, 320
inverters, 409
microphones, laptops, 409-410
motherboards, 89-90
paper
impact printers, 319
thermal printers, 324
power supplies, 160
printheads, impact printers, 319
print ribbons, impact printers, 319
screens, 408
slot covers, 139
toner (EP) cartridges, 322
touch screens, 273
webcams, 409-410
wireless cards, 404
replay attacks, 883
requirements
job requirements, preparing for, 3
power supplies, wireless networks, 491-492
system requirements, apps, 751
virtualization, 501
researching memory, 189
reservations, DHCP, 562
resetting
BIOS, 112
factory, 384
hard resets, 416-417
maintenance counters, 323
PC, 791, 795
soft resets, 416
Windows, 723
resin, 3-D printers, 303
resistance
meter readings, 152
multimeters, 537
voltage, 152-153
resizing partitions, 238
resolution
displays, 266, 275, 409, 747
printers, 330
resolving
names, DNS, 566
problems, troubleshooting process, 463
resources
conflicts, BIOS/UEFI, 114
dedicated resources, cloud computing, 508
shared resources, cloud computing, 507
unavailable resource, troubleshooting, 575-576
viewing with Device Manager, 114
virtualization, 501
responding to security incidents, 928-929
response times, mobile devices, 411
rest, data at, 903
restarting
computers, warm boots, 104
machines, 694
services, 794
shutdowns vs, 798
restore points, 646, 737-738, 741
restoring
OS security, 899-902
System Restore, 737
wbadmin command, 690
Windows, 723
restricting
login times, 890
user permissions, 890
retention levers, expansion slots, 86
retention plates, 78
retinal scanners, physical security, 868
reviews, peer, 964

RF signals, low, 559
RFI (Radio Frequency Interference), 138
RFID (Radio Frequency ID), physical security, 865
RG-6 coaxial cables, 49
RG-59 coaxial cables, 49
rights, user accounts, 762
risk analysis, change management, 965
risk management, levels of risk, 965
RJ11
  connectors, 527-530
  ports, 44, 54
RJ45
  connectors, 527-530
  ports, 46, 50, 54
  wall jacks, 532
rm command, macOS, 835-836
rmdir command, 685
RMM (Remote Monitoring and Management), 919
robocopy command, 664-665, 686
rogue antivirus apps, 906
rogue AP, 928
roles in IT, 2
roll back Windows updates, 739
rollback plans, 966
rollers, printer
  inkjet printers, 306
  troubleshooting, 341
rolling back device drivers, 748
ROM (Read-Only Memory), BIOS ROM checksum error messages, 456
root access, unauthorized, 414-415
root directories, 657
root user accounts, 836
rootkits, 496, 878
routers, wireless, 540-541, 548-549
  DHCP server configurations, 562
  DMZ, 571
  installing, 926-927
  IP filtering, 925
  passwords, changing, 570
  static IP addressing, 561
  usernames, changing, 570
RS-232 ports, 44
.RTF files, 631
run as administrator permissions, 897
Ryzen 3 processors, 75
Ryzen 5 processors, 75
Ryzen 7 processors, 75
Ryzen 9 processors, 75
Ryzen AI processors, 75
Ryzen Threadripper processors, 75

S

SaaS (Software as a Service), 504
SAE (Simultaneous Authentication of Equals), 923
Safe Boot, 778
Safe Mode
  bootups, 736
  macOS, 829
  Windows, 777, 795
safety
  aerosol cans, disposal laws, 149
  air filtration masks, 945
  antistatic bags, 949
  component handling/storage, 949-950
  compressed air, 945
  dust cleanup, 957
  dust masks, 945
  electronic safety, 949
  environmental impacts, 945-946
  equipment, 944
  ESD, 949
  fire extinguishers, 459, 943
  goggles, 149, 944
  laser printers, 309
  LCD, 265
  lifting, 20, 945
  maintenance, 20
  memory, installing, 190
  monitors, installing, 40
  MSDS, 149, 943
  OSHA, 943
  personal safety, 945
  power handling
    battery backups, 954
    line conditioners, 953
    MOV, 952
    SPS, 956
    surge suppressors, 951-953
    UPS, 954-956
  SDS, 149
  self-grounding, 949
  technical field kits, 944
  toner, 948-949
  trip hazards, 952
  troubleshooting, 20
  USB devices, removing, 34
  vacuums, 945
  ventilation, 959
  workplaces
    environmental impacts, 945-946
    equipment, 944
    fire extinguishers, 943
    government regulations, 942
    lifting techniques, 945
    MSDS, 943
    OSHA, 943
    personal safety, 945
sags, voltage, 951
SAML (Security Assertion Markup Language), 873
SAN (Storage Area Networks), 518, 524
sandboxes, 411
  testing, 966
  virtualization, 498
SAS (Serial-Attached SCSI), 219, 222
SATA (Serial ATA), 219
  15-pin SATA power ATX power supply connectors, 154
  AHCI mode, 228
  BIOS/UEFI settings, 228
  cabling, 223
  connectivity, 220-221
  connectors, 141
  eSATA, 221
    brackets, 120
    installing eSATA cards, 120-121
    mounting/unmounting drives, 225-226
    partitions, 233
    troubleshooting drives, 249
  hard drives, power requirements, 161
  installing devices, 223
  Legacy mode, 228
  mSATA drives, 402
  Molex-to-SATA converters, 156

mSATA, 220
BIOS/UEFI settings, 228
installing, 225
ports, enabling in BIOS/UEFI, 224
RAID BIOS/UEFI configuration settings, 240
RAID mode, 228
SATA Configuration setting (BIOS/UEFI), 108
satellite modems, 488-489
saving
files, Windows, 632
screenshots, 7
SC connectors, 51
SCADA (Supervisory Control and Data Acquisition) systems, 585
scalability, cloud storage, 805
scanners
ADF scanners, 17, 288
app scanners, 386
barcode scanners, 288
cloud scanning, 337-338
data privacy, 337
fingerprint scanners, physical security, 868
flatbed scanners, 17, 288-289
handheld scanners, 288
installing, 289
palm print scanners, physical security, 868
preventive maintenance, 289
retinal scanners, physical security, 868
sharing, 583
troubleshooting, 583
types of, 288
USB scanners, 289
user authentication, 337
vulnerability scanners, 883
scheduling tasks, 755
scope
of change, change management, 966
DHCP, 562
screened subnets, 571, 913, 924
screens
aspect ratios, 450
autorotating, 421
blank/black screens, troubleshooting, 90 163, 271, 792-793
BSOD, 272, 457, 793
captures, 7
conferencing features, 451
contrast ratios, 451
dark screens, troubleshooting, 792
digitizers, replacing, 273
displays
subsystem design, 450-451
video adapters, 451
enlarging, 365
flashing screens, troubleshooting, 271
home screens
Android, 364
iPhones, 365
inverters, 407-409
laptops, Wi-Fi antennas, 407
locks, mobile devices, 412
moving between screens, mobile devices, 366
number of, system design, 450
privacy screens, physical security, 866
proprietary screen crashes, 90, 457
replacing, 408
resolution, 266, 275, 409
savers, energy efficiency, 162
screenshots, 7
sharing, macOS, 823-824
splash screens, 964
subsystem design, 450-451
timeouts/screen locks, 890
touch screens, 266, 273
troubleshooting
autorotation failures, 421
backlight failures, 421
blank/black screens, 90 163, 271, 792-793
BSOD, 272
burn-in, 272
dark screens, 792
dead pixels, 271
digitizers, 273
dim displays, 271, 421
distorted images, 271
flashing screens, 271
flickering displays, 422
fuzzy images, 271
incorrect colors, 271
no display, 421
proprietary screen crashes, 90
sizing text, 271
touch screens, 273, 422
types of, 450
video adapters, 451
screwdrivers, 139
scribes, 394
scripting
advantages of, 693
alphanumeric characters, 701
AND operators, 708
apps, installing, 695
automating
backups, 695
processes, 693, 694
batch scripting
.bat files, 693
Notepad, 692
command prompt
accessing, 656
appearance of, 657
attrib command, 665, 669
backslashes (\) in file structures, 659
backups, automating, 695
bcdedit command, 669-670
bootrec command, 670
cd command, 659-660, 671
chkdsk command, 671-672
chkntfs command, 672
cipher command, 672-673
closing, 676
cls command, 673
command command, 673
[command name] /? command, 668
command switches, 661-662
copy command, 664-665, 673
defrag command, 673
del command, 663, 674
dir command, 660-662, 669, 674
directories, 657
disable command, 675
diskpart command, 675
dism command, 675
drive navigation inputs, 669

dxdiag command, 675-676
enable command, 676
exit command, 676
expand command, 676
explorer command, 677
format command, 677
formatting commands, 657
full paths in, 663
gpresult command, 677
gpupdate command, 678
help command, 668, 678
hostname command, 678
ipconfig command, 678-679
md command, 662-663, 679
mkdir command, 662-663, 679
mmc command, 679
more command, 680
msconfig command, 680
msinfo32 command, 680
mstsc command, 680
naming directories, 657
naming files, 657
navigating directories, 659-663
nbtstat command, 681
net command, 681
netdom command, 682
netstat command, 683
net use command, 681
net user command, 682
notepad command, 683
nslookup command, 683
organizing files, 657
overview, 656
pathping command, 684
ping command, 684-685
PowerShell, 666
rd command, 663, 685
regedit command, 685
regsvr32 command, 685
ren command, 686
rmdir command, 663, 685
robocopy command, 664-665, 686
services.msc command, 686
set command, 687, 698
sfc command, 687
shutdown command, 688
starting tools with commands, 666
subdirectories, 657
systeminfo command, 688
taskkill command, 689
tasklist command, 689
telnet command, 689
tracert command, 690
tree structure of files, 657-659
type command, 664, 690
wbadmin command, 690
whoami command, 690-691
winver command, 691
wscript command, 691
xcopy command, 664-665, 691-692
commands
administrative privileges, 656
attrib command, 665, 669
bcdedit command, 669-670
bootrec command, 670
cd command, 659-660, 671
chkdsk command, 671-672
chkntfs command, 672
cipher command, 672-673
cls command, 673
command command, 673
[command name] /? command, 668
common commands list, 667-668
copy command, 664-665, 673
defrag command, 673
del command, 663, 674
dir command, 660-662, 669, 674
disable command, 675
diskpart command, 675
dism command, 675
drive navigation inputs, 669
dxdiag command, 675-676
enable command, 676
exit command, 676
expand command, 676
explorer command, 677
format command, 677
formatting, 668
gpresult command, 677
gpupdate command, 678
help command, 668, 678
hostname command, 678
ipconfig command, 678-679
learning, 666
md command, 662-663, 679
mkdir command, 662-663, 679
mmc command, 679
more command, 680
msconfig command, 680
msinfo32 command, 680
mstsc command, 680
nbtstat command, 681
net command, 681
netdom command, 682
netstat command, 683
net use command, 681
net user command, 682
notepad command, 683
nslookup command, 683
output, multiple pages, 662
pathping command, 684
periods (.) in commands, 661
ping command, 684-685
rd command, 663, 685
regedit command, 685
regsvr32 command, 685
ren command, 686
rmdir command, 663, 685
robocopy command, 664-665, 686
services.msc command, 686
set command, 687, 698
sfc command, 687
shutdown command, 688
standard (user) privileges, 656
starting tools with commands, 666
systeminfo command, 688
taskkill command, 689
tasklist command, 689
telnet command, 689
tracert command, 690
two periods (..) in commands, 661
type command, 664, 690
usage considerations, 665
wbadmin command, 690
whoami command, 690-691
wildcards, 664
WinRE limited commands, 662
winver command, 691
writing, 666
wscript command, 691
xcopy command, 664-665, 691-692

comments
- colons (:), 704
- hash characters (#), 703-704
- quotation marks (" "), 703
- slashes (//), 703
- within scripts, 703

common scripting languages, 693
comparison (equality) operators, 705
compiled programs, 692
conditions
- compound conditions, 708
- testing with logical operators, 708

consequences of scripting, mitigating, 695
constructs, 704
decision (selection) structures, 704
- dual-alternative structures, 706
- examples of, 707-708
- multiple alternative structures, 706-707
- relational operators, 705
- single-alternative structures, 705

defined, 656, 692
environment variables
- accessing, 696
- editing, 697
- system environment variables, 696
- user environment variables, 696
- viewing, 698

floating point numbers, 701
gathering information/data, 695
information/data gathering, 695
initiating updates, 695
installing apps, 695
integers, 701
interpreted programs, 692
JavaScript (.js), 694
logical operators, 708
login scripts, 888
loops, 704, 711
mitigating consequences of scripting, 695
NOT operators, 708
OR operators, 708
overview, 656
PATH variables, 696
peer reviews, 695
PowerShell (.psl), 666, 694, 712
programming, 699
property sheets, 691
Python scripts (.py), 694
remapping network drives, 695
restarting machines, 694
shell scripts (.sh), 693
strings, 701
syntax, 698
system environment variables, 696
team programming, 695
testing scripts, 696
text files, 692-694
updates, 695
use cases, 694-695
user environment variables, 696
variables, 699
- data types, 701
- declaring, 701
- environment variables, 696-698
- initializing, 701
- keywords, 700
- naming, 700-701
- PATH variables, 696
- use cases, 702-703

VBScript (.vbs), 694, 712
wildcards, 664
XSS attacks, 883
scroll lock key, 16
scrolling actions (mobile devices), 366
SCSI (Small Computer System Interface), SAS
- cabling, 222
- drives, 219

SD (Secure Device) cards, 360-361
SDK (Software Development Kits), 371
SDN (Software-Defined Networking), 586
SDRAM (Synchronous DRAM), 180
SDS (Safety Data Sheets), 149
searches
- File Explorer (Windows), 635
- integrated searches, 493
- Internet, 6-7
- search engines, examples of, 6
- Spotlight, macOS, 821
- Windows 11, 626

security
- access management, 571
- account recovery, 902
- administrators/supervisors, 873
- ads
  - blockers, 497
  - high number of ads, 414
- AES, 568, 903
- allow lists, 913
- Android, 413
- anti-malware, 862, 870
- antivirus software, 732, 870
- AP, 570, 926-927
- attacks
  - access attacks, 882
  - adware/pop-ups, 880
  - backdoor attacks, 882
  - BEC attacks, 882
  - boot sector viruses, 878
  - botnets, 879, 882
  - brute force attacks, 882
  - cryptojacking/cryptomining, 879
  - DDOS attacks, 882
  - dictionary attacks, 874, 882
  - DoS attacks, 882
  - dumpster diving, 869, 881
  - evil twin attacks, 882
  - fileless malware, 879
  - impersonation attacks, 880
  - insider attacks, 882
  - keyloggers, 879
  - malware, 878-880
  - MITM attacks, 883
  - password spraying attacks, 883
  - phishing, 881-882
  - piggybacking, 881
  - PUP, 880
  - QR code phishing, 881
  - ransomware, 878
  - reconnaissance attacks, 883
  - replay attacks, 883
  - rootkits, 878

shoulder surfing, 866-867, 881
smishing, 881
Smurf attacks, 883
social engineering attacks, 875, 880
spear phishing, 881
spoofing attacks, 883
spyware, 878
SQL injection attacks, 883
stalkerware, 879
supply chain/pipeline attacks, 883
tailgating, 866, 881
TCP/IP hijacking attacks, 883
Trojan malware, 878-879
viruses, 878-880
vishing, 881
vulnerability scanners, 883
whaling, 881
zero-day attacks, 883
zombie attacks, 883
audit logs, data privacy, 337
AUP, 863
authentication, 864, 884
authenticator apps, 872
DMARC, 912
failures, 873
identity synchronization, 872
JIT access, 873
Kerberos, 873
multifactor authentication, 872
OTP, 872
PAM, 873
RADIUS, 873
SAE, 923
SAML, 873
soft tokens, 872
SSO, 872
TACACS+, 873
TOTP, 872
authenticator apps, 412
authorization, 884
AutoPlay, disabling, 904
AutoRun disabling, 904
backups, 899-902
badging, data privacy, 337
best practices, 930
biometric security, 867
activating, 869
fingerprint scanners, 868
FRT, 868-869
mobile devices, 378, 412
palm print scanners, 868
retinal scanners, 868
voice recognition, 868
BIOS, 873-874
BitLocker, 622, 903
BitLocker Drive Encryption, 623, 903
BitLocker Recovery Password Viewer, 623
BitLocker To Go, 623
boot sector viruses, 878
boots, 873
bootups, 873
botnets, 879
browsers, 494-496
BYOD, 862
cable locks, laptops, 410
certificates of destruction, 869
child exploitation, 929
content filtering, 920
data at rest, 903
data security
account recovery, 902
AES, 903
backups, 899-902
BitLocker, 903
BitLocker To Go, 903
data at rest, 903
device encryption, 903
disabling AutoPlay, 904
disabling AutoRun, 904
EFS, 904
hard drive storage, 904
patch management, 898
restores, 899-902
unknown notifications, 898
unprotected systems, 898
update management, 898
data privacy
audit logs, 337
badging, 337
secure print, 338
deny lists, 913
DEP, 617
desktop alerts, 880
device encryption, 903
digital security certificates, 906
directory services, 870
DMZ, 913, 924
DNS, 495, 909-910
documentation, 869
DRM, 876
EDR, 884
EFS, 623, 639, 904
email, 910-911
encryption, 865
AES, 903
BitLocker, 903
BitLocker To Go, 903
data at rest, 903
device encryption, 414, 903
disabling AutoPlay, 904
disabling AutoRun, 904
Drive Encryption setting (BIOS/UEFI), 109
EFS, 904
full device encryption, 903
other people's files, 904
SAE, 923
end-user education, 875-876
EOL, 898
event logs, 890
facial recognition, 412, 874
FACTA, 869
fake security warnings, mobile devices, 411
FERPA, 869
fingerprints, 412, 874
firewalls, 870, 913
AP configurations, 570
port forwarding, 916
Windows Defender Firewall, 914-917
wireless networks, 922
folder options, 897
fTPM setting (BIOS/UEFI), 109
GDPR, 878
groups, 886
guards, 865
hard drives, 904-905
HIPAA, 878
HSM, 88
HTTPS, 492

identification
access management, 870
passwordless security, 874
PIN, 874
Windows Hello, 874
IDS, 920
incident response, 928-929
Internet appliances, 920
Internet security
allow lists, 913
deny lists, 913
digital security certificates, 906
DMZ, 913, 924
DNS, 909-910
email, 910-911
firewalls, 913
malware removal, 907-908
Microsoft Defender Antivirus, 906
proxy servers, 912
rogue antivirus apps, 906
screened subnets, 571, 913, 924
UPnP, 914
VPN, 919-920
Windows Defender Firewall, 914-917
Intrusion Detection/Notification setting (BIOS/UEFI), 109
iOS passcode settings, 413
IoT, 573, 928
IPS, 921
Keychain Access, macOS, 832-833
laptops
cable locks, 410
data-usage limit notifications, 414
failed login attempts, 413
jailbreaking, 414-415
leaked personal files/data, 414
system lockouts, 413
unauthorized account access, 413
unauthorized location tracking, 414
unauthorized root access, 414-415
licensing, 876-877
load balancers, 920
local access
AD functions, 885-886
group policies, 889
local security policies, 889
user management, 884
locks, 885, 890
logging off when not in use, 875
logical security
ACL, 871
anti-malware, 870
antivirus software, 870
authentication, 872-873
BIOS/UEFI, 873-874
directory services, 870
disabling unused ports, 871
firewalls, 870
identity access management, 870
login OS security, 874-875
ports, 871
principle of least privilege, 871
trusted/untrusted sources, 871
VPN, 871
Zero Trust models, 870
logins, 874-875
logs, 757-758
LoJacks, 109, 873
malware
anti-malware, 870
fileless malware, 879
removing, 907-908
Trojan malware, 878-879
MDM, 922
MDR, 884
MNDA, 875
mobile devices, 927-928
authenticator apps, 412
biometric security, 412
data-usage limit notifications, 414
DMZ, 924
facial recognition locks, 412
failed login attempts, 413
fake security warnings, 411
fingerprint locks, 412
IP address filtering, 925
jailbreaking, 414-415
leaked personal files/data, 414
MAC address filtering, 924
malicious apps, 411
patterns, 412
PIN codes, 412
screen locks, 412
spoofing apps, 411
swipe locks, 412
system lockouts, 413
TKIP, 923
unauthorized account access, 413
unauthorized apps, 411
unauthorized location tracking, 414
unauthorized root access, 414-415
USS, 410
WEP, 923
Windows Hello, 412
WPA, 923
WPA2, 923
WPA3, 923
WPS, 925
motherboards, 87
multifunction (all-in-one) devices, 302
NAT, 917
NDA, 875
networks
access, 884-886, 889
attacks, 882, 883
remote access, 918-919
NIC, 567-568
non-compliant systems, 862
order of volatility, 929
overview, 862
parental controls, 929
passwordless security, 874
password manager, 492
passwords, 412
AP, 570, 926
BIOS/UEFI settings, 108
BitLocker Recovery Password Viewer, 623
boot passwords, 873
changing default administrator password, 885
complexity, 874
expiration dates, 890
expired passwords, 875
failed logins, 875
formatting, 874

Keychain Access, macOS, 832-833
logging off when not in use, 875
managing, 875
mobile device synchronization, 381
number of characters, 874
OTP, 872
passwd command, Linux, 846
policies, 863, 963
power-on passwords, 873
rainbow tables, 883
reminders, 874
routers, 570
requiring, 890
social engineering attacks, 875, 880
special characters, 874
spraying attacks, 883
TOTP, 872
uniqueness, 874
usernames, 874
Passwords app, macOS, 832
PAT, 917
patch management, 898
patterns, mobile devices, 412
PCI DSS, 877
permissions
changing, 891
NTFS permissions, 891, 894-896
running as administrators, 897
share permissions, 891-894
UAC, 897
PHI, 878
phishing, incident response, 929
physical security
access control vestibules (mantraps), 866-867
alarm systems, 866
bade readers, 865
biometrics, 867-869
bollards, 863
cable locks, 865
documentation, 869
door locks, 863
equipment locks, 865
guards, 865
hardware tokens, 865-866
HSM, 865
key cards, 864
key fobs, 865
keys, 863
lighting, 865
magnetometers, 866
mobile digital keys, 865
motion sensors, 866
privacy screens, 866
RFID, 865
smart cards, 865-866
tokens, 865
TPM, 865
USB locks, 865
video surveillance, 866
picture passwords, 412
PII, 877
PIN, 874
piracy, 876-877
policies, 964
anti-malware, 862
AUP, 863
BYOD, 862
email, 863
emergency procedures, 863
password policies, 863
physical access, 862
regulatory compliance, 863
remote access, 863
user profiles, 863
ports, 871, 916
print, data privacy, 338
printers/multifunction (all-in-one) devices, 302
private browsing, 494
proof of incineration, 869
proof of recycling, 869
ransomware, 878
regulated data, 877
remote access, 918-919
restores, 899-902
routers, 570, 925
scans, Windows installations, 731
screened subnets, 571, 913, 924
Secure Boot setting (BIOS/UEFI), 109
secure management access, 571
secure print, data privacy, 338
security certificates, verifying in browsers, 495
shredding documents, 869
smartphones, 413-415
spyware, incident response, 929
SSH, 918
SSID, 926
student records, 869
supervisors/administrators, 873
Telnet, 918
third-party vendors, 869
threats/vulnerabilities, 620
access attacks, 882
adware/pop-ups, 880
backdoor attacks, 882
BEC attacks, 882
boot sector viruses, 878
botnets, 879, 882
brute force attacks, 882
cryptojacking/cryptomining, 879
DDOS attacks, 882
dictionary attacks, 874, 882
DoS attacks, 882
dumpster diving, 869, 881
evil twin attacks, 882
fileless malware, 879
impersonation attacks, 880
insider attacks, 882
keyloggers, 879
malware, 878-880
MITM attacks, 883
password spraying attacks, 883
phishing, 881-882
piggybacking, 881
PUP, 880
QR code phishing, 881
ransomware, 878
reconnaissance attacks, 883
replay attacks, 883
rootkits, 878
shoulder surfing, 866-867, 881
smishing, 881
Smurf attacks, 883
social engineering attacks, 875, 880
spear phishing, 881
spoofing attacks, 883
spyware, 878
SQL injection attacks, 883
stalkerware, 879
supply chain/pipeline attacks, 883

tailgating, 866, 881
TCP/IP hijacking attacks, 883
Trojan malware, 878-879
viruses, 878-880
vishing, 881
vulnerability scanners, 883
whaling, 881
XSS attacks, 883
zero-day attacks, 883
zombie attacks, 883
TKIP, 567
TLS, 587
tokens, 865
TPM, 87, 109-110, 873
trusted/untrusted sources, 871
UEFI, 873-874
unknown notifications, 898
unprotected systems, 898
update management, 898
UPnP, 914
users
BIOS/UEFI, 873
managing, 884
usernames and passwords, 874
USS, 410
UTM systems, 920
virtualization, 502
viruses, 878-880
antivirus software, 870
BIOS/UEFI, 112
incident response, 929
Virus Protection setting (BIOS/UEFI), 108
VM, 502
VPN, 871, 919-920
WEP, 567, 923
Windows
files/folders, 639
installations, scans, 731
Windows Defender Firewall, 914-915
Windows Firewall, 916-917
Windows Hello, 412, 874
wireless networks, 923, 927-928
DMZ, 924
IP address filtering, 925
MAC address filtering, 924
WPS, 925
wireless routers, 925-927
wireless security, 923-925, 927-928
WPA, 568, 923
WPA2, 568
WPA2 with AES, 568
WPA3, 568
XDR, 884
Zero Trust models, 870
Security option, AP configurations, 570
Security tab (Internet Options Control Panel), 494
SEG (Security Email Gateways), 911
selection (decision) structures, 704-708
selection, programming, 699
self-grounding, 138, 949
self-tests, printers, 338
sensitive material, printers/multi-function (all-in-one) devices, 302
sequences, programming, 699
serial cables, 44
serial ports, 44
serial transmissions, 480-481
servers
AAA servers, 584
authentication servers, 584
autodiscovery, 380
client-side DNS, 566
database servers, 584
DHCP servers, 562, 584
DNS servers, 565-566, 584, 840
endpoint management servers, 584
file servers, 584
fileshare servers, 584
home servers, system design, 445-446
isolation, 498
Kerberos authentication servers, 873
logging servers, 585
mail servers, 585
network servers, 584-585
NTP servers, 585
print servers, 335-336, 582, 585
proxy servers, 495, 912
SAN connectivity, 524
syslog servers, 585
virtualization, 498
web servers, 585
service packs, 460, 646, 736
service releases, software, 460
services, 769
cloud file storage services, 505
cloud services, 337
Component Services, 755
DaaS, 499, 504
deploying, 506-507
directory services, 870
disabling, 794
DNS, 565-566, 584
IaaS, 504
KMS, 734
learning about, 794
logs, 757
metered utilization services, 508
PaaS, 504
rates, 508
restarting, 794
SaaS, 504
Services and Applications, Windows, 769
services.msc, 794
SLP, 590
startup failures, 793
troubleshooting startup failures, 793
WDS, 734
Services and Applications, Windows, 769
services.msc command, 686, 794
Services tab, Task Manager, 784
Services window, MMC, 686
Session layer (OSI model), 540
set command, 687, 698
setting/meeting expectations (soft skills), 974
Settings app, Windows 10/11, 640-641
Setup (UEFI), 105-106
Setup programs, 104-105
setups
errors/freezes, OS update limitations, 620
locations, printer installations, 324

logs, 736-737, 757
POST errors, troubleshooting, 111
sfc (System File Checker), 687, 738
SFTP (Secure File Transfer Protocol), 589
SFX12V power supplies, 154
Shadow Copy technology, 737
share permissions, 891-894
Shared Folders tool, 759
shares, 594-595, 759
shareware, 876
sharing
files, 898
folders, 759, 896
multifunction devices, 582-583
printers, 344-345, 582-583
print servers, 335-336
Windows environments, 332-333
wireless printers, 334-335
resources, cloud computing, 507
scanners, 583
screens, macOS, 823-824
subfolders, 896
system memory, 268
shell scripts (.sh), 693
shells, 819
shielding, speakers, 282
shortcuts, Windows 11, 627
shoulder surfing, 866-867, 881
Show Desktop area, Windows 11, 627
shredding documents, 869
shrinking partitions, 767
shutdown command, 688, 845-846
shutdowns
projectors, 276
random shutdowns, 163, 195
restarting vs, 798
troubleshooting, 90, 163, 195, 798
Windows 11 options, 625
side-by-side apps, Windows, 722
side-loading apps, 371
signal strength
antennas, 558
wireless networks, 426
signatures, digital, 745-746
signed drivers, 745-746
SIM (Subscriber Identification Module) cards, 368, 947
SIM (System Image Manager), 734
simple volumes, 237
sine waves, 954
single-alternative structures, 705
single-mode fiber cables, 52
single rank memory, 182
site surveys, 557
sizing
icons, Windows desktops, 634
text, troubleshooting, 271
skills
creating text files, 7
of technicians, 3
screen captures, 7
search skills, 6, 7
written communication skills, 166
SLA (Service-Level Agreements), 960
slashes (//), comments, 703
sleep-and-charge USB ports, 34
sleep mode
hard drives, 236
mobile devices, 366
slick printer rollers, troubleshooting, 341
slots
covers, replacing, 139
expansion slots, 13-14
laptops, 390
motherboards, 83
PCI, 83
retention levers, 86
M.2, 218-219
motherboards, 83, 187-188
SD card, 361
slow performance, troubleshooting, 423
boots, 795
browsers, 497-498
network speeds, 559
profile loads, 795-796
storage devices, 243-244
systems, 784
Windows, 784
SLP (Service Location Protocol), 590
sluggish performance, troubleshooting
hard drives, 249
memory, 195
response times, mobile devices, 411
S.M.A.R.T. (Self-Monitoring, Analysis and Reporting Technology), troubleshooting, 248-249
smart cameras, 359
smart card readers, 361
smart cards, physical security, 865-866
smart devices
IoT, 572
security, 573
smartphones, 358
cellular networks, 366-367
disposal/recycling, 946
eSIM cards, 368
IMEI, 367
IMSI, 368
security, 413-415
SIM cards, 368
troubleshooting
app failures, 418-419
autorotating screens, 421
backlight failures, 421
batteries, 423-424
Bluetooth connectivity, 426-427
damaged ports, 415
dim displays, 421
flickering displays, 422
frozen systems, 424
GPS, 426
hard resets, 416-417
liquid damage, 415
network issues, 425-426
NFC, 427
no display, 421
no power, 424
OS update failures, 417
overheating, 424
performance, 423
random reboots, 415
screens, 421-422
soft resets, 416
touch screens, 422

unexpected app behavior, 418
Wi-Fi connectivity, 425-426
SMB (Server Message Blocks), 332, 583, 589
S/MIMEW (Secure MIME), 379
smishing, 881
smoke, troubleshooting, 163, 273, 459
SMS (Short Message Service) text messages, 872, 881
SMTP (Simple Mail Transfer Protocol), 379, 590
Smurf attacks, 883
snap-ins
adding/removing, 754
Component Services, 755
Computer Management console, Windows, 754
MMC, 754
snapshots/checkpoints, VM, 501
SNMP (Simple Network Management Protocol), 590
snug connectors, 142
social engineering attacks, 875, 880
SoC (System on a Chip), 66
SODIMM (Small-Outline DIMM), 178-179, 400
soft resets, 416
soft skills
active listening, 2, 92-93, 970
addressing non-IT personnel, 56
appearance, 428-429
avoiding distractions, 971-972
be humble, 855
being on time, 200, 971
being proactive, 598
changing one thing at a time, 123
confidence, projecting, 200, 969
confidential/private materials, dealing with, 974
cultural sensitivity, 970
customers
building trust, 931
customer service, 967
difficult customers, dealing with, 467-468, 972-973
documenting changes, 123
expectations, setting/meeting, 974
grooming, 968
maintaining a positive attitude, 200
making/keeping commitments, 972
mentoring, 509
organization, 968
phone communication skills, 252-253
positive attitude, maintaining, 3, 200, 292-293 969
proper language, 968-969
punctuality, 200, 971
staying current, 647
teamwork, 200
time management, 971
troubleshooting, changing perspectives when, 713-714
trust, building, 931
work ethics, 348
written communication skills, 166
soft token authentication, 872
software, 8
anti-malware, mobile devices, 386
antivirus software, 870
Microsoft Defender Antivirus, 906
mobile devices, 386
reinitializing, 735
rogue antivirus apps, 906
Windows installations, 732
botnets, 882
commercial licenses, 876
compatibility, 621
DaaS, 504
DRM, 876
extensible software, 621
file recovery software, 245
firewalls, 870, 913-917
firmware, AP, 926
IaaS, 504
installing, 461, 750-752
interfering software, disabling from OS installations, 732
legacy software, 498
Linux CLI, obtaining software with, 848, 849
malware, 878-880, 907-908
open source software, 818, 876
OS incompatibility, 620
PaaS, 504
packages, pre-downloading, 849
patches, 460
perpetual licenses, 876
personal licenses, 876
piracy, 876-877, 929
pre-downloading, 849
RAID, 239
reinstalling, 461
removing, 750-751
SaaS, 504
SDK, 371
SDN, 586
service packs, 460
service releases, 460
shareware, 876
spyware, 878, 929
stalkerware, 879
troubleshooting, 460
updating with Software Updater (Linux), 843
valid licenses, 876
viruses, 878-880
vulnerability scanners, 883
Windows compatibility, 725
Software Updater, Linux, 843
solid ink printers, 308
SOP (Standard Operating Procedures), 959
sound
2.0 audio subsystems, 450
2.1 audio subsystems, 450
cards, 277
defined, 43
installing, 278-279
muting, 280
port connectivity, 279
system design, 450
theory of operation, 278
Windows operations, 279
microphones, system design, 450
ports, colors, 278
POST codes, 455
Sound utility, Windows, 746
speakers, system design, 449

subsystems
logistics, 450
port connectivity, 450
voice recognition, physical security, 868
SOW (Statements of Work), 966
space requirements, OS, 751
spam, 911
spanned volumes, 237
sparks, troubleshooting, 273
S/PDIF (Sony/Phillips Digital Interface) ports, 43, 54
SPD (Serial Presence Detect), memory, 182
speakers
amplification, 281
choosing, 282
frequency response ranges, 282
mobile devices, 362
motherboards, 276
power ratings, 281
shielding, 282
system design, 449
troubleshooting, 282-283
USB speakers, 282
volume control, 282-283
spear phishing, 881
special characters
file/folder names, Windows, 631
passwords, 874
special function keys, 399
special thermal paper, 312, 324
speckling (pages), troubleshooting, 345-346
speeds
buses, 68-70
clamping speed, 952
clock speeds, 69
CPU, 69
data transfer speeds, wireless networks, 559
DSL, 484
memory, 189
motherboards, 68-69
NIC, 569
overclocking, 80
processors, 67, 68
serial transmissions, modems, 481
slow network speeds, 559
throttle managing, 80
Windows boot process, speeding up, 789-790
SPF (Sender Policy Frameworks), 911
SPICE (Simple Protocol for Independent Computer Environments), 918
spikes, 951
spills, keyboards, 16
spinning pinwheels, troubleshooting, 195, 250, 457, 830
splash screens, 964
splitting partitions, 767
spoofing attacks, 411, 883
spoolers, print, 331, 343
Spotlight, macOS, 821
spraying attacks, password, 883
spreading/pinching open actions (mobile devices), 366
SPS (Standby Power Supplies), 956
spyware, 878, 929
SQL (Structured Query Language), injection attacks, 883
square waves, 954
SRAM (static RAM), 178
SRU (System Restore utility), 738
SSD (Solid-State Drives), 391, 402-404, 769
archival storage, 217
B+M keys, 218
defragmenting, 245
ESD, 144
installing, 226, 227
M.2 slots, 218, 219
M.2 SSD, BIOS/UEFI settings, 228
NVMe, 218, 228
overview, 217
SSHD, 217-218
static electricity, 227
troubleshooting, 251
upgrading, 228
SSH (Secure Shell), 589, 918
SSHD (Solid-State Hybrid Drives), 217-218, 402
SSID (Service Set Identifiers), 551, 926
SSID not found messages, 567
wireless networks, 571
SSL (Secure Sockets Layer), 587-589
SSL/TLS (Secure Sockets Layer/Transport Layer Security), email, 379
SSO (Single Sign-Ons), 872
stalkerware, 879
standard accounts, 884
standard changes, change management, 965
standard formatting, hard drives, 904
standard (full) formatting, 235
standard user accounts, 763
standard (user) privileges, commands, 656
standby mode, power supplies, 159
standoffs, 145
staple jams, troubleshooting, 341
star topologies, 520
Start button, Windows 11, 624
Start screen, Windows, 627-630
start/stop bits, 481
starting
apps during Windows startup, 784
macOS in Safe mode, 829
remote desktops, 680
tools with commands, 666
Startup apps tab, Task Manager, 783
startup failures, services, 793
startup programs, disabling in Windows, 791
Startup Settings menu, Windows, 776-777
static electricity
antistatic tools, 78, 136-138, 148
EMI, 138
ESD, 136-138, 144
RFI, 138
SSD, 227
static IP address configurations, 560-561
status, hard drives, 766
status indicators, LED, 246
status messages, hard drives, 250
staying current (soft skills), 647
ST connectors, 51

stepper motors, inkjet printers, 306
sticky hard drives, troubleshooting, 248
stop (kill tasks), 782
storage
  archival, SSD, 217
  basic disks, 236
  basic storage, 236
  BIOS/UEFI configuration, 228
  boot volumes, 237
  byte binary prefixes, 20
  cloud storage, 214, 722, 805-806, 900. *See also* synchronizing
  component storage, safety, 949-950
  credentials, 760
  device
    configuration, overview, 222
    removing, 144
  disk caches, 241-243
  Disk Management tool, 765-767
  Disk Management, Windows, 236-237
  dynamic disks, 237
  dynamic storage, 236
  EB, 20
  EiB, 20
  external hard drives, 402
  fault tolerance, 238-240
  files, cloud file storage services, 505
  flash memory, 360
  GB, 20
  GiB, 20
  hard drives
    2.5-inch, 215
    3.5-inch, 215
    basic disks, 236
    boot volumes, 237
    defragmenting, 244
    disk caches, 241-243
    disk mirroring (RAID 1), 239
    disk striping (RAID 0), 239
    drive activity LED, 246
    drive letters, 657
    dynamic disks, 237
    fault tolerance, 238-240
    form factors, 215
    HDI, 216
    head crashes, 216
    hibernation/sleep mode, 236
    lost clusters, 243
    magnetic hard drives, 215
    mounts, 225
    MTBF, 216
    overview, 215
    platters, 215
    RAID, 238-240, 251
    RAW volumes, 237
    resizing partitions, 238
    SCSI, 219
    security, 904
    simple volumes, 237
    spanned volumes, 237
    status messages, 250
    striped volumes, 237
    swap files, 242
    system volumes, 237
    troubleshooting, 243-249
    types of, 215
    volumes, 237
  hibernation/sleep mode and hard drives, 236
  hybrid drives, 402
  iCloud, macOS, 822
  installing devices, troubleshooting, 246-249
  internal laptop drives, 402
  JSOD. *See* spanned volumes
  kB, 19-20
  KiB, 20
  laptops, 360, 401-402
  logical drives, 233
  MB, 19-20
  mechanical hard drives, 402-404
  MiB, 20
  mobile devices, 360-361
  mSATA drives, 402
  NAS devices, 219, 443
  off-site storage, 214, 900
  OneDrive, 722
  on-site storage, 900
  optical drives, 772
    connectivity, 285
    DirectX, 287
    DVD/Blu-ray region codes, 285
    features of, 284-285
    installing, 286
    interfaces, 285
    ISO files/images, 285
    overview, 283-284
    preventive maintenance, 287
    reading Blu-ray discs, 284
    symbols, 285
    testing, 286
    troubleshooting, 286-287
    writable media, 284
  overview, 214
  partitions, resizing, 238
  PB, 20
  performance, 243-244, 249
  PiB, 20
  pools, 241, 768
  RAID
    "array missing" error messages, 251
    BIOS/UEFI settings, 240
    configuring, 238
    failures, 251
    fault tolerance, 238-240
    FCM, 239
    hardware RAID, 240
    hot swappable RAID drives, 240
    levels of, 239-240
    RAID 0, 239
    RAID 0+1, 239
    RAID 1, 239
    RAID 5, 239
    RAID 6, 239
    RAID 10, 239
    "RAID not found" error messages, 251
    software RAID, 239
    troubleshooting, 251
  RAM, laptops, 360
  RAW volumes, 237
  removable storage, 198-199, 623
  SAN, 518, 524
  SAS drives, 219
  SATA
    cabling, 223
    installing devices, 223
    ports, enabling in BIOS/UEFI, 224
  SD cards, 360-361
  simple volumes, 237
  spanned volumes, 237

INDEX

SSD, 391, 402-404
archival storage, 217
installing, 226-227
overview, 217
SSHD, 217
static electricity, 227
troubleshooting, 251
upgrading, 228
SSHD, 402
Storage option, AP configurations, 571
storage pools, 768
Storage Spaces Control Panel, 768
striped volumes, 237
subsystem design, 449
swap files, 242
system volumes, 237
TB, 19-20
TiB, 20
troubleshooting
new device installations, 246-247
performance, 243-244, 249
previous installed devices, 247-249
virtual memory, 241
volumes, 237-238
Windows Storage Spaces, 240-241
YB, 20
YiB, 20
ZB, 20
ZiB, 20
STP (Shielded Twisted Pair) cables, 50, 526-527
straight through (patch) cables, 528
streaks (printing), troubleshooting, 346
streaming, virtual apps, 505
strings, 701
striped volumes, 237
striping (RAID 0), disk, 239
student records, security, 869
styluses (touch pens), 362, 422
su command
Linux, 845
macOS, 835
subdirectories, 631, 657, 663
subfolders, 631, 896
subnets
masks, 545-546, 985-987
screened subnets, 571, 913-924
subscribers (Internet), data caps, 379
subsystem design
audio, 449-450
displays, 450-451
storage, 449
subtrees, Windows registry, 643
sudo command
Linux, 846
macOS, 835-836
supervisors/administrators, BIOS/UEFI security, 873
supply chain/pipeline attacks, 883
support, virtualization, 74
surge suppressors, 162, 951-953
surveillance (video), physical security, 866
surveys, site, 557
S-Video ports, 40
swabs, urethane, 148
swap files, 242
swap partitions, 728
swelling capacitors, troubleshooting, 90
swipe/flick actions (mobile devices), 366
swipe locks, mobile devices, 412
switches, 519, 541
command switches, 661-662
managed/unmanaged switches, 520
motherboard switches, 458
PoE switches, 533
SDN, 586
swollen batteries, 423
symbols
Ethernet ports, 47
Event Viewer, 757
Sync Center Control Panel utility, Windows, 752
synchronizing
browsers, 495
files, 505
identity synchronization, 872
mobile devices, 381-384
Windows, 752
syntax, scripting, 698
synthetic backups, 900
syslog servers, 585
Sysprep, 734
system boards (mobile motherboards), 395
System Configuration utility, Windows, 680, 777-780
systemd, Linux, 840
System File Checker, 246, 249, 687
System Image Recovery, 791
System Information
BIOS/UEFI, 107
macOS, 831
opening, 680
System menu, Linux, 841
System Restore, 737, 741, 793
System Tools section, Computer Management console, 755
Event Viewer, 756-758
Shared Folders tool, 759
Task Scheduler, 755
systeminfo command, 688
systems
app requirements, 751
audio
subsystems, 449-450
workstations, 442
bootups, troubleshooting, 109
cases, 447-448
chipsets, 447
configuring, Windows, 680, 777-780
cooling systems, 447
CPU, 447
dates/times, troubleshooting, 111
display subsystems, 450-451
environment variables, 696
environmental concerns, 446
files, 772-773
System File Checker, 246, 249, 687
viewing, 898
folders, macOS, 823
gaming PC, 441
graphic/CAD/CAM workstations, 441
home servers, 445-446
images, 644-645, 791
instability, troubleshooting, 797

lockouts, 413
logs, 757-758
macOS
settings, 827-829
updates, 824
memory, 447
motherboards, 447
NAS devices, 443
partitions, 234
power supplies, 447-448
processors, 447
recycling components, 446
resources, 113-114
restoring, 737, 741, 793
storage subsystems, 449
thick client workstations, 445
thin client workstations, 444
tools, Computer Management console, 755
Event Viewer, 756-758
Shared Folders tool, 759
Task Scheduler, 755
updates, macOS, 824
video workstations, 442
virtualization workstations, 443
volumes, 237, 772

T

T568A wiring standard, 51, 528
T568B wiring standard, 528
tables, rainbow, 883
tablets, 358
disposal/recycling, 946
SD card slots, 361
tabs, browsers, 493, 629
TACACS+ (Terminal Access Controller Access-Control System+), 873
tailgating, 866, 881
tangs, cabling, 50, 527
tap/touch actions (mobile devices, 365
taskbars
multi-monitor taskbars, 722
Windows 11, 624-625
taskkill command, 689
tasklist command, 689
Task Manager, Windows, 782
App history tab, 783
CPU tab, 786
Details tab, 784
Memory tab, 786
Performance tab, 193-194, 782, 785-787
Services tab, 784
Startup apps tab, 783
Users tab, 784, 787
Task Scheduler, 755
Task View, Windows 11, 626
TB (Terabytes), 19-20
TCP (Transmission Control Protocol), 588
TCP/IP (Transmission Control Protocol/Internet Protocol), 540
Application layer, 541, 590
CIFS, 589
connection-oriented protocols, 590
devices, 541
DHCP, 589
DNS, 589
example of, 588-590
FTP, 589
hijacking attacks, 883
HTTP, 589
HTTPS, 589
IMAP, 589
Internet layer, 541, 590
LDAP, 589
NBT, 589
Network Access layer, 541, 590
NTP, 589
POP3, 589
protocol stacks, checking on NIC, 576
RDP, 589
SFTP, 589
SLP, 590
SMB, 589
SMTP, 590
SNMP, 590
SSH, 589
telnet, 590
Transport layer, 541, 590
team programming, 695
teamwork (soft skills), 200
technical field kits, 944
technical questions, 2
technicians
gun slinger technicians, 123
qualities, 2
skills, 3
soft skills
active listening, 970
appearance, 428-429
attitude, 292-293
avoiding distractions, 971-972
be humble, 855
being on time, 200
being proactive, 598
building customer trust, 931
changing one thing at a time, 123
changing troubleshooting perspectives, 713-714
confidential/private materials, 974
cultural sensitivity, 970
customer services, 967
dealing with difficult customers, 467-468
difficult customers, 972-973
documenting changes, 123
grooming, 968
maintaining a positive attitude, 200, 969
making/keeping commitments, 972
mentoring, 509
organization, 968
phone communication skills, 252-253
projecting confidence, 200, 969
proper language, 968-969
punctuality, 200, 971
setting/meeting expectations, 974
staying current, 647
teamwork, 200
time management, 971
work ethics, 348
written communication skills, 166
tools, 139
telnet, 590, 689, 918
temperature/humidity control, safety, 958

Temperature Monitoring setting (BIOS/UEFI), 108
Terminal, macOS, 834
terminating twisted pair cables, 527-530
testing
backups, 899
cables, 530, 537
conditions with logical operators, 708
optical drives, 286
POST, 104
power supplies, 164
printers, 329, 338
sandbox testing, 966
scripts, 696
test development, virtualization, 498
theories of probable cause, troubleshooting process, 461-462
tethering, 377, 489
text files, 692-694
creating, 7
more command, 680
type command, 690
text messages, SMS, 872, 881
text, sizing, 271
textboxes, Windows, 629
TFX12V power supplies, 154
theories of probable cause, troubleshooting process
BIOS/UEFI POST error messages, 456-457
bootup process, 453-454
error messages, 455-457
hardware errors, 459
POST codes, 455
random device failures, 459-460
software errors, 460
testing, 461-462
UEFI diagnostics, 458
thermal pads, 77
thermal paper, 312, 324
thermal paste, 77-78
thermal printers, 303, 311
debris removal, 324
feed assemblies, 312, 324
heating elements, 312, 324
maintenance, 324
printheads, 312-313
thermal paper, 312, 324
thermal solutions, 81
thermal wax transfer printers, 308
thick client workstations, 445
thin client workstations, 444
third-party vendors, security, 869
This PC tile, Windows Start screen, 628
threads, 71-72, 786
threats/vulnerabilities, security, 620
access attacks, 882
adware/pop-ups, 880
backdoor attacks, 882
BEC attacks, 882
boot sector viruses, 878
botnets, 879, 882
brute force attacks, 882
cryptojacking/cryptomining, 879
DDOS attacks, 882
dictionary attacks, 874, 882
DoS attacks, 882
dumpster diving, 869, 881
evil twin attacks, 882
fileless malware, 879
impersonation attacks, 880
insider attacks, 882
keyloggers, 879
malware, 878-880
MITM attacks, 883
password spraying attacks, 883
phishing, 881-882
piggybacking, 881
PUP, 880
QR code phishing, 881
ransomware, 878
reconnaissance attacks, 883
replay attacks, 883
rootkits, 878
shoulder surfing, 866-867, 881
smishing, 881
Smurf attacks, 883
social engineering attacks, 875, 880
spear phishing, 881
spoofing attacks, 883
spyware, 878
SQL injection attacks, 883
stalkerware, 879
supply chain/pipeline attacks, 883
tailgating, 866, 881
TCP/IP hijacking attacks, 883
Trojan malware, 878-879
viruses, 878-880
vishing, 881
vulnerability scanners, 883
whaling, 881
XSS attacks, 883
zero-day attacks, 883
zombie attacks, 883
throttle management, 69, 80
throughput. *See* bandwidth
Thunderbolt cables/ports, 36-37, 54
TiB (Tebibytes), 20
ticket systems, help desks, 962
.TIF (.TIFF) files, 632
Tiles view, Windows File Explorer, 634
tiles, Windows Start screen, 627-628
time
activation clocks, 734
managing (soft skills), 971
inaccurate system dates/times, troubleshooting, 111
NTP, 585, 589
punctuality (soft skills), 200, 971
Time Machine, macOS, 825-826
timeouts/screen locks, 890
tips, exams, 5
TKIP (Temporal Key Integrity Protocol), 567, 923
TLS (Transport Layer Security), 587-589
TN LED (Twisted Nematic LED), 265
tokens, physical security, 865
tone generators, 537
toner
handling, 317
laser printers, 311, 322-323
safety/disposal, 948-949
spills, 311
unfused toner, troubleshooting, 347
toner probes, 537
toner vacuums, 148

tools
AC circuit testers, 164
air filtration masks, 945
antistatic bags, 949
antistatic wristbands/gloves, 78
browser troubleshooting tools, 497
cable testers, 530, 537
cable (wire) strippers, 529, 537
change boards, 964
compressed air, 945
crimpers, 529-530, 537
deployment tools, 734
diagonal cutters, 139
digital meters, resistance readings, 152
disassembly tools, 139
dust masks, 945
ESD, 949
fire extinguishers, 943
laptop repairs, 394
laser printer maintenance kits, 322
line conditioners, 953
loopback plugs, 537
maintenance kits, 148
multimeters, 151, 537
needle-nose pliers, 139
network (breakout) taps, 537
power supply testers, 164
punchdown blocks, 537-538
punchdown tools, 50, 537-538
safety goggles, 944
screwdrivers, 139
scribes, 394
starting with commands, 666
surge suppressors, 951-953
System Tools section, Computer Management console, 755-759
technical field kits, 944
tone generators, 537
toner probes, 537
vacuums, 945
Wi-Fi analyzers, 558
Windows Memory Diagnostic tool, 196
Tools tab, System Configuration utility, 780
top command, Linux, 845
topology diagrams, networks, 960
Torvalds, Linus, 617, 839
TOTP (Time-based One-Time Passwords/Passcodes), 872
touch and hold/long touch actions (mobile devices), 365
touch calibration, trackpads, 421
touch command, macOS, 835-836
touch pens (styluses), 362
touch screen displays, 266, 407
removing, 273
replacing, 273
troubleshooting, 422
touch/tap actions (mobile devices), 365
touchpads
removing, 397
repairing, 397
tower cases, 10, 11
TPM (Trusted Platform Modules), 87
BIOS/UEFI, 109, 873
clearing, 110
security, 110, 865
versions of, 110
tracert command, 577, 690
track (drawing) pads, 363-364
track points, 363
tracking, location
GPS, 411
unauthorized tracking, 414
trackpads, 421
tractor feeds, 313
traffic (networks), troubleshooting, 425
transfer corona, laser printers, 323
transferring phase, laser printer imaging process, 310
transfer speeds, 20
transmit power (wireless networks), reducing, 926
Transport layer
OSI model, 540
TCP/IP, 541, 590
“tray not recognized” error messages, 340
trays, printer, 313-315, 318, 330, 340
tree structures, files, 657-659
triggering, port, 916
trip hazards, 952
triple-channel memory, 188
Trojan malware, 878-879
troubleshooting. *See also* preventive maintenance; recovery; repairing
alarms, 247
application logs, 758
apps
closure failures, 418
crashes, 757
hanging apps, 757
installation failures, 419
load failures, 419
unexpected app behavior, 418
update failures, 419
audio, 282-283
displays, 272
projectors, 276
backlight bulbs, 421
backups, 451-453
batteries, 423-424
BIOS issues, 113
blank/black screens, 163, 792-793
Bloom’s Taxonomy, 452
Bluetooth connectivity, 426-427
bootups, 453-454, 790-791
blank screen on bootup, 90
“Bootable device not found.” error messages, 113
failures, 247, 790-791
finding missing bootloaders, 854
graphical interfaces, 791
resetting PC, 791
slow boot, 795
system boots from the wrong device, 109
browsers
basic issues, 496-497
degraded (slow) performance, 497-498
extensions, 495
plug-ins, 495
slow performance, 497-498
tools, 497
BSOD, 247, 457, 758, 793
burning smells, 90, 163
cable modems, 581-582
cabling, video connectivity, 271
capacitors, 90

changing perspectives (soft skills), 713-714
clicking sounds, 247, 286
clock drift, 750
configurations, 122
connectivity, 574-576
continuous reboots, 90
CPU, 79, 83
cursor drift, 421
dark displays, 792
data loss/corruption, 245
degraded performance, 423
with Device Manager, 122
dimness
  images, 271
  screens, 421
displays
  audio, 272
  autorotation failures, 421
  backlight failures, 421
  digitizers, 273
  dim displays, 421
  flickering display, 422
  no display, 421
  touch screens, 273
DLL, 754
DNS, 909, 910
Dock (macOS), missing, 820
documenting outcomes, 463
DSL modems, 581-582
email, 910-911
error messages, 455-457
eSATA drives, 249
extended read/write times, 244
failures to boot, 790-791
File Explorer, 422
FireWire ports, 798
flash drives, 198
flowcharts, 464-466
frozen systems, 424
full system functionality, verifying, 463
GPS, 426
graphical interfaces, 791
grinding noises, 247, 286
hard drives
  bootup failures, 247
  data loss/corruption, 245
  extended read/write times, 244
  fragmented drives, 244
  noises, 247
  performance, 243-244, 249
  read/write failures, 249
hardware, 459
identifying problems, 452-453
inaccurate system dates/times, 111
information gathering, 451
inkjet printers, 345-346
intermittent wireless connectivity, 425-426
Internet connectivity, 425, 574-576
isolating problems, 461-462
kernel panic, 831
keyboards, 16
laptops
  app failures, 418-419
  autorotating screens, 421
  backlight failures, 421
  battery failures, 423-424
  Bluetooth connectivity, 426-427
  damaged ports, 415
  dim displays, 421
  flickering displays, 422
  frozen systems, 424
  GPS, 426
  hard resets, 416-417
  keyboards, 420
  liquid damage, 415
  network issues, 425-426
  NFC, 427
  no display, 421
  no power, 424
  OS update failures, 417
  overheating, 424
  performance, 423
  random reboots, 415
  soft resets, 416
  touch screens, 422
  trackpads, 421
  unexpected app behavior, 418
  Wi-Fi connectivity, 425-426
laser printers, 346-347
liquid damage, 415
locked/frozen systems, 784
macOS
  kernel panic, 831
  Safe mode, 829
memory, 191, 195-196, 785
misfeeds, 339
missing
  bootloaders, 854
  Dock (macOS), 820
  drives in the OS, 246
  Task Manager tabs, 782
mobile devices
  app failures, 418-419
  autorotating screens, 421
  backlight failures, 421
  battery failures, 423-424
  Bluetooth connectivity, 426-427
  damaged ports, 415
  dim displays, 421
  flickering displays, 422
  frozen systems, 424
  GPS, 426
  hard resets, 416-417
  keyboards, 420
  liquid damage, 415
  network issues, 425-426
  NFC, 427
  no display, 421
  no power, 424
  OS update failures, 417
  overheating, 424
  performance, 423
  question marks (?), 426
  random reboots, 415
  soft resets, 416
  touch screens, 422
  trackpads, 421
  unexpected app behavior, 418
  Wi-Fi connectivity, 425-426
motherboards, 90-91
mouse/mice, 16
multifunction devices, 583
multipage misfeeds, 339
networks
  authentication issues, 585
  Bluetooth connectivity, 426-427
  GPS, 426
  high traffic, 425
  ifconfig command, 576
  ipconfig command, 576
  net command, 578
  netdom command, 579
  NFC, 427

nslookup command, 578
pathping command, 577
ping command, 574-576
status, 573-574
tracert command, 577
unavailable resources, 575-576
Wi-Fi connectivity, 425-426
Windows, 796-797
NFC, 427
NIC, 579-581
no connectivity, 574-576
noises, 163
nonfunctioning/undetected devices with Device Manager, 747-748
no power, 163, 424
optical drives, 286-287
OS
no OS found error messages, 737
update failures, 417
overheating, 90, 163, 424
overview, 451-452
page orientation, 344
performance
memory, 785
mobile devices, 423
storage devices, 243-244, 249
pinwheels, spinning, 457
plans of action, 463
port flapping, 575
POST
beeps, 90, 163
codes, 455
errors, 111
memory, 191
power failures, 954-956
power supplies, 163-165
preventive measures, 463
printers, 583, 771-772
connectivity, 339
double images, 347
faded print, 340
firmware, 338
garbled print, 340
grinding noises, 339
impact printers, 345
incorrect paper size, 340
indicator lights, 338
light printing, 345
lines down printed pages, 339
paper feeds, 339
paper jams, 339
slick rollers, 341
streaks, 346
toner, 347
USB-attached printers, 342
Windows environments, 342-343
printheads, 339
print queues, 343
processors, unusual noises, 83
profile loads, 795-796
projectors, 275-276
proprietary crash screens, 457
RAID, 251
random device failures, 459-460
random shutdowns, 90, 163
read/write failures, 249
reboots, 90, 163, 415
reimaging computers, 733-734
resolving problems, 463
resource conflicts, 114
safety, 20
scanners, 583
screens
blank screens, 90
digitizers, 273
proprietary screen crashes, 90
touch screens, 273
services, 793
Setup programs, 105
setups, POST errors, 111
shutdowns, 90, 163, 798
slow performance, 423, 784
slow profile loads, 795-796
sluggish performance, 249
S.M.A.R.T. errors, 248-249
smartphones
app failures, 418-419
autorotating screens, 421
backlight failures, 421
battery failures, 423-424
Bluetooth connectivity, 426-427
damaged ports, 415
dim displays, 421
flickering displays, 422
frozen systems, 424
GPS, 426
hard resets, 416-417
liquid damage, 415
network issues, 425-426
NFC, 427
no display, 421
no power, 424
OS update failures, 417
overheating, 424
performance, 423
random reboots, 415
soft resets, 416
touch screens, 422
unexpected app behavior, 418
Wi-Fi connectivity, 425-426
smoke, 163, 459
software, 460
speakers, 282-283
speckled pages, printers, 345-346
spinning pinwheels, 195, 250
SSD, 251
staple jams, 341
storage
new device installations, 246-247
performance, 243-244, 249
previously installed devices, 247-249
styluses, 422
swelling capacitors, 90
systems
boots from the wrong device, 109
dates/times (inaccurate), 111
instability, Windows, 797
logs, 758
slow performance, 784
Task Manager, missing tabs, 782
text, sizing issues, 271
theories of probable cause
BIOS/UEFI POST error messages, 456-457
bootup process, 453-454
error messages, 455-457
hardware errors, 459
POST codes, 455
random device failures, 459-460
software errors, 460
testing, 461-462
UEFI diagnostics, 458
thermal paste, 78

trackpads, 421
UEFI, 113, 458
unavailable resources, 575-576
undetected/nonfunctioning devices with Device Manager, 747-748
unintentional network connections, 426
unplugging computers, 150
unusual noises, 83
USB
devices, 119-120
ports, 798
verifying full system functionality, 463
video, 270-273, 792-793
video adapters, 459
Wi-Fi connectivity, 425-426
Windows
boot process, 791
installations, 735-736
network settings, 796-797
profiles, 795-796
shutdowns, 798
slow performance, 784
summary of steps, 799
system instability, 797
Windows Defender Firewall, 916, 917
Windows Troubleshooting Wizard, 750
wireless networks, 928
trust (soft skills), building, 931
trusted sources, web browsers, 492
trusted/untrusted sources, security, 871
tunnel vision, avoiding, 3
TVS (Transient Voltage Suppressing) ratings, surge suppressors, 953
twisted pair cables
corporate networks, 531-532
RJ11 connectors, 527-530
RJ45 connectors, 527-530
STP cables, 526-527
terminating, 527-530
UTP cables, 526-530
two periods (..) in commands, 661
two-sided printing, 313
.txt files, 632, 664
TXT records, DNS, 565
Type 1 (native) hypervisors, 501
Type 2 (hosted) hypervisors, 501
Type A-B-C fire extinguishers, 943
Type C fire extinguishers, 943
type command, 664, 690

U

UAC (User Account Control), 722, 764, 897
Ubuntu, 840-844
UDP (User Datagram Protocol), 588-590
UEFI (Unified Extensible Firmware Interface)
advanced menu, 107
audio beeps, 456
boot manager, 454
boot process, 454
configuration settings, 107-109
diagnostics, 458
flashing, 112-113
M.2 SSD settings, 228
main menu, 106
mSATA settings, 228
NVMe SSD settings, 228
on-board NIC, 569
POST error messages, troubleshooting, 456-457
RAID configuration settings, 240
resource conflicts, 114
SATA
ports, 224
settings, 228
security, 873-874
Setup, 105-106
storage devices, configuring, 228
system boots from the wrong device, troubleshooting, 109
TPM considerations, 110
viruses, 112
UL ratings, surge suppressors, 953
Unallocated status messages, 250
unattended installations, Windows, 723
unauthorized
account access, 413
apps, 411
location tracking, 414
root access/jailbreaking, 414-415
unavailable resources, troubleshooting, 575-576
unboxing printers, 325
unbuffered memory, 181
uncompressing files, 676
undervoltage, 951
undetected/nonfunctioning devices, troubleshooting with Device Manager, 747-748
unexpected app behavior, troubleshooting, 418
unfreezes, change, 964
uninstalling apps, 418-419, 824
unintentional network connections, troubleshooting, 426
uniqueness, passwords, 874
universal access, cloud storage, 805
Unknown status messages, 250
unlicensed ranges, wireless connectivity, 491
unlocking
BitLocker encrypted hard drives, 903
mobile devices, 366
unmanaged/managed switches, 520
unplugging computers, 150
unprotected systems, OS security, 898
Unreadable status messages, 250
untrusted sources
browsers, 492
security, 871
unusable partitions in Disks, 852
unused ports, disabling, 871
unusual noises, troubleshooting, 83, 163
unwanted notifications, OS security, 898
updatedb command, Linux, 845, 853
updating
apps
failures, troubleshooting, 419
MDM and, 385
Automatic Updates, 739
boot orders, 735
browsers, 496
drivers, 116
firmware, 112-113
initiating updates, 695
managing updates, 898

mobile OS, 411
OS, 735
limitations, 620
troubleshooting failures, 417
Software Updater, Linux, 843
system updates, macOS, 824
Windows
changing settings, 740
network settings, 796-797
roll back Windows updates, 739
Windows Update Assistant, 725
upgrading
BIOS, 105
CPU, 80-81
memory, 183, 196, 400
motherboards, 89-90
power supplies, 160
printers, 318
processors, 80
SSD, 228
Windows, 723-724, 731
UPnP (Universal Plug and Play), 571, 914
upstream/downstream data, fiber networks, 487
UPS (Uninterruptible Power Supplies), 162, 954-956
upward (forward) compatibility, 621
urethane swabs, 148
USB Permissions setting (BIOS/UEFI), 108
USB (Universal Serial Bus)
cables, 32
connectors, 32
converters, 35, 46
devices, removing, 34
endpoints, 749-750
Ethernet, USB-to-Ethernet converters, 35
expansion cards, 117-118
flash drives, 197-199
headers, 117
USB hubs, 33
installing devices, 117
locks, physical security, 865
"Not enough USB controller resources" error messages, 749-750
Permissions setting (BIOS/UEFI), 108
ports, 35, 54
charging, 34
connectors, 32
microUSB ports, 33, 371-372
miniUSB ports, 33, 371-372
PD, 32
power management, 119-120
sleep-and-charge, 34
USB 2.0 ports, 31
USB 3.0 ports, 31
USB 4.x ports, 31
USB-C ports, 37, 371-372
printers, connectivity, 325-326, 342
removing devices, 34
scanners, 289
speakers, 282
troubleshooting
devices, 119-120
flowcharts, 465
wireless NIC, 376, 549
USB-PD, 32
USB Permissions setting (BIOS/UEFI), 108
user interfaces
command-line interface, 615
GUI, 615
macOS, 819-821
shells, 819
Ubuntu, 841
usernames, passwords, 874
users
accounts
administrator accounts, 763, 884
managing, 759-764
recovery options, 763-764
root users, 836
standard user accounts, 763
UAC, 722, 764, 897
authentication, printers/scanners, 337
BIOS/UEFI security, 873
child accounts, 884
concurrent users (share permissions), maximum number of, 892
educating, security, 875-876
end-user acceptance, change management, 966
environment variables, 696
EULA, 876
forums, Linux, 854
group accounts, 885
groups accounts, 885
guest accounts, 884
impersonation attacks, 880
managing, 884
MNDA, 875
NDA, 875
new user/exiting user checklists, 960
permissions, restricting, 890
PHI, 878
PII, 877
privileges, 656
profiles, Windows, 643, 863
standard accounts, 884
Users tab, Task Manager, 784, 787
USMT (User State Migration Tool), 726
USS (Universal Security Slots), 410
utilities, macOS
Activity Monitor, 830
Boot Camp, 834
Console, 831
Disk Utility, 833-834
Keychain Access, 832-833
System Information, 831
Terminal, 834
UTM (Unified Threat Management) systems, 920
UTP (Unshielded Twisted Pair) cables, 49-50, 526-530

V

VA LED (Vertical Alignment LED), 265
vacuum bags, 148, 323
vacuums, 945
portable vacuums, 148
preventive maintenance, 150
toner vacuums, 148
valid licenses, 876
vapor cooling, 77

variables, 699
data types, 701
declaring, 701
displaying, 687, 698
environment variables, 696-698
initializing, 701
keywords, 700
naming, 700-701
PATH variables, 696
set command, 687, 698
use cases, 702-703
VBScript (.vbs), 694, 712
vCards (VCF), contact synchronization, 382
VDI (Virtual Desktop Infrastructures), 499
vendor-specific logs, 757
vendors (third-party), security, 869
ventilation, 157, 959
verifying
Bluetooth devices on networks, 594
full system functionality, 463
hardware with Device Manager, 122
OS installations, 735
security certificates in browsers, 495
versions of Windows, determining, 642
VGA (Video Graphics Array)
cables, 39
ports, 39, 54
vi command, macOS, 835
video
adapters, 451
installing, 269-270
troubleshooting, 459
AGP, 84
displays
color gamut, 266
LCD, 264-265
LED, 264
mini-LED, 264
OLED, 264
pixel density, 265
pixel pitch, 265
refresh rates, 265
screen resolution, 266
touch screen, 266
editing workstations, system design, 442
GPU, 72
iGPU, 72
integrated graphics cards, 266
memory, 268-269
memory, space allocation, 178
overview, 264
PCIe video cards
adapters, 86
expansion slots, 84-85
lanes, 85
power requirements, 161
ports
analog signals, 38
digital signals, 38
DP, 40, 54
DVI-A ports, 54
DVI-D ports, 54
DVI ports, 39, 54
HDMI ports, 41, 54
summary, 42
S-Video ports, 40
VGA ports, 39, 54
projectors, 275-276
subsystems, 264
surveillance, physical security, 866
systems, 270
troubleshooting, 270-271, 792-793
video cards
AMD processors, 268
capture cards, 268
dGPU, 267
iGPU, 266
installing, 269, 270
power connectors, 267
Video options setting (BIOS/UEFI), 108
View tab options, File Explorer (Windows), 897-898
viewing
amount of installed memory, 184
environment variables, 698
events
logs, 756-757
symbols, 757
file extensions, 898
hidden files, 898
Linux processes, 847-848
mapped drive paths in File Explorer, 597
resources with Device Manager, 114
subnet masks, 985
system files, 898
virtualization
apps, streaming, 505
assistants, 370
cross platform virtualization, 498
defined, 73
desktops, 499, 504
emulators, 501
host machines, 501
hyperthreading, 502
Hyper-V, 73, 502, 727
hypervisors, 501
legacy software, 498
memory, 241, 786
networks, VNC, 918
NIC, 504, 569-570
OS licenses, 501
PC, 498
printing, 316
requirements, 501
resources, 501
sandboxes, 498
security, 502
servers, 498
snapshots/checkpoints, VM, 501
support, 74
test development, 498
Virtualization Support setting (BIOS/UEFI), 109
VM, 73, 443, 501-502
VNC, 918
Windows XP Mode, 502
workstations, system design, 443
viruses, 878-880
antivirus software, 870
Microsoft Defender Antivirus, 906
mobile devices, 386
reinitializing, 735
rogue antivirus apps, 906
Windows installations, 732
BIOS/UEFI, 112
boot sector viruses, 878
incident response, 929

mobile devices, 386
Virus Protection setting (BIOS/UEFI), 108
VM, 502
vishing, 881
VLAN (Virtual Local Area Networks), 545
VM (Virtual Machines), 443, 501
containers, 503
defined, 73
external networks, 502
Hyper-V, 722
internal networks, 502
security, 502
viruses, 502
VNC (Virtual Network Computing), 918
voice recognition, physical security, 868
VoIP (Voice over IP), 484-486
volatility, order of, 929
voltage, 150
3.3V output voltage, 153
5V output voltage, 153
12V output voltage, 153
110V vs. 220V input voltage, 153
brownouts, 951
clamping voltage, 952
current, 152-153
DC power supplies, 157
dual voltage memory, 182
dual-voltage power supplies, 153
input voltage selectors, 156
multimeters, 151, 537
ohms, 152-153
overvoltage, 951
polarity, 151-153
power supplies, checking, 163
resistance, 152-153
sags, 951
spikes, 951
surges, 951
undervoltage, 951
unplugging computers, 150
volume control, speakers, 282-283
volumes (drive partitions), 729
adding to hard drives, 767
boot volumes, 237, 772
NTFS, 235
RAW volumes, 237
resizing partitions, 238
simple volumes, 237
spanned volumes, 237
storage volumes, 237
striped volumes, 237
system volumes, 237, 772
VPN (Virtual Private Networks), 871, 919-920
VRAM (video RAM), 192-193, 751
vulnerabilities/threats, security
access attacks, 882
adware/pop-ups, 880
backdoor attacks, 882
BEC attacks, 882
boot sector viruses, 878
botnets, 879, 882
brute force attacks, 882
cryptojacking/cryptomining, 879
DDOS attacks, 882
dictionary attacks, 874, 882
DoS attacks, 882
dumpster diving, 869, 881
evil twin attacks, 882
fileless malware, 879
impersonation attacks, 880
insider attacks, 882
keyloggers, 879
malware, 878-880
MITM attacks, 883
password spraying attacks, 883
phishing, 881-882
piggybacking, 881
PUP, 880
QR code phishing, 881
ransomware, 878
reconnaissance attacks, 883
replay attacks, 883
rootkits, 878
shoulder surfing, 866-867, 881
smishing, 881
Smurf attacks, 883
social engineering attacks, 875, 880
spear phishing, 881
spoofing attacks, 883
spyware, 878
SQL injection attacks, 883
stalkerware, 879
supply chain/pipeline attacks, 883
tailgating, 866, 881
TCP/IP hijacking attacks, 883
Trojan malware, 878-879
viruses, 878-880
vishing, 881
vulnerability scanners, 883
whaling, 881
XSS attacks, 883
zero-day attacks, 883
zombie attacks, 883
vulnerability scanners, 883
.VXD files, 632

W

Wake on LAN, 159-160, 569
Wake on Ring, 159
wall jacks, RJ45, 532
wallets, mobile, 371
WAN (Wide Area Networks), 518
wireless broadband connectivity, 490
WWAN, configuring, 572
WAP (Wireless Access Points), 541
warm bootups, 104, 460
warranties, asset management, 963
wattage ratings, power supplies, 160
watts, 152-153
wbadmin command, 690
WDS (Windows Deployment Services), 734
WEA (Wireless Emergency Alerts), 370
web browsers
ad blockers, 497
address bars, 6, 493
bookmarks, 493
clearing data, 494
configuration settings, 494-495
default browsers, 494
Edge tile, Windows Start screen, 628
extensions, 493-495
Firefox, 496-497
Google Chrome, 496-497
hashes, 492
history, 493

integrated searches, 493
Microsoft Edge, 496-497
Internet Options Control Panel settings, 494
settings, 493-494
password manager, 492
patching, 495
performance, 497-498
plug-ins, 493-495
pop-ups, 497
private browsing, 494
as proxy servers, 495
redirection, 496
refresh option, 493
rootkits, 496
Secure DNS, 495
security, 492-497
synchronizing, 495
tabs, 493
troubleshooting
basic issues, 496-497
degraded (slow) performance, 497-498
extensions, 495
plug-ins, 495
slow performance, 497-498
tools, 497
trusted sources, 492
untrusted sources, 492
updating, 496
verifying security certificates, 495
web credentials, 759
web servers, 585
webcams/cameras, 17, 290-291, 362, 407-410, 868-866
websites, bookmarks, 493
WEP (Wired Equivalent Privacy), 923
WEP (Wireless Encryption Protocol), 567
WFX12V power supplies, 154
whaling, 881
while loops, 709-710
whoami command, 690-691
Widgets, macOS, 820
widths, channels, 556
Wi-Fi
analyzers, 386, 558
antenna connectors, 405
antennas, 407
calling, 370
connectivity, troubleshooting, 425-426
M-2 slots, 218-219
networks. *See* WLAN
Wi-Fi 5 (802.11ac) wireless standard, 375, 548
Wi-Fi 6 (802.11ax) wireless standard, 375, 548
Wi-Fi 7 (802.11be) wireless standard, 375, 548
WiGig (802.11ad) wireless standard, 548
wildcards, 664
Windows, 616
activation clocks, 734
adding devices
audio devices, 746
clock drift, 750
Device Manager, 743-748
display settings, 746-747
Not enough USB controller resources" error messages, 749-750
Sound utility, 746
USB endpoints, 749-750
Advanced Boot Options menu, 776-777
Apply button, 629
apps
Apps & Features Settings utility, 752
compatibility, 751
disabling, 780
installing, 752
launching, 751
repairing, 753
requirements, 751
side-by-side apps, 722
starting during Windows startup, 784
Automatic Updates, 739
backups, 644-645, 740-741
balanced power, 799
baselines, 785
Bluetooth & Devices Settings utilities, 746
bootrec /fixboot command, 773
bootrec /fixmbr command, 773
bootrec /scanos command, 773
bootup
Advanced Boot Options menu, 776-777
overview, 772
reboots, 797
speeding up boot process, 789-790
System Configuration utility, Windows, 777-780
Task Manager, 782
troubleshooting, 790-791, 795
boot volumes, 772
checkboxes, 630
Close button, 629
command prompt, 656
compatibility, 195, 725-727
Component Services, 755
Computer Management console, 754
Disk Management tool, 765-767
Local Users and Groups tool, 762-764
ODBC Data Sources tool, 770
Print Management console, 771
Services and Applications section, 769
Storage Spaces Control Panel, 768
System Tools section, 755-759
User Account Management section, 759
configuring, 741-743
context menus, 630
context-sensitive help, 630
Control Panel, 641
CPU, requirements, 751
credentials, 759-762
data backups, 740-741
deploying, 733-734
desktop icons, sizing, 634
device drivers, 745-748
Device Manager, 743
dialog boxes, 629-630
digital signatures, 745-746
disabling apps, 780
Disk Cleanup tool, 768
Disk Management, 230, 236-237
display settings, 746

DLL, troubleshooting, 754
dongle requirements, 751
drop-down menus, 630
enhanced features, 722
Error Checking tool, 768
Event Viewer, 756-759
File Explorer
  Content view, 634
  copying files, 640
  Details view, 634
  display options, 634
  file attributes, 637
  file compression, 639
  file encryption, 639
  file structures, 658-659
  indexing, 636
  List view, 634
  moving files, 640
  paths, 632-634
  searches, 635
  starting, 677
  Tiles view, 634
File History backups, 741
files
  attributes, 637
  compression, 639
  copying, 640
  encryption, 639
  extensions, 631-632
  filenames, 631
  moving, 640
  paths, 632-634
  saving, 632
  structures, 658-659
file systems, 728-729
folders
  attributes, 637
  compression, 639
  copying, 640
  encryption, 639
  moving, 640
  naming, 631
  subfolders, 631
graphics cards, 751
Group Policy, 677-678
hard drives
  planning drive space, 729
  space requirements, 751
hibernation mode, 799
high performance power plans, 799
Hyper-V, 73, 722
indexing, 636
Installation Assistant, 725
installing
  antivirus software, 732
  backups before OS installations, 731
  clean installations, 723
  compatibility mode, 727
  corporate deployments, 733-734
  disabling interfering software, 732
  drivers, 731
  file systems, 728-729
  hardware, 730
  image deployments, 723
  in-place upgrades, 723-724
  installation media, 726
  licenses, 734
  multiboots, 723
  partitions, 727-730
  PCmover Express, 726
  phases of, 732
  recovery partitions, 723
  remote network installations, 723
  repair installations, 723, 738
  resets/restores, 723
  security scans, 731
  selecting networks, 732
  selecting network type, 733
  troubleshooting installations, 735-736
  types of installations, 722
  unattended installations, 723
  USMT, 726
  verifying installations, 735
  ZTI, 723
libraries, 631
licenses, 734
Local Users and Groups tool, 762-763
memory
  Memory Diagnostic tool, 196
  performance, 785
microphones, 280-281
Microsoft Store, 722
multi-monitor taskbars, 722
network settings, 590-594, 796-797
Notepad, 683
  batch scripting, 692
  printing from, 342
ODBC Data Sources tool, 770
OEM versions, 725
older apps, compatibility, 195
OneDrive, 722
OOBE, 732
Optimize Drives tools, 768-769
partitions, 727-730
performance, monitoring, 784
  baselines, 785
  Performance Monitor, 787-788
  Reliability Monitor, 789
  Resource Monitor, 788
  Task Manager, 785-787
planning drive space, 729
power options, 799-800
power saver plans, 799
PowerShell (.psl), 694
  cmdlets, 712
  .NET Core, 712
  opening, 666
printers, 327-328, 331
  connectivity, 342-343
  default printers, 328
  print drivers, 329-330
  print queues, 329
  sharing, 332-333
  testing, 329
Print Management console, 771
productivity, cloud-based productivity tools, 804-807
profiles, 795-796
Program Compatibility Troubleshooter, 727
radio buttons, 630
RAM requirements, 751
ReadyBoost, 790
rebooting, 748
recovery, 645-646, 791
ReFS, 768
    registry, 116
  backups, 644, 740-741
  editing, 643
  regedit command, 685
  regedit.exe command prompt, 643
  regedit program (.reg), 741

INDEX

regedt32.exe command prompt, 643
regsvr32 command, 685
subtrees, 643
troubleshooting, 793
user profiles, 643
reimaging computers, 734
reinstalling, 738
Reliability Monitor, measuring performance, 789
reloading, 737-738
reload OS, 645
remote desktops
Remote Assistance, 801-803
Remote Desktop Connection, 801-803
starting, 680
repair installations, 738
resetting PC, 795
Resource Monitor, measuring performance, 788
restore points, 646, 737-738, 741
roll back updates, 739
Safe Mode
bootups, 777
troubleshooting slow boots, 795
services
learning about, 794
restarting, 794
troubleshooting, 793
Services and Applications, 769
setup log files, 736-737
sfc, 738
shutdowns, troubleshooting, 798
snap-ins, 754-755
software
installing, 750-752
removing, 750-751
sound cards, 279
Sound utility, 746
SRU, 738
Start screen, 630
startup
disabling startup programs, 791
starting apps during startup, 784
Startup Settings menu, 776-777
Storage Spaces Control Panel, 768
subdirectories, 631
Sync Center Control Panel utility, 752
synchronization, 752
System Configuration utility, 777-780
system files, 772-773
System Image Recovery, 791
system images, 644-645
System Information window, 680
system instability, troubleshooting, 797
System Restore utility, 737, 741
system volumes, 772
tabs, 629
Task Manager, 782
App history tab, 783
CPU tab, 786
Details tab, 784
measuring performance, 785-787
Memory tab, 786
Performance tab, 193-194, 782, 785-787
Services tab, 784
Startup apps tab, 783
Users tab, 784, 787
Task Scheduler, 755
textboxes, 629
threads, 786
troubleshooting
black screens, 792-793
bootups, 790-791, 795
DLL, 754
installations, 735-736
summary of steps, 799
system instability, 797
video issues, 792-793
Windows Troubleshooting Wizard, 750
UAC, 722
updating, 735
Automatic Updates, 739
changing settings, 740
roll back updates, 739
Windows Update, 739-740
Windows Update Assistant, 725
upgrading, 723-724, 731
user account management
administrator accounts, 763
Credential Manager, 759, 762
Local Users and Groups tool, 762-763
recovering user accounts, 763-764
rights, 762
standard user accounts, 763
UAC, 764
user profiles, 643
USMT, 726
versions, 642, 691
VRAM requirements, 751
WDS, 734
Windows ADK, 734
Windows Defender Firewall, 914-917
Windows Disk Cleanup, 244
Windows Hello, 412, 874
Windows interactions, 629-630
Windows Storage Spaces, 240-241
Windows Time Service, 750
Windows Troubleshooting Wizard, 750
Windows Update Assistant, 725
Windows Updates, 739-740
Windows XP Mode, 502
WinRE, 249, 645, 662, 722-776
WinRM, 918
workgroups, 622
WRP, 738
Windows 10
basic usage overview, 623
configuration settings, 742
desktops, 623
Disk Management, partitioning hard drives, 232
Enterprise edition, 618
File Explorer, View tab options, 897-898
hardware requirements, 730
Home edition, 618
Hyper-V, 727
icons, 623
memory
limitations, 183-184
recommendations, 183
Microsoft Defender, 906

N versions, 618
OOBE, 623
Pro and Pro Education editions, 618
Pro for Workstations edition, 618
Settings app, 640-641
upgrading, paths, 724
Windows 11 comparisons, 619
Windows Backup, 901
Windows Hello, 874
Windows Update Assistant, 725
wireless security, 924
Windows 11
Apps utility, 752
configuration settings, 742
Control Panel, 641
desktops, 623-627
Enterprise edition, 618
File Explorer, 615, 630
accessing, 897
Options button, 635
View tab options, 897-898
hardware requirements, 730
Home edition, 618
Hyper-V, 727
icons, 623
indexing options, 636
Installation Assistant, 725
memory, 183-184
Microsoft Defender, 906
N versions, 618
OOBE, 623
Pro and Pro Education editions, 618
Pro from Workstations edition, 618-619
Recycle Bin, 628
Settings app, 640-641
shortcuts, 627
tiles, 627
upgrading, paths, 724
Windows 10 comparisons, 619
Windows Backup, 901
Windows Hello, 874
wireless security, 923
WinRE (Windows Recovery Environment), 249, 645, 662, 722-776
WinRM (Windows Remote Management), 918
winver command, 691
wiping
hard drives, 904
mobile devices, 411
wire (cable) strippers, 529, 537
wired connectivity, 559
Ethernet, projectors, 275
mobile devices, 371-373
printers, 325
wireless antennas, 541
directional antennas, 556
gain, 557
laptops, 406
MIMO, 558
MU-MIMO, 558
omnidirectional antennas, 556
path loss, 556
radiation patterns, 556
ranges, 557
signal strength, 558
wireless AP
changing usernames/passwords, 570
configuring, 570
DMZ, 571
installing, 926-927
wireless bridges, 548
wireless broadband, 490
wireless cards
laptops, 389
replacing, 404
wireless connectivity
Bluetooth, 55
IR, 55
long-range fixed wireless, 490
mobile devices
802.11 wireless standard, 375-376
Airplane mode, 376
biometric security, 378
Bluetooth, 373-374
cellular data, 379
hotspots, 377
IR, 379
NFC, 377-378
tethering, 377
NFC, 55
power requirements, 491-492
presenters, 55
projectors, 275
radio, 55
wireless broadband, 490
wireless extenders, 551
wireless locators, 386
wireless networks
802.11ac (Wi-Fi 5) wireless standard, 548
802.11ad (WiGig) wireless standard, 548
802.11a wireless standard, 548
802.11ax (Wi-Fi 6) wireless standard, 548
802.11be (Wi-Fi 7) wireless standard, 548
802.11b wireless standard, 548
802.11e wireless standard, 548
802.11g wireless standard, 548
802.11i wireless standard, 548
802.11n wireless standard, 548
AC addresses, 921
antennas, 556-558
AP, 548-552, 921, 926-927
Basic QoS, 571
bridges, 548
channel ID, 553-556, 571
configuration profiles, 922
content filtering, 571
data transfer speeds, 559
design, 550
desktop workstations, 547
device connectivity, 559
DHCP, 571
DMZ, 571
DNAT, 571
extenders, 551
external interference, 558-559
firewalls, 922
firmware, 571
frequencies, 546
frequency bands, 550
guest access, 927
intermittent wireless connectivity, 558
IoT, 572-573
IP filtering, 571
MDM, 922
multifunction devices, 548
NAT, 571

NIC, 548, 549
overview, 546
port forwarding/mapping, 571
printers, 325, 334-335
QoS, 571
regulations, 556
repeaters, 552
routers, 548, 549
security, 923-928
AP, 926-927
DMZ, 924
IP address filtering, 925
MAC address filtering, 924
TKIP, 923
WEP, 923
WPA, 923
WPA2, 923
WPA3, 923
WPS, 925
signal strength, 426
site surveys, 557
SSID, 571
transmit power, reducing, 926
troubleshooting, 928
UPnP, 571
Wi-Fi analyzers, 558
WLAN, 518, 523, 921
WMN, 518
WWAN, 518, 572
wireless NIC, 376, 567-568
Wireless option, AP configurations, 570
wireless printers, 334-336
wireless regulations, 556
wireless repeaters, AP as, 552
wireless routers, 541
changing usernames/passwords, 570
DHCP server configurations, 562
DMZ, 571
installing, 926-927
IP filtering, 925
static IP addressing, 561
wireless security, 927-928
DMZ, 924
IP address filtering, 925
MAC address filtering, 924
TKIP, 923
WEP, 923
Windows 10, 924
Windows 11, 923
WPA, 923
WPS, 925
wiring standards
T568A, 51, 528
T568B, 528
WISP (Wireless Internet Service Providers), 490
WLAN (Wireless LAN), 518, 523, 921
WMN (Wireless Mesh Networks), 518
work ethics (soft skills), 348
workgroups, 521-523, 622, 733
workplace safety
environmental impacts, 945-946
equipment, 944
fire extinguishers, 943
fire safety, 943
government regulations, 942
lifting techniques, 945
MSDS, 943
OSHA, 943
personal safety, 945
trip hazards, 952
ventilation, 959
workstations
account expiration dates, 890
audio/video workstations, 442
graphic/CAD/CAM workstations, 441
group policy editor, 890
guest accounts, disabling, 890
login times, restricting, 890
OS, 619
passwords, 890
Pro for Workstations edition, Windows 10/11, 618-619
thick workstations, 445
thin workstations, 444
timeout/screen locks, 890
user permissions, restricting, 890
virtualization workstations, 443
wireless connectivity, 547
WPA (Wi-Fi Protected Access), 568, 923
WPA2 (Wi-Fi Protected Access 2), 568, 923
WPA3 (Wi-Fi Protected Access 3), 568, 923
.WPS files, 632
WPS (Wi-Fi Protected Setup), 925
.WRI files, 632
wrist straps, antistatic, 136-137
writable media, optical drives, 284
Write permissions, 895
writing
commands, 666
communication skills, 166
WRP (Windows Resource Protection), 738
wscript command, 691
WWAN (Wireless WAN), 518, 572

X-Y-Z

x64 processors, 66
x86 processors, 66
xcopy command, 664-665, 691-692
XDR (Extended Detection and Response), 884
xDSL modems, 483-484
Xeon processors, 74
XFS (Extended File Systems), 843
XLS (XLSX) files, 632
XMP (Extreme Memory Profiles), 182
XPS files, Print to XPS (virtual printing), 316
XSS (Cross-Site Scripting) attacks, 883

YB (Yottabytes), 20
YiB (Yobibytes), 20

ZB (Zettabytes), 20
zero-day attacks, 883
Zero Trust models, 870
zeroing out devices, Linux, 852
ZFS, 843
ZiB (Zebibytes), 20
ZIF sockets, 76
ZIP files, 632
zombie attacks, 883
zooming in/out of objects, mobile devices, 366
ZTI (Zero-Touch Installations), 723

To receive your 10% off Exam Voucher, register your product at:

www.pearsonitcertification.com/register

and follow the instructions.

Pearson

Where are the companion content files?

Thank you for purchasing this Premium Edition version of Complete A+ Guide to IT Hardware and Software

This product comes with companion content. You have access to these files by following the steps below:

1. Go to **pearsonITcertification.com/register** and log in.
2. Click on the "Access Bonus Content" link in the Registered Products section of your account page for this product, to be taken to the page where your downloadable content is available.

Please note that many of our companion content files can be very large, especially image and video files.

If you are unable to locate the files for this title by following the steps at left, please visit **pearsonITcertification.com/support** and select the chat, phone, or web ticket options to get help from a tech support representative.

The Professional and Personal Technology Brands of Pearson

Addison Wesley · Cisco Press · informIT · PEARSON IT Certification · que · SAMS

From the Library of Zanac Hsia