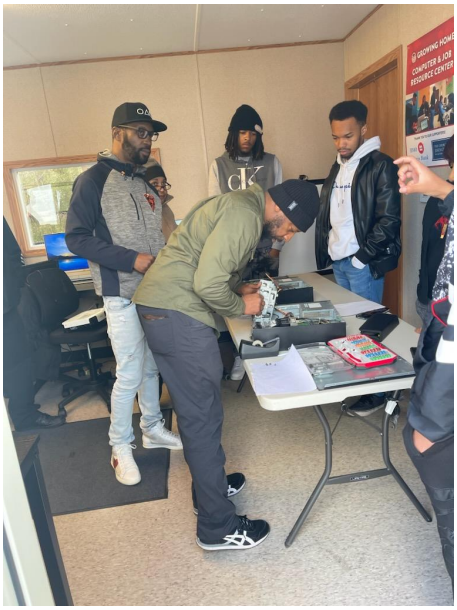
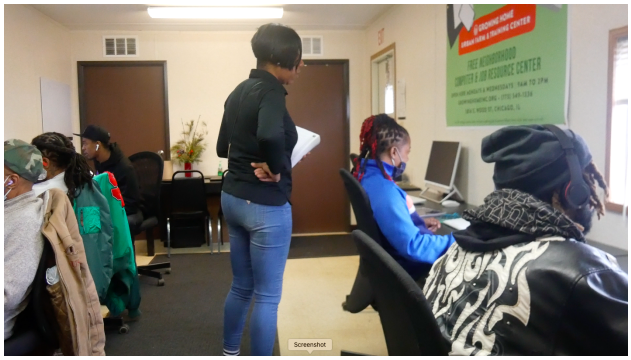
GROWING HOME

2022/2023 Growing Home IT-Training Photos

Please enjoy these photos of Growing Home's IT-Training and Workforce Development Programs in action! We invite you to come tour our facilities and see our program in person when you have the availability.



Growing Home IT-Technology Participants engage in hands-on learning to understand the ins and outs of computer technology at our Resource Center.



Growing Home staff provide one-on-one and group learning environments for trainees in our programs. Photo to the right shows half of our brand new Computer Resource Center, open to participants and the public for free.

6429 S. Honore St, Chicago, IL 60636 | 773.549.1336
www.growinghomeinc.org

GROWING HOME

Growing Home trainees attend job fairs alongside Growing Home staff. Left is Growing Home trainees dressed professionally and ready to go for interviews! Right are two Growing Home graduates at a job fair, engaging live with employers (and dressed stylishly with Growing Home's partnership with Dress for Success!).

Growing Home Workforce Development staff out recruiting at various hiring and resource fairs in the community.

6429 S. Honore St, Chicago, IL 60636 | 773.549.1336
www.growinghomeinc.org

Growing Home IT-Training Curriculum

As part of our current 8-Week IT-Training, Growing Home follows the first part of the Cisco-IT Essentials Curriculum (Part 1).

With Growing Home's plan to expand to a 12-week IT-Training Program in CompTia Certifications in the Fall of 2023, Growing Home will follow the A+, Network and Security+ curriculum that coincide with the training and exam certification. Attached are the curriculum guide as well as sample lessons for each certification (Part 2, 3, 4).

GROWING HOME

GROWING HOME | CISCO | CompTIA

IN ENGLEWOOD

LEARN THE LATEST IN INFORMATION TECHNOLOGY START YOUR CAREER WITH OUR INDUSTRY-RECOGNIZED TRAINING.

- Stipend program available
- Paid Internship Opportunity Upon Graduation
- IT Essentials Certificate from CISCO or COMPTIA Network
- 8-Week Program

UPCOMING TRAINING

- Mon. thru Wed. 9am-12pm
- April 17 - June 12
- July 10 - September 4
- Sept. 25 - November 20

REGISTER NOW

5814 S. Wood Street, Chicago IL 60636
Phone: 773.434.7144, Option 4
Email: info@growinghomeinc.org
Online: growinghomeinc.org/center
QR Scan Code and Register

Growing Home IT-Training Curriculum

Cisco-IT Essentials Curriculum (Part 1)

6429 S. Honore St, Chicago, IL 60636 | 773.549.1336
www.growinghomeinc.org

CISCO

IT Essentials

PC Hardware and Software Companion Guide

Fourth Edition

Cisco | Networking Academy®
Mind Wide Open™

IT Essentials: PC Hardware and Software Companion Guide

Fourth Edition

Cisco Networking Academy

Cisco Press

800 East 96th Street

Indianapolis, Indiana 46240 USA

IT Essentials: PC Hardware and Software Companion Guide, Fourth Edition

Cisco Networking Academy

Copyright© 2011 Cisco Systems, Inc.

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

All rights reserved. No part of this book may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or by any information storage and retrieval system, without written permission from the publisher, except for the inclusion of brief quotations in a review.

Printed in the United States of America

First Printing October 2010

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

ISBN-13: 978-1-58713-263-6

ISBN-10: 1-58713-263-x

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

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

Warning and Disclaimer

This book is designed to provide information about the Cisco Networking Academy IT Essentials: PC Hardware and Software course. Every effort has been made to make this book as complete and as accurate as possible, but no warranty or fitness is implied.

The information is provided on an "as is" basis. The authors, Cisco Press, and Cisco Systems, Inc. shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this book or from the use of the discs or programs that may accompany it.

The opinions expressed in this book belong to the author and are not necessarily those of Cisco Systems, Inc.

Publisher
Paul Boger

Associate Publisher
Dave Dusthimer

Manager, Global Certification
Erik Ullanderson

Business Operation Manager, Cisco Press
Anand Sundaram

Executive Editor
Mary Beth Ray

Managing Editor
Sandra Schroeder

Development Editor
Dayna Isley

Senior Project Editor
Tonya Simpson

Copy Editor
Bill McManus

Technical Editors
Rick McDonald,
William Shurbert

Editorial Assistant
Vanessa Evans

Book Designer
Louisa Adair

Cover Designer
Sandra Schroeder

Composition
Studio Galou, LLC

Indexer
Tim Wright

Proofreader
Sheri Cain

Trademark Acknowledgments

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

Corporate and Government Sales

The publisher offers excellent discounts on this book when ordered in quantity for bulk purchases or special sales, which may include electronic versions and/or custom covers and content particular to your business, training goals, marketing focus, and branding interests. For more information, please contact: **U.S. Corporate and Government Sales** 1-800-382-3419 corpsales@pearsontechgroup.com

For sales outside the United States, please contact: **International Sales** international@pearsoned.com

Feedback Information

At Cisco Press, our goal is to create in-depth technical books of the highest quality and value. Each book is crafted with care and precision, undergoing rigorous development that involves the unique expertise of members from the professional technical community.

Readers' feedback is a natural continuation of this process. If you have any comments regarding how we could improve the quality of this book, or otherwise alter it to better suit your needs, you can contact us through email at feedback@ciscopress.com. Please make sure to include the book title and ISBN in your message.

We greatly appreciate your assistance.

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

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

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

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

©2007 Cisco Systems, Inc. All rights reserved. CCVP, the Cisco logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, Packet, PIX, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0609R)

About the Contributing Editor

Ben Conry (CCNA, CCAI, A+) is the lead instructor for Information Technology Essentials in the Baltimore County Public Schools. He teaches computer repair, networking, and cybersecurity at Sollers Point Technical High School. Conry has been honored for his commitment to educational excellence and for preparing students for college and the work force, and is recognized widely as an authority on the CompTIA A+ exam. He co-authored the Maryland State Department of Education core learning goals for Cisco Academy IT Essentials. Conry holds a master's degree in instructional technology from Johns Hopkins University. He lives in Lutherville, Maryland with his wife, Marisa, and their children, Daniel and Elijah.

About the Technical Reviewers

Rick McDonald teaches computer and networking courses via distance at the University of Alaska Southeast in Ketchikan, Alaska, where he is an associate professor. He holds a BA degree in English and an MA degree in educational technology from Gonzaga University in Spokane, Washington. After several years in the airline industry, he returned to full-time teaching. Rick started in the Cisco Academy in North Carolina and taught CCNA and CCNP courses and was a CCNA instructor trainer. Previous Academy projects include co-authoring *Network Fundamentals, CCNA Exploration Companion Guide*, and co-authoring *Routers and Routing Basics, CCNA 2 Companion Guide*. He also developed CCNP study guides and contributed as a technical editor on a previous edition of the CCNA 2 and 3 textbooks. His current project is developing methods for delivering hands-on training via distance in Alaska using web conferencing and NETLAB tools.

Bill Shurbert is a professor of information technology at NHTI, Concord's Community College, in Concord, New Hampshire. Bill holds a bachelor's degree in technical management from Southern New Hampshire University. He enjoys teaching Cisco CCNA and Wireless networking classes. In his off time, you can find Bill and Joanne, his wife of 28+ years, sailing the waters of Lake Winnipesaukee.

Contents at a Glance

Introduction xxxvi

Chapter 1: Introduction to the Personal Computer 1

Chapter 2: Safe Lab Procedures and Tool Use 51

Chapter 3: Computer Assembly–Step by Step 79

Chapter 4: Basics of Preventive Maintenance and Troubleshooting 103

Chapter 5: Fundamental Operating Systems 115

Chapter 6: Fundamental Laptops and Portable Devices 187

Chapter 7: Fundamental Printers and Scanners 239

Chapter 8: Fundamental Networks 277

Chapter 9: Fundamental Security 345

Chapter 10: Communication Skills 377

Chapter 11: Advanced Personal Computers 403

Chapter 12: Advanced Operating Systems 465

Chapter 13 Advanced Laptops and Portable Devices 515

Chapter 14 Advanced Printers and Scanners 551

Chapter 15: Advanced Networks 585

Chapter 16 Advanced Security 633

Appendix: Answers to Check Your Understanding Questions 671

Glossary 675

Index 713

Contents

Introduction xxxvi

Chapter 1 Introduction to the Personal Computer 1

Objectives 1

Key Terms 1

Explain IT Industry Certifications 3

Identify Education and Certifications 4

Describe the A+ Certification 5

Describe the EUCIP Certification 5

Module 1: PC Hardware 5
Module 2: Operating Systems 5
Module 3: Local Area Network and Network Services 6
Module 4: Expert Network Use 6
Module 5: IT Security 6

Describe a Computer System 6

Identify the Names, Purposes, and Characteristics of Cases and Power Supplies 7

Describe Cases 7

Describe Power Supplies 9

Connectors 9
Electricity and Ohm's Law 10

Identify the Names, Purposes, and Characteristics of Internal Components 12

Identify the Names, Purposes, and Characteristics of Motherboards 13

Identify the Names, Purposes, and Characteristics of CPUs 14

Identify the Names, Purposes, and Characteristics of Cooling Systems 19

Identify the Names, Purposes, and Characteristics of ROM and RAM 20

ROM 20
RAM 21
Memory Modules 22
Cache Memory 22
Error Checking 22

Identify the Names, Purposes, and Characteristics of Adapter Cards 23

Identify the Names, Purposes, and Characteristics of Storage Drives 24

Floppy Drive 25
Hard Drive 25
Optical Drive 26
External Flash Drive 26
Types of Drive Interfaces 26

Identify the Names, Purposes, and Characteristics of Internal Cables 29

Identify the Names, Purposes, and Characteristics of Ports and Cables 30

Serial Ports and Cables 31

Modem Ports and Cables 31

USB Ports and Cables 32

FireWire Ports and Cables 32

Parallel Ports and Cables 33

SCSI Ports and Cables 34

Network Ports and Cables 34

PS/2 Ports 35

Audio Ports 36

Video Ports and Connectors 36

Identify the Names, Purposes, and Characteristics of Input Devices 37

Identify the Names, Purposes, and Characteristics of Output Devices 39

Monitors and Projectors 39

All-in-One Printer 42

Speakers and Headphones 42

Explain System Resources and Their Purposes 43

Interrupt Requests 43

Input/Output (I/O) Port Addresses 44

Direct Memory Access 45

Summary 47

Summary of Exercises 47

Check Your Understanding 48

Chapter 2 Safe Lab Procedures and Tool Use 51

Objectives 51

Key Terms 51

Explain the Purpose of Safe Working Conditions and Procedures 52

Identify Safety Procedures and Potential Hazards for Users and Technicians 52

General Safety Guidelines 53
Electrical Safety Guidelines 53
Fire Safety Guidelines 53

Identify Safety Procedures to Protect Equipment from Damage and Data from Loss 55

Electrostatic Discharge 55
Electromagnetic Interference 56
Climate 56
Power Fluctuation Types 56
Power Protection Devices 57

Identify Safety Procedures to Protect the Environment from Contamination 58

Material Safety Data Sheet 58
Proper Disposal of Batteries 60
Proper Disposal of Monitors or CRTs 60
Proper Disposal of Toner Kits, Cartridges, and Developers 61
Proper Disposal of Chemical Solvents and Aerosol Cans 61

Identify Tools and Software Used with Personal Computer Components and Their Purposes 61

Identify Hardware Tools and Their Purpose 62

ESD Tools 62
Hand Tools 62
Cleaning Tools 63
Diagnostic Tools 63

Identify Software Tools and Their Purpose 63

Disk Management Tools 63
Protection Software Tools 64

Identify Organizational Tools and Their Purpose 65

Personal Reference Tools 65
Internet Reference Tools 65
Miscellaneous Tools 66

Implement Proper Tool Use 68

Demonstrate Proper Use of an Antistatic Wrist Strap 68

Demonstrate Proper Use of an Antistatic Mat 70

Antistatic Mat 70
Workbench 70

Demonstrate Proper Use of Various Hand Tools 71

Screws 71
Flat-Head Screwdriver 71
Phillips-Head Screwdriver 72
Hex Driver 72
Part Retriever, Needle-Nose Pliers, or Tweezers 72

Demonstrate Proper Use of Cleaning Materials 73

Computer Cases and Monitors 74
LCD Screens 74
CRT Screens 74
Component Contacts 74
Keyboard 74
Mouse 75

Summary 76

Summary of Exercises 76

Labs 76

Worksheets 76

Check Your Understanding 77

Chapter 3 Computer Assembly—Step by Step 79

Objectives 79

Key Terms 79

Open the Case 80

Install the Power Supply 80

Attach the Components to the Motherboard and Install the Motherboard 81

Install a CPU and a Heat Sink/Fan Assembly 82

CPU 82
Heat Sink/Fan Assembly 83

Install the RAM 84

Install the Motherboard 85

Install Internal Drives 86

Install Drives in External Bays 86

Install the Optical Drive 86

Install the Floppy Drive 87

Install Adapter Cards 88

Install the NIC 88

Install the Wireless NIC 89

Install the Video Adapter Card 89

Connect All Internal Cables 91

Connect the Power Cables 91

Motherboard Power Connections 91
SATA Power Connectors 91
Molex Power Connectors 91
Berg Power Connectors 92

Connect the Data Cables 92

PATA Data Cables 92
SATA Data Cables 92

Reattach the Side Panels and Connect External Cables to the Computer 93

Reattach the Side Panels to the Case 93

Connect External Cables to the Computer 93

Floppy Drive Data Cables 94

Boot the Computer for the First Time 96

Identify Beep Codes 96

Describe BIOS Setup 97

Summary 99

Summary of Exercises 99

Labs 99

Virtual Desktop Activities 100

Check Your Understanding 100

Chapter 4 Basics of Preventive Maintenance and Troubleshooting 103

Objectives 103

Key Terms 103

Explain the Purpose of Preventive Maintenance 104

Hardware 104

Software 105

Benefits 105

Identify the Steps of the Troubleshooting Process 106

Explain the Purpose of Data Protection 106

Data Backup 107

Identify the Problem 107

Conversation Etiquette 108
Open-Ended Questions 108
Closed-Ended Questions 108
Documenting Responses 109
Event Viewer 109
Device Manager 110
Beep Codes 110
BIOS Information 110
Diagnostic Tools 111

Establish a Theory of Probable Causes 111

Test the Theory to Determine an Exact Cause 111

Implement the Solution 111

Verify Solution, Full System Functionality, and If Applicable, Implement Preventive Measures 112

Document Findings, Actions, and Outcomes 112

Summary 113

Summary of Exercises 113

Check Your Understanding 113

Chapter 5 Fundamental Operating Systems 115

Objectives 115

Key Terms 115

Explain the Purpose of an Operating System 117

Describe Characteristics of Modern Operating Systems 117

Control Hardware Access 117
File and Folder Management 118
User Interface 118
Application Management 120

Explain Operating System Concepts 120

Modes of Operation 120
Real Mode 121
Protected Mode 121
Virtual Real Mode 121
Compatibility Mode 122
32-Bit Versus 64-Bit 122
Processor Architecture 123

Describe and Compare Operating Systems to Include Purpose, Limitations, and Compatibilities 123

Describe Desktop Operating Systems 123

Microsoft Windows 124
Apple Mac OS 124
UNIX/Linux 125

Describe Network Operating Systems 125

Determine Operating System Based on Customer Needs 126

Identify Applications and Environments That Are Compatible with an Operating System 126

Determine Minimum Hardware Requirements and Compatibility with the OS Platform 127

Hardware Compatibility List 128

Install an Operating System 129

Identify Hard Drive Setup Procedures 130

Partitioning and Formatting 130

Prepare the Hard Drive 131

Install the Operating System Using Default Settings 134

Create User Accounts 136

Complete the Installation 137

Describe Custom Installation Options 139

Disk Cloning 139
Network Installation 140
Recovery Disc 140

Factory Recovery Partition *141*

Identify the Boot Sequence Files and Registry Files 141

Windows XP Boot Process *141*
NTLDR and the Windows Boot Menu *142*
Windows Registry *142*
NT Kernel *143*

Describe How to Manipulate Operating System Files 143

Startup Modes *144*

Describe Directory Structures 145

File Extensions and Attributes *145*
Describe NTFS and FAT32 *147*

Navigate a GUI (Windows) 148

Manipulate Items on the Desktop 149

Display Properties *150*
Desktop Items *150*
Start Menu *151*
My Computer *151*
Launching Applications *152*
My Network Places *152*

Explore Control Panel Applets 153

Control Panel Applets *153*
Display Settings *155*

Explore Administrative Tools 155

Computer Management *156*
Device Manager *156*
Task Manager *157*
Services *158*
Performance Monitor *158*
Event Viewer *159*
MMC *159*
Remote Desktop *160*
Performance Settings *160*

Install, Navigate, and Uninstall an Application 161

Add or Remove Programs Applet *162*
Add an Application *162*
Uninstall an Application *163*

Describe Upgrading an Operating System 164

Upgrading the Operating System to Windows XP *164*
Upgrading the Operating System to Windows Vista *165*

Identify and Apply Common Preventive Maintenance Techniques for Operating Systems 166

Create a Preventive Maintenance Plan 166

Preventive Maintenance Planning 166
Device Driver Updates 167
Firmware Updates 167
Operating System Updates 167
Security 167
Startup Programs 168

Schedule a Task 168

System Utilities 169
Automatic Updates 169
Restore Point 170
Backup Status and Configuration 171
ERD and ASR 172

Back Up the Hard Drive 172

Normal Backup 173
Copy Backup 173
Differential Backup 173
Incremental Backup 174
Daily Backup 174
Backup Media 174

Troubleshoot Operating Systems 175

Review the Troubleshooting Process 175

Step 1: Identify the Problem 175
Step 2: Establish a Theory of Probable Causes 176
Step 3: Determine an Exact Cause 176
Step 4: Implement a Solution 177
Step 5: Verify Solution and Full System Functionality 177
Step 6: Document Findings 178

Identify Common Problems and Solutions 178

Summary 182

Summary of Exercises 182

Labs 182

Worksheets 183

Check Your Understanding 183

Chapter 6 Fundamental Laptops and Portable Devices 187

Objectives 187

Key Terms 187

Describe Laptops and Other Portable Devices 189

Identify Common Uses of Laptops 190

Identify Common Uses of PDAs and Smartphones 190

Identify and Describe the Components of a Laptop 191

Describe the Components Found on the Outside of the Laptop 192

Describe Input Devices Found on Laptops 196

Describe the Components Found on the Laptop Docking Station 199

Compare and Contrast Desktop and Laptop Components 202

Compare and Contrast Desktop and Laptop Motherboards 202

Compare and Contrast Desktop and Laptop Processors 203

Compare and Contrast Desktop and Laptop Power Management 203

Compare and Contrast Desktop and Laptop Expansion Capabilities 204

Explain How to Configure Laptops 208

Describe How to Configure Power Settings 209

Configuring Power Settings in Windows XP and Vista 211
Managing Power Usage 211
Power Management for the Hard Drive and the Display 212
Setting the Laptop Power Options 213
Adjusting Low Battery Warnings 214

Describe the Safe Installation and Removal of Laptop Components 215

Battery Replacement Steps 216
Optical Drive Replacement Steps 216
Hard Drive Replacement Steps 217
Expansion Memory Replacement Steps 217
PC Expansion Card Replacement Steps 217
Hot-Swappable Device Removal Steps 218

Laptop Communication Hardware Installation and Configuration 218

Ethernet Installation and Configuration Steps 218
Wireless Ethernet Installation and Configuration Steps 219
Modem Installation and Configuration Steps 219
Bluetooth Installation and Configuration Steps 220
Infrared Installation and Configuration Steps 220
Cellular WAN Installation and Configuration Steps 221

Growing Home IT-Training Curriculum

CompTia A+ Certification (Part 2)

6429 S. Honore St, Chicago, IL 60636 | 773.549.1336
www.growinghomeinc.org

CompTIA

The Official CompTIA

A+

Core 1 Study Guide

Exam 220-1101

Official CompTIA Content Series for CompTIA Performance Certifications

Course Edition: 1.0

Acknowledgments

James Pengelly, Author

Becky Mann, Director, Product Development

James Chesterfield, Senior Manager, User Experience and Design

Danielle Andries, Manager, Product Development

Notices

Disclaimer

While CompTIA, Inc. takes care to ensure the accuracy and quality of these materials, we cannot guarantee their accuracy, and all materials are provided without any warranty whatsoever, including, but not limited to, the implied warranties of merchantability or fitness for a particular purpose. The use of screenshots, photographs of another entity's products, or another entity's product name or service in this book is for editorial purposes only. No such use should be construed to imply sponsorship or endorsement of the book by nor any affiliation of such entity with CompTIA. This courseware may contain links to sites on the Internet that are owned and operated by third parties (the "External Sites"). CompTIA is not responsible for the availability of, or the content located on or through, any External Site. Please contact CompTIA if you have any concerns regarding such links or External Sites.

Trademark Notice

CompTIA®, A+®, and the CompTIA logo are registered trademarks of CompTIA, Inc. in the United States and other countries. All other product and service names used may be common law or registered trademarks of their respective proprietors.

Copyright Notice

Copyright © 2022 CompTIA, Inc. All rights reserved. Screenshots used for illustrative purposes are the property of the software proprietor. Except as permitted under the Copyright Act of 1976, no part of this publication may be reproduced or distributed in any form or by any means, or stored in a database or retrieval system, without the prior written permission of CompTIA, 3500 Lacey Road, Suite 100, Downers Grove, IL 60515-5439.

This book conveys no rights in the software or other products about which it was written; all use or licensing of such software or other products is the responsibility of the user according to terms and conditions of the owner. If you believe that this book, related materials, or any other CompTIA materials are being reproduced or transmitted without permission, please call 1-866-835-8020 or visit **https://help.comptia.org**.

Table of Contents

Lesson 1: Installing Motherboards and Connectors 1

- Topic 1A: Explain Cable Types and Connectors 2
- Topic 1B: Install and Configure Motherboards 17
- Topic 1C: Explain Legacy Cable Types 34

Lesson 2: Installing System Devices 43

- Topic 2A: Install and Configure Power Supplies and Cooling 44
- Topic 2B: Select and Install Storage Devices 52
- Topic 2C: Install and Configure System Memory 65
- Topic 2D: Install and Configure CPUs 72

Lesson 3: Troubleshooting PC Hardware 81

- Topic 3A: Apply Troubleshooting Methodology 82
- Topic 3B: Configure BIOS/UEFI 90
- Topic 3C: Troubleshoot Power and Disk Issues 98
- Topic 3D: Troubleshoot System and Display Issues 110

Lesson 4: Comparing Local Networking Hardware 119

- Topic 4A: Compare Network Types 120
- Topic 4B: Compare Networking Hardware 125
- Topic 4C: Explain Network Cable Types 133
- Topic 4D: Compare Wireless Networking Types 145

Lesson 5: Configuring Network Addressing and Internet Connections 159

- Topic 5A: Compare Internet Connection Types 160
- Topic 5B: Use Basic TCP/IP Concepts 170
- Topic 5C: Compare Protocols and Ports 183
- Topic 5D: Compare Network Configuration Concepts 189

Lesson 6: Supporting Network Services 199

Topic 6A: Summarize Services Provided by Networked Hosts 200

Topic 6B: Compare Internet and Embedded Appliances 212

Topic 6C: Troubleshoot Networks 218

Lesson 7: Summarizing Virtualization and Cloud Concepts 227

Topic 7A: Summarize Client-Side Virtualization 228

Topic 7B: Summarize Cloud Concepts 235

Lesson 8: Supporting Mobile Devices 243

Topic 8A: Set Up Mobile Devices and Peripherals 244

Topic 8B: Configure Mobile Device Apps 261

Topic 8C: Install and Configure Laptop Hardware 274

Topic 8D: Troubleshoot Mobile Device Issues 283

Lesson 9: Supporting Print Devices 293

Topic 9A: Deploy Printer and Multifunction Devices 294

Topic 9B: Replace Print Device Consumables 309

Topic 9C: Troubleshoot Print Device Issues 325

Appendix A: Mapping Course Content to CompTIA® A+® Core 1 (Exam 220-1101) A-1

Solutions S-1

Glossary G-1

Index I-1

About This Course

CompTIA is a not-for-profit trade association with the purpose of advancing the interests of information technology (IT) professionals and IT channel organizations; its industry-leading IT certifications are an important part of that mission. CompTIA's A+ certification is a foundation-level certification designed for professionals with 12 months hands-on experience in a help desk support technician, desk support technician, or field service technician job role.

CompTIA A+ certified professionals are proven problem solvers. They support today's core technologies from security to cloud to data management and more. CompTIA A+ is the industry standard for launching IT careers into today's digital world. It is trusted by employers around the world to identify the go-to person in end-point management and technical support roles. CompTIA A+ is regularly re-invented by IT experts to ensure that it validates core skills and abilities demanded in the workplace.

Course Description

Course Objectives

This course can benefit you in two ways. If you intend to pass the CompTIA A+ Core 1 (Exam 220-1101) certification examination, this course can be a significant part of your preparation. But certification is not the only key to professional success in the field of IT support. Today's job market demands individuals with demonstrable skills, and the information and activities in this course can help you build your skill set so that you can confidently perform your duties in any entry-level PC support role.

On course completion, you will be able to do the following:

- Install, configure, and troubleshoot PC motherboards, system components, and peripheral devices.
- Compare networking hardware types and configure local addressing and Internet connections.
- Summarize uses for network services, virtualization, and cloud computing.
- Support the use of mobile devices and print devices.

Target Student

The Official CompTIA A+ Core 1 (Exam 220-1101) is the primary course you will need to take if your job responsibilities include supporting the use of PCs, mobile devices, and printers within a corporate or small office home office (SOHO) network. You can take this course to prepare for the CompTIA A+ Core 1 (Exam 220-1101) certification examination.

Please note that in order to become A+ certified, a candidate must pass both Exams 220-1101 and 220-1102.

Prerequisites

To ensure your success in this course, you should have 12 months of hands-on experience working in a help desk technician, desktop support technician, or field service technician job role. CompTIA ITF+ certification, or the equivalent knowledge, is strongly recommended.

The prerequisites for this course might differ significantly from the prerequisites for the CompTIA certification exams. For the most up-to-date information about the exam prerequisites, complete the form on this page: www.comptia.org/training/resources/exam-objectives

How to Use the Study Notes

The following notes will help you understand how the course structure and components are designed to support mastery of the competencies and tasks associated with the target job roles and will help you prepare to take the certification exam.

As You Learn

At the top level, this course is divided into **lessons,** each representing an area of competency within the target job roles. Each lesson is composed of a number of topics. A **topic** contains subjects that are related to a discrete job task, mapped to objectives and content examples in the CompTIA exam objectives document. Rather than follow the exam domains and objectives sequence, lessons and topics are arranged in order of increasing proficiency. Each topic is intended to be studied within a short period (typically 30 minutes at most). Each topic is concluded by one or more activities designed to help you apply your understanding of the study notes to practical scenarios and tasks.

In addition to the study content in the lessons, there is a glossary of the terms and concepts used throughout the course. There is also an index to assist in locating particular terminology, concepts, technologies, and tasks within the lesson and topic content.

In many electronic versions of the book, you can click links on key words in the topic content to move to the associated glossary definition, and you can click page references in the index to move to that term in the content. To return to the previous location in the document after clicking a link, use the appropriate functionality in your eBook viewing software.

Watch throughout the material for the following visual cues.

Student Icon	Student Icon Descriptive Text
	A **Note** provides additional information, guidance, or hints about a topic or task.
	A **Caution** note makes you aware of places where you need to be particularly careful with your actions, settings, or decisions so that you can be sure to get the desired results of an activity or task.

As You Review

Any method of instruction is only as effective as the time and effort you, the student, are willing to invest in it. In addition, some of the information that you learn in class may not be important to you immediately, but it may become important later. For this reason, we encourage you to spend some time reviewing the content of the course after your time in the classroom.

Following the lesson content, you will find a table mapping the lessons and topics to the exam domains, objectives, and content examples. You can use this as a checklist as you prepare to take the exam, and review any content that you are uncertain about.

As a Reference

The organization and layout of this book make it an easy-to-use resource for future reference. Guidelines can be used during class and as after-class references when you're back on the job and need to refresh your understanding. Taking advantage of the glossary, index, and table of contents, you can use this book as a first source of definitions, background information, and summaries.

Lesson 1

Installing Motherboards and Connectors

LESSON INTRODUCTION

One of the main roles for a CompTIA A+ technician is to install and configure personal computer (PC) hardware. This hands-on part of the job is what draws many people to a career in information technology (IT) support. As an IT professional, you will set up desktop computers and help end users to select a system configuration and peripheral devices that are appropriate to their work. You will often have to connect peripheral devices using the correct cables and connectors and install plug-in adapter cards.

To complete these tasks, you must understand how the peripheral devices and internal PC components are connected via the motherboard. As you may encounter many different environments in your work, you must also be able to distinguish and support both modern and legacy connection interfaces.

Lesson Objectives

In this lesson, you will:

- Explain cable types and connectors.
- Install and configure motherboards.
- Explain legacy cable types.

Topic 1A

Explain Cable Types and Connectors

CORE 1 EXAM OBJECTIVES COVERED

3.1 Explain basic cable types and their connectors, features, and purposes.

A PC is made up of many different components. All these components need to be able to communicate with each other so that the computer can function properly. If you can distinguish connection interfaces and connectors quickly, you will be able to support users by installing, upgrading, and replacing PC peripherals efficiently.

Personal Computers

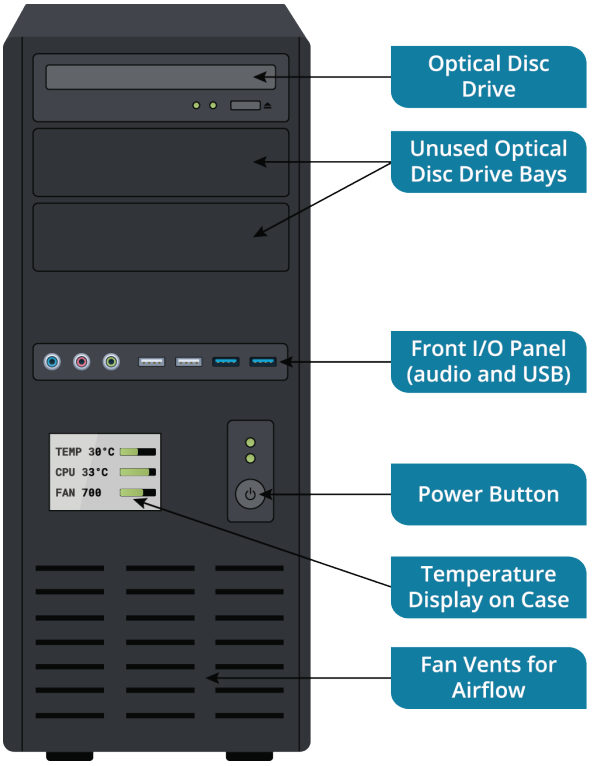
The components of a personal computer (PC) are divided between those that are designed to be handled by the user—peripheral devices—and those that would be damaged or dangerous if exposed. Peripheral devices typically perform the function of input (keyboard, mouse, microphone, and camera), output (monitor and speakers), or external storage.

The system case/chassis houses the internal components. These include the motherboard, central processing unit (CPU), system memory modules, adapter cards, fixed disks, and power supply unit. Most cases use a tower form factor that is designed to be oriented vertically and can be placed on a desk or on the floor.

PCs can also be purchased as all-in-one units. All-in-one means that the internal components are contained within a case that is also a monitor.

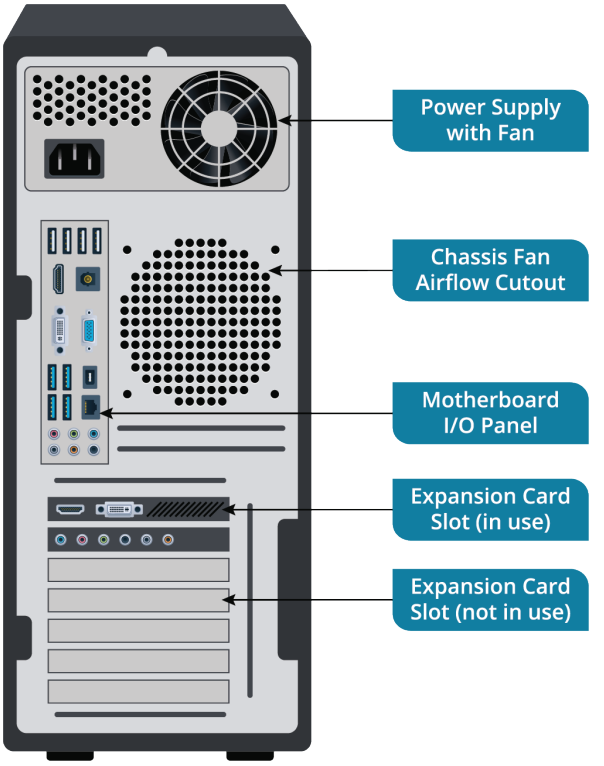
To perform PC maintenance, you must understand how to open a desktop computer's case.

- A tower case has a side cover that can be removed by sliding the panel from its housing. Cases might be secured by screws or retaining clips and might have anti-tamper security mechanisms. Always refer to the system documentation, and follow the recommended steps.
- The front panel provides access to the removable media drives, a power on/off switch, and light- emitting diodes (LEDs) to indicate drive operation. The front cover can be removed but may require the side panel to be removed first to access the screws or clips that secure it.



Features on the front of a typical PC case. (Image © 123RF.com)

The rear panel provides access to the power supply unit (PSU) sockets. The PSU has an integral fan exhaust. Care should be taken that it is not obstructed, as this will adversely affect cooling. There may be an additional case fan.



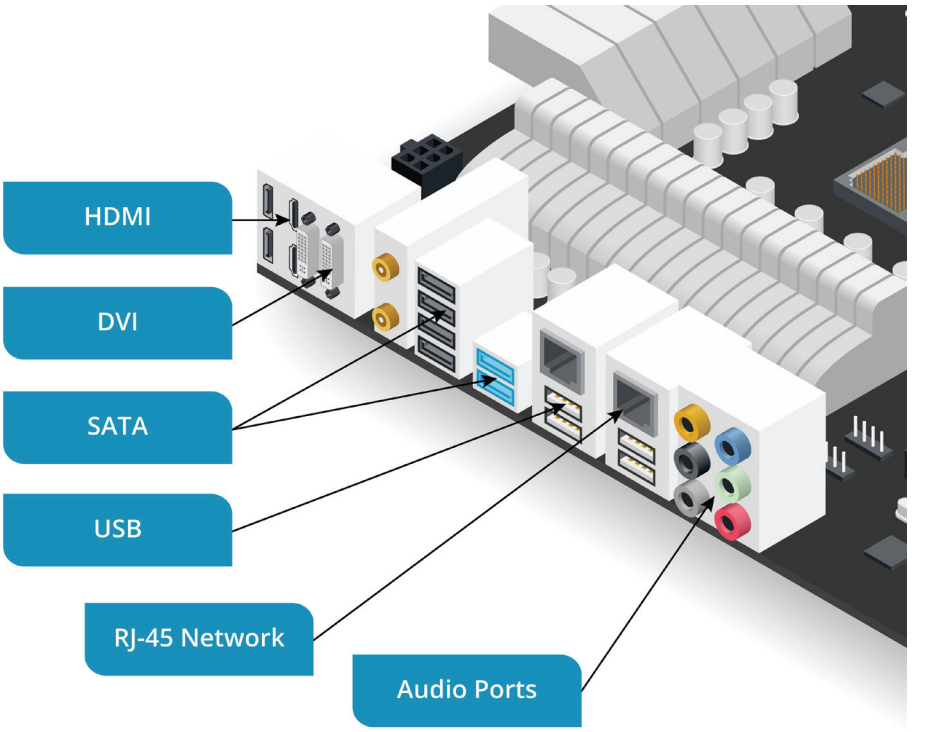
Features on the rear panel of a typical PC case. (Image © 123RF.com)

Below the PSU, there is a cutout aligned with the motherboard's input/output (I/O) ports. These allow for the connection of peripheral devices.

At the bottom of the rear panel there are cutout slots aligned with the position of adapter card slots to allow cables to be connected to any I/O ports on the cards. These slots should either be covered by an adapter card or a metal strip known as a blanking plate. Uncovered slots can disrupt the proper flow of air around components in the PC and cause overheating and increase the amount of dust in the system.

Peripheral Devices

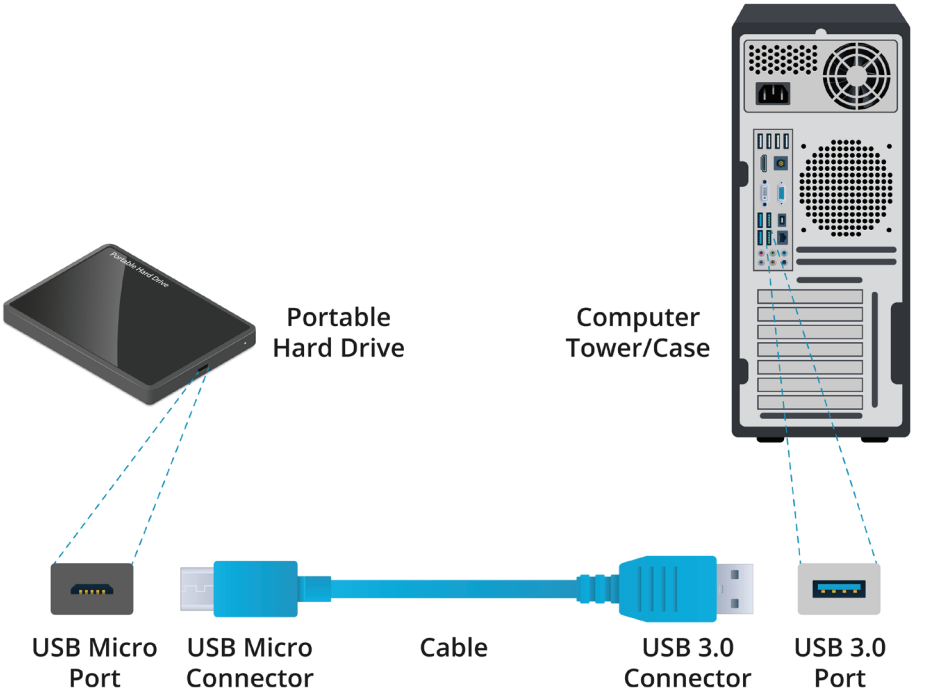
An input/output (I/O) port allows a device to be connected to the PC via a **peripheral cable**. Some ports are designed for a particular type of device, such as a graphics port to connect a monitor. Other ports support a variety of device types. External ports are positioned at the rear or front of the PC through cutouts in the case. They can be provided on the motherboard or as an expansion card.



I/O ports on a motherboard. (Image © 123RF.com)

Interfaces, Ports, and Connectors

A hardware port is the external connection point for a particular type of bus interface. A bus allows the transfer of data to and from devices. The connector is the part of a peripheral cable that can be inserted into a port with the same shape or form factor. Each bus interface type might use multiple connector form factors. Most connectors and ports now use edge contacts and either have an asymmetric design called *keying* to prevent them from being inserted the wrong way around or are reversible.



A peripheral cable for the Universal Serial Bus (USB) interface with different connector types being used to connect a portable hard drive and a desktop computer. (Image © 123RF.com)

Binary Data Storage and Transfer Units

When comparing bus interfaces, it is important to use appropriate units. Computers process binary data. Each binary digit or bit (b) can have the value one or zero. Storage is often measured in multiples of eight bits, referred to as a byte (B). A lowercase "b" unit refers to a bit, while uppercase means a byte.

Transfer rates are expressed in units per second of the following multiples of bits and bytes:

- 1000—Kilobits (Kb/s or Kbps) and kilobytes (KB/s and KBps).
- 1000x1000—Megabits (Mb/s) or megabytes (MB/s).
- 1000x1000x1000—Gigabits (Gb/s) and gigabytes (GB/s).

Universal Serial Bus Cables

The Universal Serial Bus (USB) is the standard means of connecting most types of peripheral device to a computer. USB peripheral device functions are divided into classes, such as human interface (keyboards and mice), mass storage (disk drives), printer, audio device, and so on.

A USB is managed by a host controller. Each host controller supports multiple ports attached to the same bus. In theory, there could be up to 127 connected devices per controller, but to overcome the limitations of sharing bandwidth, most PC motherboards provision multiple USB controllers, each of which has three or four ports.

USB port symbol. Variations on this basic icon identify supported features, such as higher transfer rates and power delivery. Wikimedia Commons (commons.wikimedia.org/wiki/File:USB_icon.png)

USB Standards

There have been several iterations of the USB standard. Each version introduces better data rates. A version update may also define new connector form factors and other improvements. The **USB 2.0** HighSpeed standard specifies a data rate of 480 Mbps shared between all devices attached to the same host controller. The bus is half-duplex, meaning that each device can send or receive, but not at the same time.

Iterations of USB 3.x introduced new connector form factors and upgraded transfer rates, each of which are full-duplex, so a device can send and receive simultaneously. USB 3.2 deprecated some of the older terms used to describe the supported transfer rate:

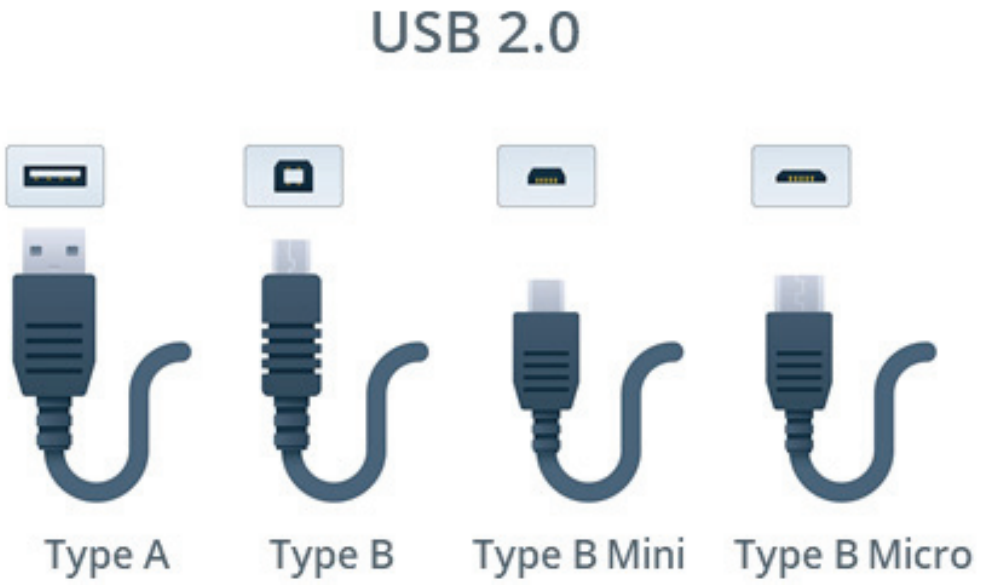
Standard	Speed	Connectors	Legacy Designation
USB 3.2 Gen 1 SuperSpeed USB	5 Gbps	USB-A, USB-C, USB Micro	USB 3.0
USB 3.2 Gen 2x1 SuperSpeed USB 10 Gbps	10 Gbps	USB-A, USB-C, USB Micro	USB 3.1 SuperSpeed+
USB 3.2 Gen 2x2 SuperSpeed USB 20 Gbps	2 x 10 Gbps	USB-C	

USB 3 controllers feature two sub-controllers. One controller handles SuperSpeed-capable devices, while the other supports legacy HighSpeed, FullSpeed, and LowSpeed USB v1.1 and v2.0 devices. Consequently, legacy devices will not slow down SuperSpeed-capable devices.

USB Connector Types

The connector form factors specified in USB 2 are as follows:

- Type A—For connection to the host and some types of peripheral device. The connector and port are shaped like flat rectangles. The connector should be inserted with the USB symbol facing up.
- Type B—For connection to large devices such as printers. The connector and port are square, with a beveled top.
- Type B **Mini**—A smaller peripheral device connector. This type of connector was seen on early digital cameras but is no longer widely used.
- Type B **Micro**—An updated connector for smaller devices, such as smartphones and tablets. The micro connector is distinctively flatter than the older mini type of connector.



USB 2 ports and connectors. (Image © 123RF.com)

A USB cable can feature Type A to Type A connectors or can convert from one type to another (Type A to Type B or Type A to Micro Type B, for instance).

In USB 3, there are new versions of the Type A, Type B, and Type B Micro connectors with additional signaling pins and wires. USB 3 receptacles and connectors often have a blue connector tab or housing to distinguish them. USB 3 Type A connections are physically compatible with USB 1.1 and 2.0 connections, but the Type B/Type B Micro connections are not. So, for example, you could plug a USB 2 Type A cable into a USB 3 Type A port, but you could not plug a USB 3 Type B cable into a USB 2 Type B port.

USB 3 connectors and ports (from left to right): Type A, Type B, Micro Type B, Type C. (Image ©123RF.com)

USB 3.1 defines the USB-C connector type. This compact form factor is intended to provide a single, consistent hardware interface for the standard. The connector is reversible, meaning it can be inserted either way up. The connector design is also more robust than the earlier miniB and microB types. USB-C can use the same type of connector at both ends, or you can obtain USB-C to USB Type A or Type B converter cables.

Cable Length

The maximum cable length for LowSpeed devices is 3 m, while for FullSpeed and HighSpeed the limit is 5 m. Vendors may provide longer cables, however. Although SuperSpeed-capable cables do not have an official maximum length, up to about 3 m is recommended.

Power

As well as a data signal, the bus can supply power to the connected device. Most USB Type A and Type C ports can be used to charge the battery in a connected device.

Basic USB ports can supply up to about 4.5 watts, depending on the version. A power delivery (PD)–capable port can supply up to 100 watts, given suitable connectors and cabling.

HDMI and DisplayPort Video Cables

The USB interface supports many types of devices, but it has not traditionally been used for video. As video has high bandwidth demands, it is typically provisioned over a dedicated interface.

Video cable bandwidth is determined by two main factors:

- The resolution of the image, measured in horizontal pixels by vertical pixels. For example, 1920x1200 is the typical format of high-definition (HD) video and 3840x2160 is typical of 4K video.
- The speed at which the image is redrawn, measured in hertz (Hz) or frames per second (fps).

As examples, uncompressed HD video at 60 fps requires 4.5 Gbps, while 4K at 60 fps requires 8.91 Gbps.

The frame rate in fps is used to describe the video source, while hertz is the refresh rate of the display device and video interface. To avoid display artefacts such as ghosting and tearing, the refresh rate should match the frame rate or be evenly divisible by it. For example, if the frame rate is 60 fps and the refresh rate is 120 Hz, the video should play smoothly.

Computer displays are typically of the liquid crystal display (LCD) thin film transistor (TFT) type. Each pixel in a color LCD comprises cells with filters to generate the three additive primary colors red, green, and blue (RGB). Each pixel is addressed by a transistor to vary the intensity of each cell, therefore creating the gamut (range of colors) that the display can generate. The panel is illuminated by a light-emitting diode (LED) array or backlight.

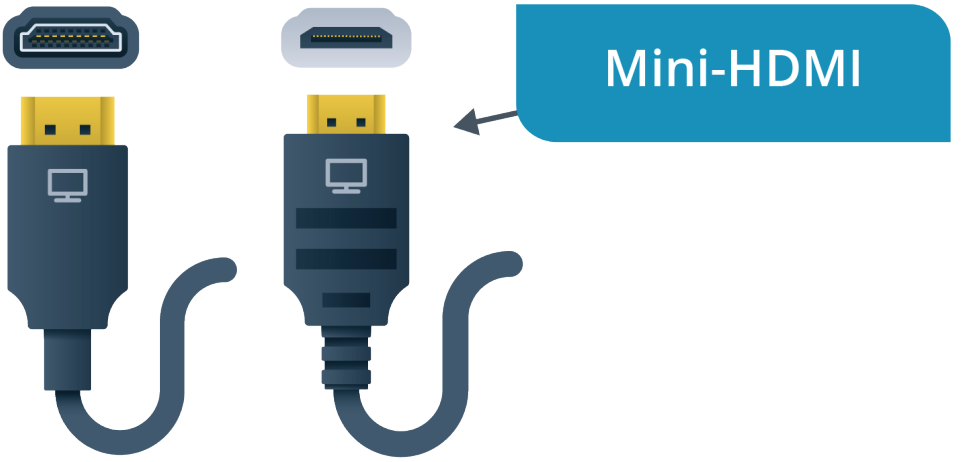
An LCD/TFT is often just referred to as a flat-panel display. They are also called LED displays after the backlight technology (older flat panels use fluorescent tube backlights). Premium flat-panel monitors are of the organic LED (OLED) type. This means that each pixel is its own light source. This allows for much better contrast and color fidelity.

High-Definition Multimedia Interface

The **High-Definition Multimedia Interface (HDMI)** is the most widely used video interface. It is ubiquitous on consumer electronics, such as televisions, games consoles, and Blu-ray players as well as on monitors designed for use with PCs. HDMI supports both video and audio, plus remote control and digital content protection (HDCP). Updates to the original HDMI specification have introduced support for high resolutions, such as 4K and 8K, and gaming features, such as the ability to vary the monitor refresh rate to match the frame rate of the video source.

Support for audio is useful because most TVs and monitors have built-in speakers. The video card must have an audio chipset for this to work, however.

There are full-size (Type A), mini (Type C), and micro (Type D) connectors, all of which are beveled to ensure correct orientation.



HDMI connector and port on the left and mini-HDMI connector and port on the right. (Image ©123RF.com)

HDMI cable is rated as either Standard (Category 1) or High Speed (Category 2). High Speed cable supports greater lengths and is required for v1.4 features, such as 4K and refresh rates over 60 Hz. HDMI versions 2.0 and 2.1 specify Premium High Speed (up to 18 Gbps) and Ultra High Speed (up to 48 Gbps) cable ratings.

DisplayPort Interface

HDMI was developed by consumer electronics companies and requires a royalty to use. **DisplayPort** was developed as a royalty-free standard by the Video Electronics Standards Association (VESA), which is an organization that represents PC graphics adapter and display technology companies. DisplayPort supports similar features to HDMI, such as 4K, audio, and content protection. There are full-size DP++ and MiniDP/mDP port and connector types, which are keyed against incorrect orientation.

A DP++ DisplayPort port and connector. (Image ©123RF.com)

Bandwidth can be allocated in bonded lanes (up to four). The bitrate of each lane was originally 2.7 Gbps but is now (with version 2.0) up to 20 Gbps.

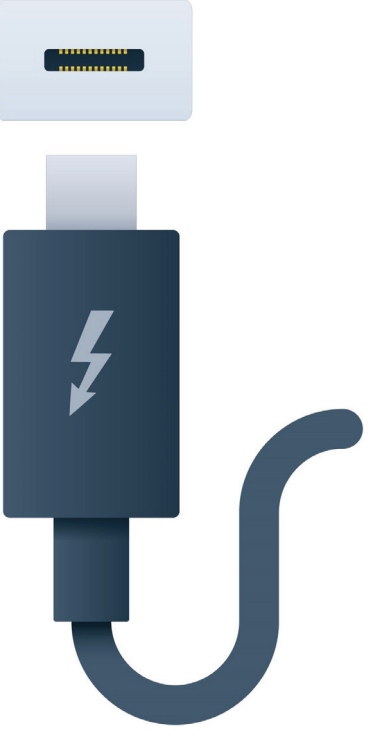
One of the main advantages of DisplayPort over HDMI is support for daisy-chaining multiple monitors to the same video source. Using multiple monitors with HDMI requires one video card port for each monitor.

Thunderbolt and Lightning Cables

Although the Thunderbolt and Lightning interfaces are most closely associated with Apple computers and mobile devices, Thunderbolt is increasingly implemented on Windows and Linux PCs too.

Thunderbolt Interface

Thunderbolt can be used as a display interface like DisplayPort or HDMI and as a general peripheral interface like USB. Thunderbolt versions 1 and 2 use the same physical interface as MiniDP and are compatible with DisplayPort so that a monitor with a DisplayPort port can be connected to a computer via a Thunderbolt port and a suitable adapter cable. Thunderbolt ports are distinguished from MiniDP by a lightning bolt/flash icon. Version 2 of the standard supports links of up to 20 Gbps. Like DisplayPort multiple monitors can be connected to a single port by daisy-chaining.



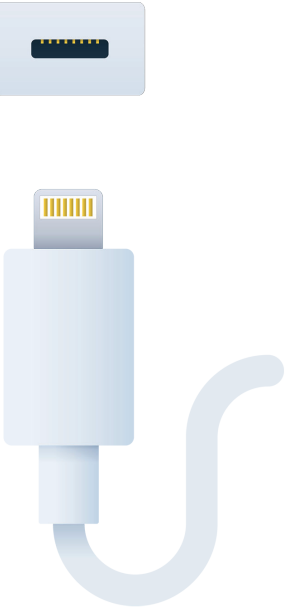
The USB-C form factor adopted for Thunderbolt 3. (Image © 123RF.com)

Thunderbolt version 3 changes the physical interface to use the same port, connector, and cabling as USB-C. Converter cables are available to connect Thunderbolt 1 or 2 devices to Thunderbolt 3 ports. A USB device plugged into a Thunderbolt 3 port will function normally, but Thunderbolt devices will not work if connected to a USB port that is not Thunderbolt-enabled. Thunderbolt 3 supports up to 40 Gbps over a short, high-quality cable (up to 0.5 m/1.6 ft.).

Not all USB-C ports support Thunderbolt 3. Look for the flash icon on the port or confirm using the system documentation. At the time of writing, converged USB 4 and Thunderbolt 4 standards have been developed, and products are starting to appear on the market.

Lightning Interface

Apple's iPhone and iPad mobile devices use a proprietary **Lightning** port and connector. The Lightning connector is reversible.



Apple Lightning connector and port. (Image ©123RF.com)

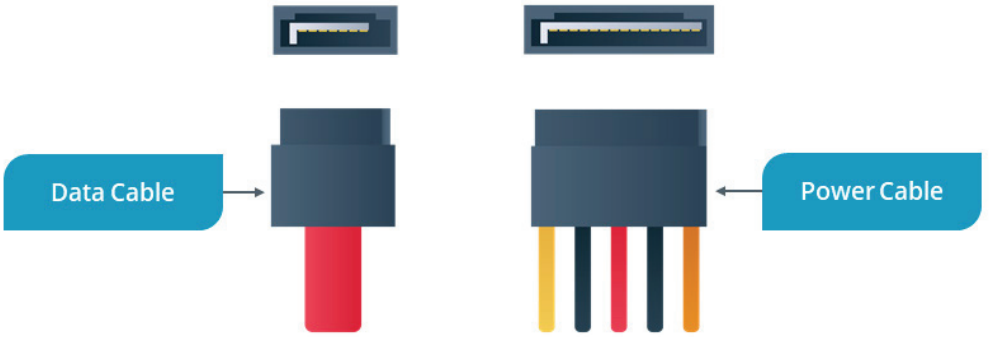
The Lightning port is found only on Apple's mobile devices. To connect such a device to a PC, you need a suitable adapter cable, such as Lightning-to-USB A or Lightning-to-USB C.

SATA Hard Drive Cables

As well as external cabling for peripheral devices, some types of internal components use cabling to attach to a motherboard port.

Serial Advanced Technology Attachment Interface

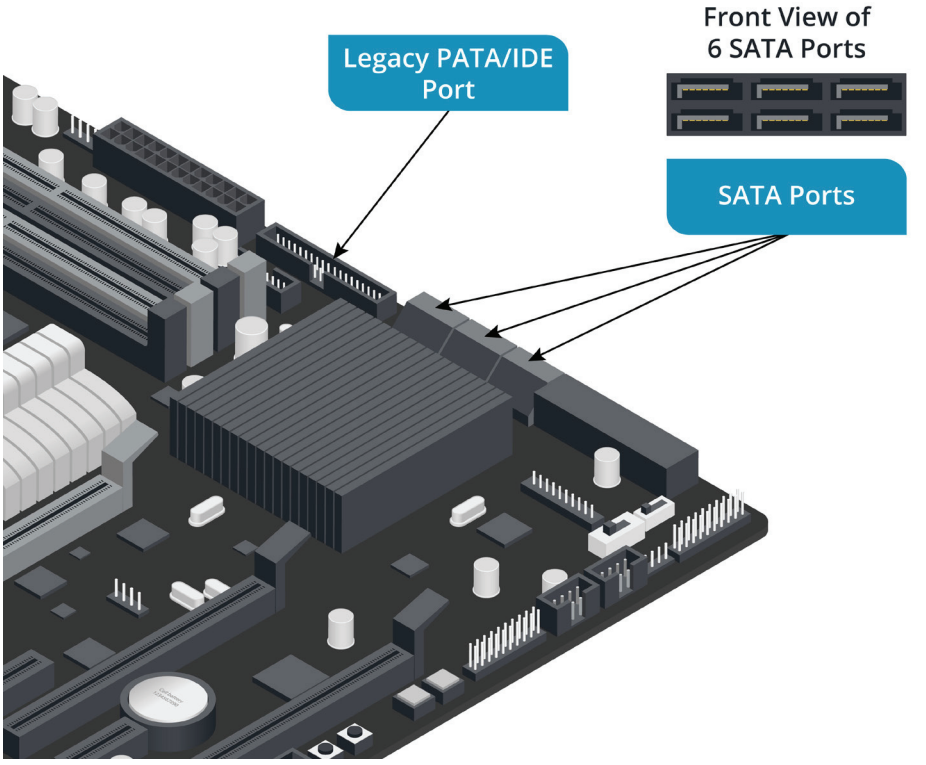
Serial Advanced Technology Attachment (SATA) is the standard means of connecting internal storage drives within a desktop PC. SATA uses cables of up to 1 m (39 in.) terminated with compact 7-pin connectors. Each SATA host adapter port supports a single device.



SATA connectors and ports (from left to right): SATA data, SATA power (with 3.3V orange wire). (Image ©123RF.com)

The 7-pin data connector does not supply power. A separate 15-pin SATA power connector is used to connect the device to the PC's power supply.

The first commercially available SATA standard supported speeds of up to 150 MBps. This standard was quickly augmented by SATA revision 2 (300 MBps) and then SATA revision 3 (600 MBps).



Motherboard SATA and legacy PATA/IDE ports. (Image ©123RF.com)

Molex Power Connectors

Internal storage device data cables are unpowered. While the SATA power connector is the best option for new devices, legacy components connect to the power supply unit (PSU) via a **Molex connector**. A Molex connector is usually white or clear plastic and has 4 pins. The color coding of the wire insulation represents the DC voltage: red (5 VDC), yellow (12 VDC), and black (ground).

A Molex connector. (Image © 123RF.com)

Some devices might have both SATA and Molex power connectors.

External SATA

There is also an **external SATA (eSATA)** standard for the attachment of peripheral drives, with a 2 m (78 in.) cable. You must use an eSATA cable to connect to an external eSATA port; you cannot use an internal SATA cable. eSATAp is a nonstandard powered port used by some vendors that is compatible with both USB and SATA (with an eSATAp cable). The USB interface dominates the external drive market, however.

Review Activity:

Cable Types and Connectors

Answer the following questions:

1. **A technician has removed an adapter card from a PC. Should the technician obtain and install a blanking plate to complete the service operation?**

2. **You are labelling spare parts for inventory. What type of USB connector is shown in the exhibit?**

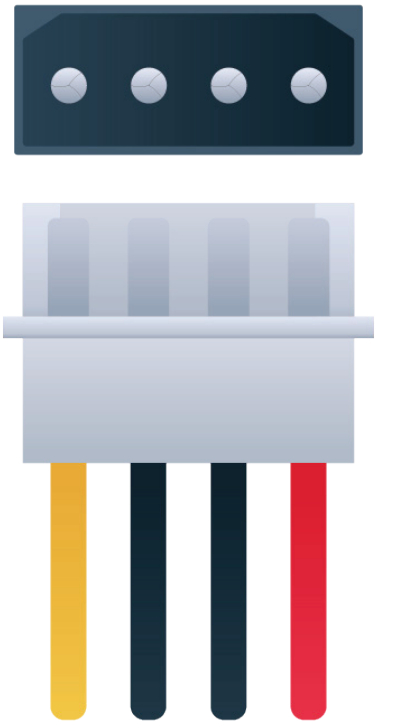
(Image ©123RF.com)

3. **What is the nominal data rate of a USB port supporting Gen 3.2 2x1?**

4. **True or false? USB-C ports and connectors are compatible with Apple Lightning connectors and ports.**

5. **A technician connects a single port on a graphics card to two monitors using two cables. What type of interface is being used?**

6. A technician is completing a storage upgrade on an older computer. Examining the power supply, the technician notices that only two of the five plugs of the type shown in the exhibit are connected to devices. What is the purpose of these plugs, and can some be left unconnected?



(Image ©123RF.com)

Topic 1B

Install and Configure Motherboards

CORE 1 EXAM OBJECTIVES COVERED

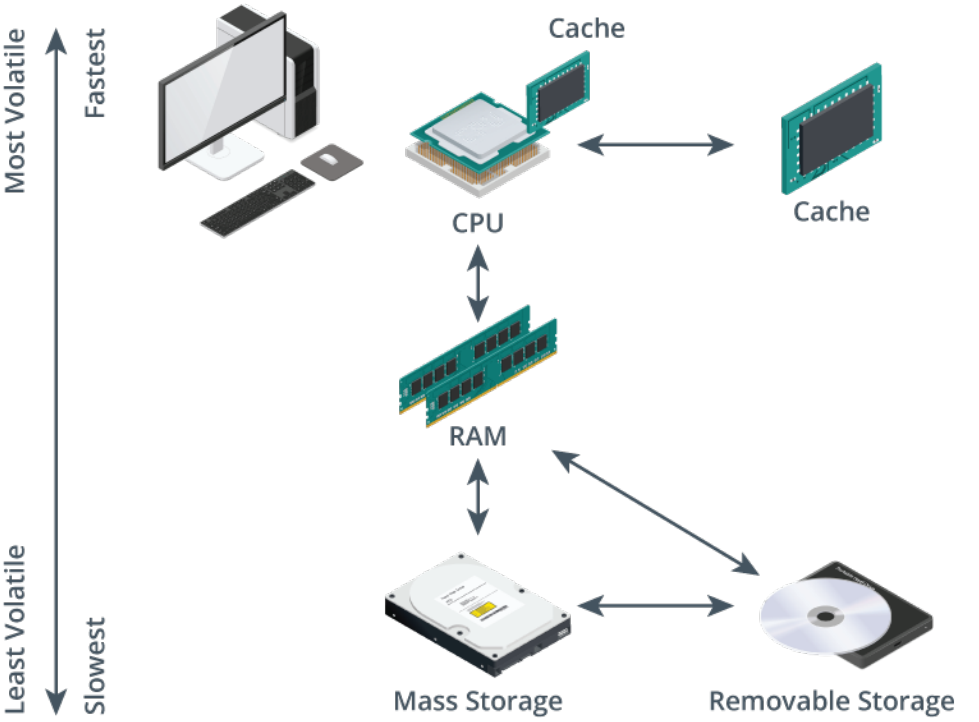
3.4 Given a scenario, install and configure motherboards, central processing units (CPUs), and add-on cards.

The motherboard houses sockets for the devices that implement the core system functions of a personal computer: compute, storage, and networking. Knowledge of motherboard types and capabilities plus the different connector types will enable you to perform component upgrades and repairs efficiently.

Motherboard Functions

All computer software and data are processed by using the ones and zeroes of binary code. Software works by running instructions in the central processing unit (CPU). This can be referred to as the compute or processing function of a PC.

Instructions and data also require storage. The CPU can only store a limited number of instructions internally at any one time. Additional storage for running programs and open data files is provided through system memory. This random-access memory (RAM) storage technology is nonpersistent. *Nonpersistent* means that the RAM devices can only hold data when the PC is powered on. Mass storage devices are used to preserve data when the computer is turned off.



CPU, cache, and RAM are fast but volatile. Mass storage and removable storage devices provide slower but permanent data retrieval. (Image ©123RF.com)

These processing and storage components are connected by bus interfaces implemented on the motherboard. The instructions and data are stored using transistors and capacitors and transmitted between components over the bus using electrical signals.

The motherboard's system clock synchronizes the operation of all parts of the PC and provides the basic timing signal for the CPU. Clock speeds are measured in megahertz (MHz) or gigahertz (GHz). Clock multipliers take the timing signal produced by the generator and apply a multiplication factor to produce different timing signals for different types of buses. This means that one type of bus can work at a different speed (or frequency) to another type of bus.

The type of motherboard influences system speed and the range of system devices and adapter cards that can be installed or upgraded. There are many motherboard manufacturers, including AOpen (Acer), ASRock, ASUSTek, Biostar, EVGA Corporation, Gigabyte, Intel, and MSI. Each motherboard is designed to support a particular range of CPUs. PC CPUs are principally manufactured by Intel and Advanced Micro Devices (AMD).

Electrical Safety and ESD

When you open the case to perform upgrades or troubleshooting, you must follow proper operational procedures to ensure your safety and minimize the risk of damaging components.

Electrical Safety

When working with a PC, you must ensure your own safety. This means that the PC must be disconnected from the power supply before opening the case. Additionally, hold the power button for a few seconds after disconnecting the power cord to ensure that all internal components are drained of charge. Do not attempt to disassemble components that are not field repairable, such as the power supply.

Electrostatic Discharge

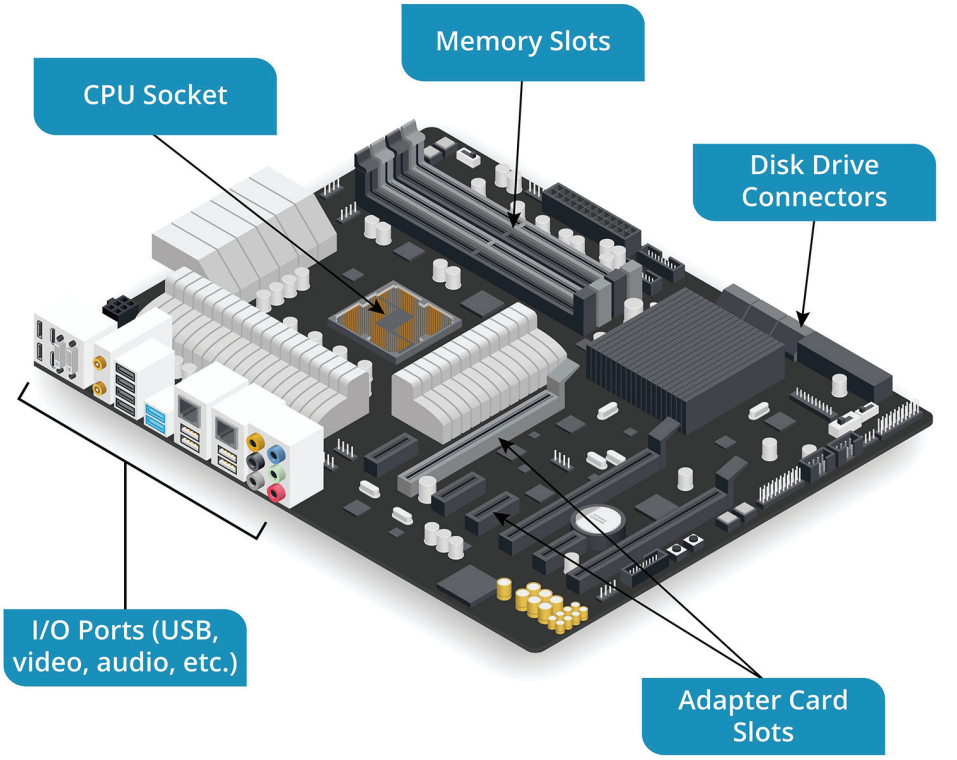
You need to use tools and procedures that minimize the risk of damage to the sensitive electronic components used inside the PC. Components such as the CPU, system RAM, adapter cards, and the motherboard itself are vulnerable to electrostatic discharge (ESD). This is where a static charge stored on your clothes or body is suddenly released into a circuit by touching it. Handle components by their edges or plastic parts, and ideally, use an anti-ESD wrist strap and other protective equipment and procedures.

ESD wrist strap on ESD mat. (Image by Audrius Merfeldas © 123RF.com)

Operational procedures covering personal safety and the use of anti-ESD equipment are covered in more detail in the Core 2 course.

Motherboard CPU and System Memory Connectors

All motherboards have a variety of **connector types** and socket types for the system devices: CPU, memory, fixed disk drives, and adapter cards.



Motherboard connectors. (Image © 123RF.com)

CPU Sockets

New motherboards are generally released to support the latest CPU models. Most PC CPUs are manufactured by Intel and AMD, and these vendors use different socket designs. Because CPU technology changes rapidly, a given motherboard will only support a limited number of processor models.

The CPU socket has a distinctive square shape. When the CPU has been installed, it is covered by a heat sink and fan.

The function of the CPU is supported by the motherboard's chipset. This consists of controllers that handle the transfer of data between the CPU and various devices. The chipset is soldered onto the motherboard and cannot be upgraded. The type of chipset on the motherboard determines the choice of processor; the type and maximum amount of RAM; and support for integrated interfaces/ports, such as video, sound, and networking. Interfaces that are not supported by the chipset can be installed or upgraded as an adapter card.

System Memory Slots

System memory uses a type of memory technology called random-access memory (RAM). Program code is loaded into RAM so that it can be accessed and executed by the processor. RAM also holds data, such as the contents of a spreadsheet or document, while it is being modified. System RAM is volatile; it loses its contents when power is removed.

System RAM is normally packaged as a dual inline memory module (DIMM) fitted to a motherboard slot. A DIMM slot has catches at either end, is located close to the CPU socket, and is numbered and often color-coded. There are successive generations of RAM technologies, such as DDR3, DDR4, and DDR5. A DIMM form factor is specific to a particular DDR version. A label next to the slots should identify the type of DIMMs supported.

The capabilities of the memory controller and number of physical slots determine how much memory can be fitted.

Motherboard Storage Connectors

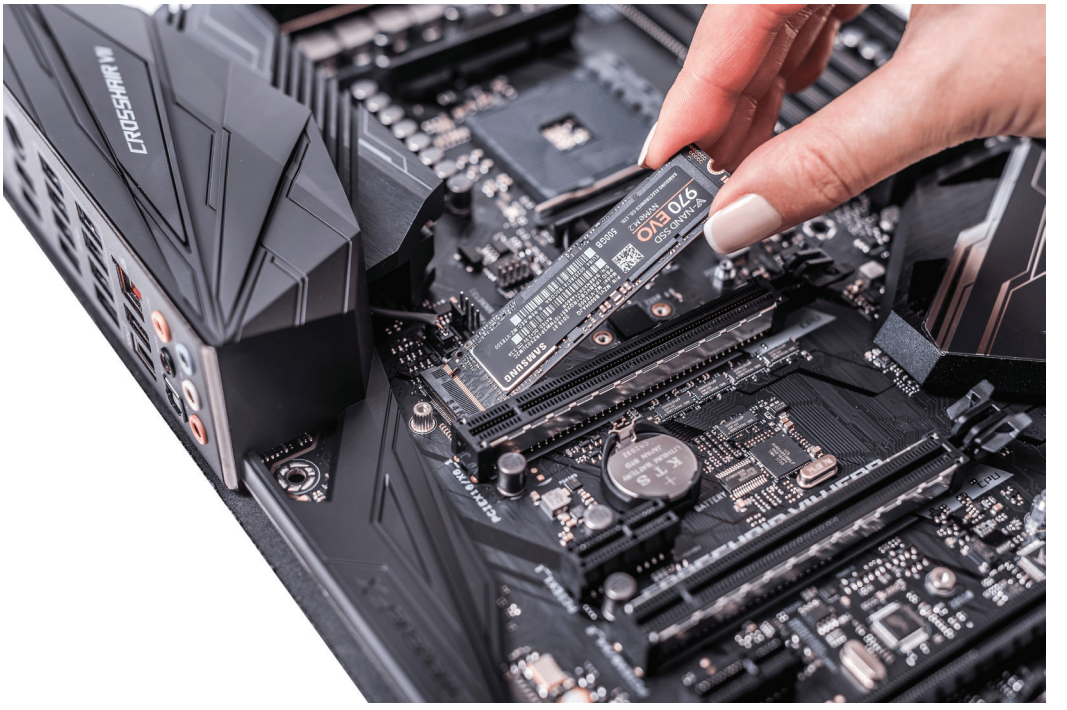
One or more fixed disks installed inside the PC case provide persistent storage for the operating system, software programs, and data files. Fixed disks use either solid state drive (SSD) or hard disk drive (HDD) technology.

Serial Advanced Technology Attachment Interface

The motherboard will contain several Serial Advanced Technology Attachment (SATA) ports to connect one or more fixed drives. SATA can also be used to connect removable drives, such as tape drives and optical drives (DVD/Blu-ray). SATA devices are installed to a drive bay in the chassis and then connected to a data port via a cable and to the power supply via a SATA power or Molex connector.

M.2 Interface

An SSD can be provisioned in an adapter card form factor. These often use an M.2 interface. An M.2 port is oriented horizontally. The adapter card is inserted at an angle and then pushed into place and secured with a screw. M.2 adapters can be different lengths (42 mm, 60 mm, 80 mm, or 110 mm), so you should check that any given adapter will fit on your motherboard. Labels indicate the adapter sizes supported. M.2 supplies power over the bus, so there is no need for a separate power cable.



M.2 form factor SSD being inserted into a motherboard connector. (Image ©123RF.com)

External SATA Interface

There is also an **external SATA (eSATA)** standard for the attachment of external drives, with a 2 m (78 in.) cable. You must use an eSATA cable to connect to an external eSATA port; you cannot use an internal SATA cable. eSATAp is a nonstandard powered port used by some vendors that is compatible with both USB and SATA (with an eSATAp cable).

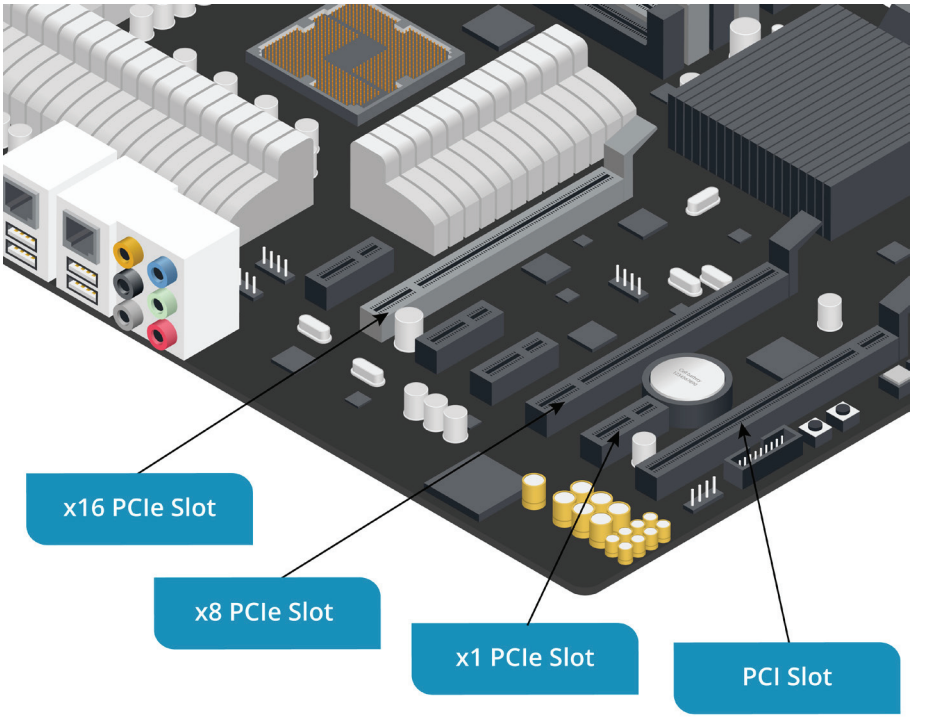
The main drawback of eSATA compared to USB or Thunderbolt external drives is that power is not supplied over the cable. This is not so much of an issue for 3.5-inch drives, which require a separate power supply, but it limits the usefulness of eSATA for 2.5-inch portable drives.

Motherboard Adapter Connectors

Expansion slots accept plug-in adapter cards to extend the range of functions the computer can perform. There are two main types of expansion slot interface.

Peripheral Component Interconnect Express Interface

The **Peripheral Component Interconnect Express (PCIe)** bus is the mainstream interface for modern adapter cards. It uses point-to-point serial communications, meaning that each component can have a dedicated link to any other component.



Motherboard PCI and PCI Express expansion slots. (Image ©123RF.com)

Each point-to-point connection is referred to as a link. Each link can make use of one or more lanes. The raw transfer rate of each lane depends on the PCIe version supported. Transfer rates are measured in gigatransfers per second (GT/s). Throughput in GB/s is the rate achieved after loss through encoding is accounted for.

Version	GT/s	GB/s for x1	GB/s for x16
2	5	0.5	8
3	8	0.985	15.754
4	16	1.969	31.508
5	32	3.938	63.015

Adapter slots with more lanes are physically longer. Each PCIe adapter card supports a specific number of lanes, typically x1, x4, x8, or x16. Ideally, the card should be plugged into a port that supports the same number of lanes. However, if insufficient slots are available, a card will fit in any port with an equal or greater number of lanes. This is referred to as up-plugging. For example, a x8 card will fit in a x8 or x16 socket. The card should work at x8 but in some circumstances may only work at x1.

It may also be possible to fit a longer card into a shorter slot, referred to as down-plugging, so long as the card is not obstructed by other features in the case.

A slot may support a lower number of lanes than its physical size suggests. The number of lanes supported by each slot is indicated by a label on the motherboard. For example, a slot that is physically x16 but supports only x8 operation will be labelled x16/x8 or x16 @ x8.

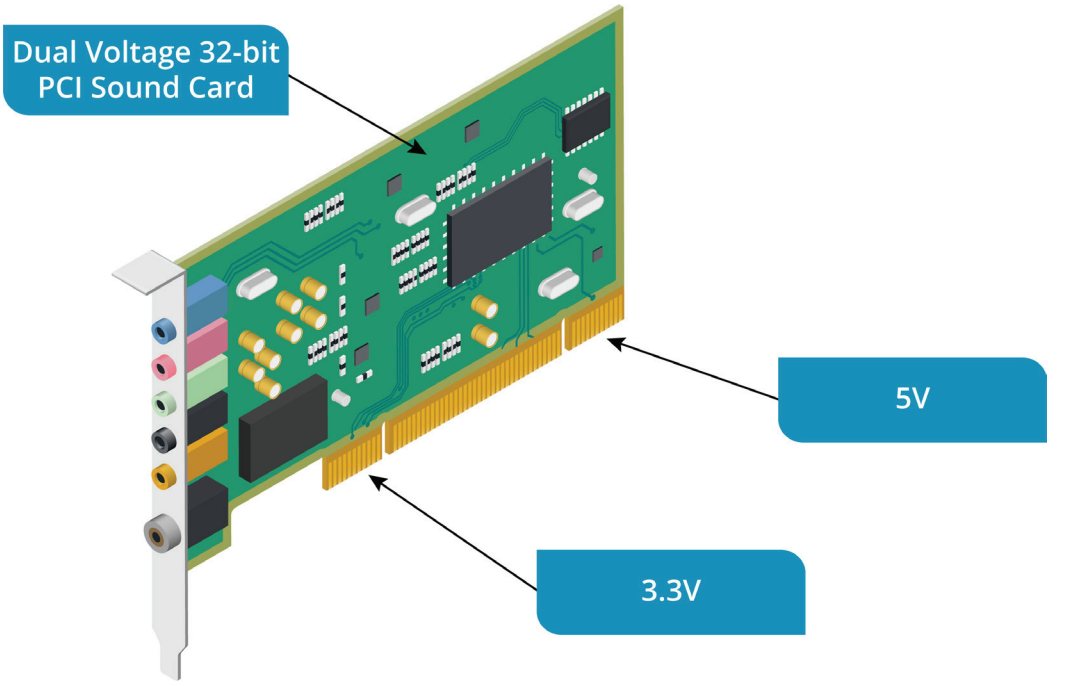
All PCIe versions are backwards-compatible. For example, you can connect a PCIe version 2 adapter to a version 4 motherboard or install a version 3 adapter into a version 2 motherboard. The bus works at the speed of the lowest version component.

PCIe can supply up to 75W to a graphics card via a dedicated graphics adapter slot and up to 25W over other slots. An extra 75W power can be supplied via a PCIe power connector.

Peripheral Component Interconnect Interface

Computers can support more than one expansion bus, often to support older technologies. **Peripheral Component Interconnect (PCI)** is a legacy bus type, having been superseded by PCI Express. PCIe is software compatible with PCI, meaning that PCI ports can be included on a PCIe motherboard to support legacy adapter cards, but PCI cards cannot be fitted into PCIe slots.

As with many legacy technologies, PCI uses parallel communications. Most types of PCI are 32-bit and work at 33.3 MHz, achieving a transfer rate of up to 133 MBps (that is, 32 bits divided by 8 to get 4 bytes, then multiplied by the clock rate of 33.3). The earliest PCI cards were designed for 5V signaling, but 3.3V and dual voltage cards became more prevalent. To prevent an incompatible PCI card from being inserted into a motherboard slot (for example, a 3.3V card in a 5V PCI slot), the keying for the three types of cards is different.



32-bit PCI sound card with dual voltage. (Image ©123RF.com)

Motherboard Form Factors

The **motherboard form factor** describes its shape, layout, and the type of case and power supply that can be used, plus the number of adapter cards that can be installed.

Advanced Technology eXtended Form Factor

The **Advanced Technology Extended (ATX)** specification is the standard form factor for most desktop PC motherboards and cases. Full-size ATX boards are 12 inches wide by 9.6 inches deep (or 305 mm x 244 mm). An ATX board can contain up to seven expansion slots.

The Micro-ATX (mATX) standard specifies a 9.6-inch (244 mm x 244 mm) square board. mATX boards can have a maximum of four expansion slots.

Most mATX boards can be mounted in ATX cases.

Information Technology eXtended Form Factor

Small form factor (SFF) PCs are popular as home machines and for use as mini servers. SFF PCs often use Via's Mini-ITX (**Information Technology Extended**) form factor.

Mini-ITX is 6.7 inches (170 mm x 170 mm) square with one expansion slot. These are designed for small cases, but do note that most mini-ITX boards can be mounted in ATX cases. There are also smaller nano-, pico-, and mobile-ITX form factors, but these are used for embedded systems and portables, rather than PCs.

No commercial motherboards were ever produced from the original plain ITX specification.

Motherboard Installation

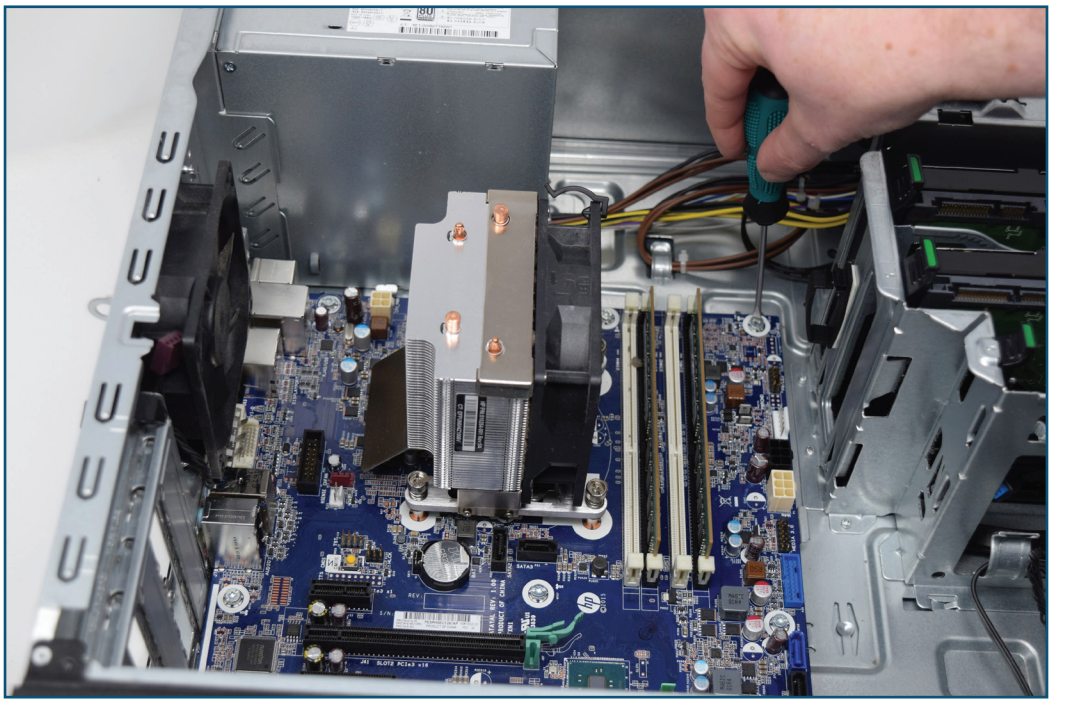
The motherboard is attached to the case by using standoffs. These hold the motherboard firmly and ensure no other part of it touches the case. The standoffs are positioned in holes that line up in the same position in the case and the motherboard if they use compatible form factors

The general procedure for installing a motherboard is as follows:

1. Use the motherboard documentation to familiarize yourself with the specific installation procedure. Check whether any jumper clips need to be adjusted. A jumper is placed over header pins in a particular orientation. For example, there might be a jumper that enables recovery mode.

The motherboard is vulnerable to electrostatic discharge (ESD). Always take anti-ESD precautions when handling and storing these devices.

2. Orient the board to the oblong I/O cutout at the rear of the case. Prepare the motherboard I/O blanking plate in the correct orientation by removing caps so that USB, audio, and video ports will be uncovered when the board is fitted. Fit the blanking plate to the case by snapping it into the cutout.
3. Insert standoffs into the case to match the hole locations on the motherboard. Standoffs are usually threaded, though older cases might use push-down pegs. There might be a guide standoff attached to the case or all standoffs might come preinstalled. Make sure that corners, long edges, and the center of the board will be supported. Do not add standoffs where there is no corresponding hole in the motherboard.
4. Optionally, add the CPU and memory modules to the motherboard before installing the board in the case.
5. Check the alignment and standoff location again and verify that each standoff is secure. If everything is correct, place the motherboard on the standoffs.



Align the board with the I/O cutout (top left) and ensure that it is supported by standoffs at the edges and in the center. (Image courtesy of CompTIA.)

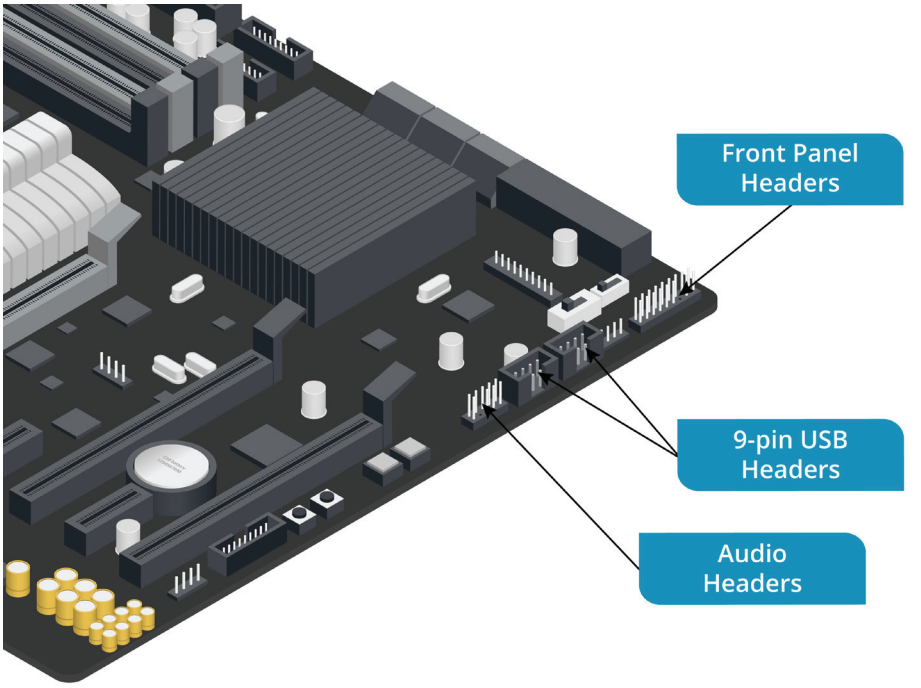
6. Secure each standoff using the appropriate screw type. Make sure that the board is firm and stable, but do not overtighten the screws or you risk cracking the board.

7. To complete PC installation, add the power and disk devices to the case, install any addon adapter cards to the motherboard, and install the data and power connectors.

Selection and installation of power, disk, system memory, and CPU devices are covered in detail in the next lesson.

Motherboard Headers and Power Connectors

In addition to slots and sockets for system devices, motherboards also include connectors for components such as case buttons, speakers, and fans.



Motherboard front panel, USB, and audio headers. (Image ©123RF.com)

Headers

Components on the front and rear panels of the case connect to **headers** on the motherboard:

- **Power button (soft power)**—Sends a signal that can be interpreted by the OS as a command to shut down rather than switching the PC off. Holding down the power button for a few seconds will cut the power, however.
- **Drive (HDD) activity lights**—Show when an internal hard disk is being accessed.
- **Audio ports**—Allow speakers and/or headphones and a microphone to be connected to the computer.
- **USB ports**—Internal USB 2 connections are made via 9-pin headers, which accept up to two 4-pin port connections (the 9th pin is to orient the cable correctly). USB 3 headers use a 2x10 format and can be cabled to two ports.

When disassembling the system, you should make a diagram of the position and orientation of header connectors. If you do not have a diagram, you will have to refer to the motherboard documentation or go by any labels printed on the wires and headers. These are not always very easy to follow, however.

Power Connectors

The motherboard also contains various connection points for the power supply and fans.

- The main P1 motherboard **power connector** is a distinctive 2-pin x 12-pin block with square pin receptacles.
- Fan connectors are 3- or 4-pin Molex KK format. There will be one for the CPU and one or more for the case fans and components such as memory and video adapters. 4-pin fan connectors support precise fan-speed control via a pulse width modulation (PWM) signal carried by the blue wire. 3-pin fans are controlled by varying the voltage.

Fans with a 3-pin connector can usually be used with 4-pin headers, but the system may not be able to vary the fan speed (or may need special configuration to be able to do so). A fan with a 4-pin connector will usually work with a 3-pin header but will not be able to use PWM.

Video Cards and Capture Cards

An **expansion card** adds functions or ports that are not supported by the integrated features of the motherboard. An expansion card can be fitted to an appropriate PCIe or PCI slot. Some of the main types of expansion card are sound, video, capture, and network.

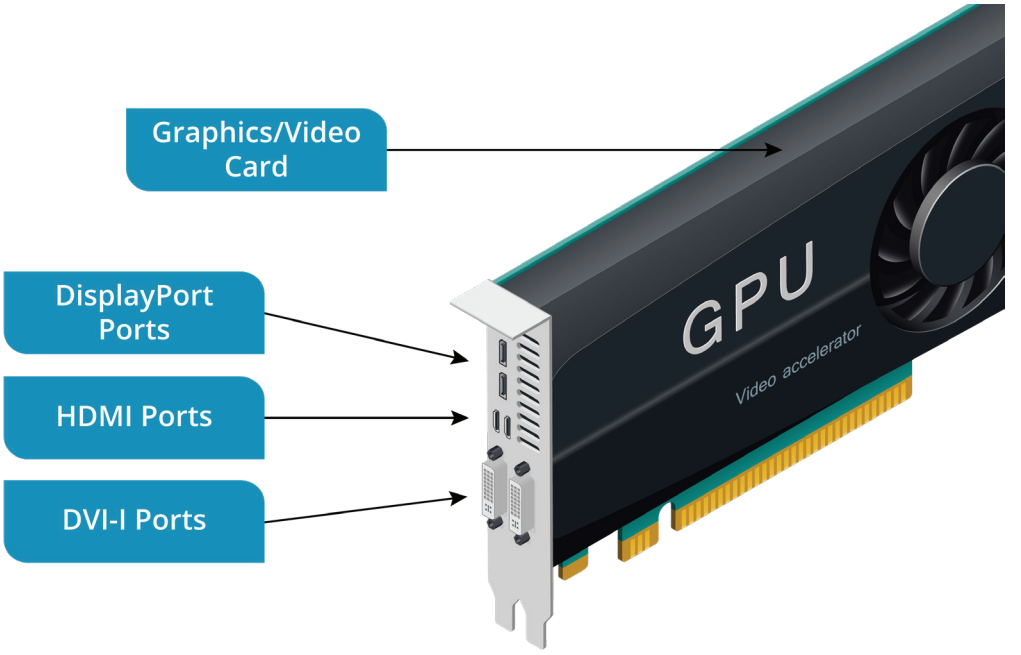
Video Cards

The **video card** (or graphics adapter) generates the signal to drive a monitor or projector. Low-end graphics adapters are likely to be included with the motherboard chipset or as part of the CPU itself. This is also referred to as an onboard adapter or onboard graphics. If a computer is to be used for 3-D gaming, computer-aided design (CAD), or digital artwork, a more powerful video adapter is required. This can be installed as an add-on card via a PCIe slot. Most graphics adapters are based on chipsets by ATI/AMD, NVIDIA, and Intel. Video cards are distinguished by the following features:

- **Graphics Processing Unit (GPU)**—A microprocessor designed and optimized for processing instructions that render 2-D and 3-D images and effects on-screen. The basic test for a GPU is the frame rate it can produce for a particular game or application. Other performance characteristics include support for levels of texture and lighting effects.
- **Graphics memory**—3-D cards need a substantial amount of memory for processing and texture effects. A dedicated card may be fitted with up to 12 GB GDDR RAM at the high end; around 4–6 GB would be more typical of current mid-range performance cards. Low-end cards use shared memory (that is, the adapter uses the system RAM). Some cards may use a mix of dedicated and shared memory.
- **Video ports**—The type and number of connectors, such as HDMI, DisplayPort, and Thunderbolt.

Graphics Double Data Rate (GDDR) memory technology is similar to the DDR modules used for system RAM.

Most modern cards use a PCIe x16 interface. Dual cards, using two (or more) slots, are also available.



A video/graphics card with DisplayPort, HDMI, and DVI-I ports. (Image ©123RF.com)

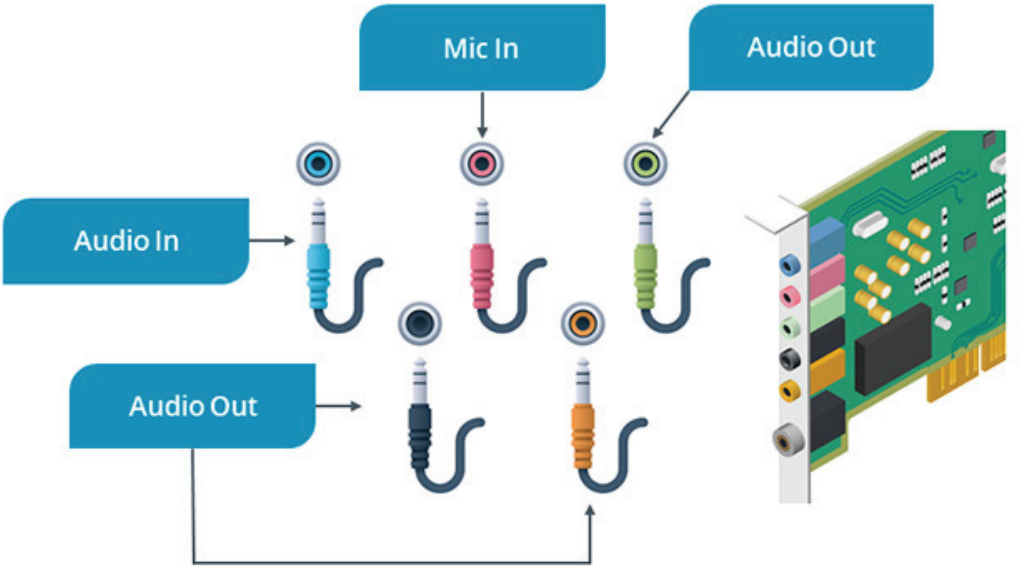
Capture Cards

Where a graphics card generates an output video signal to drive a monitor, a **capture card** is used to record video input and save it as a type of movie or streaming media file. Many capture cards are designed to record footage from computer games. Some are designed to work with PC games, while others record from game console HDMI sources or from a live camera HDMI source, such as a camcorder or security camera. Another class of capture card can act as a TV tuner and record video from broadcast TV sources.

A capture card can be fitted as an internal PCIe or as an external unit connected via USB/Thunderbolt.

Sound Cards

Audio playback is achieved via speakers or headphones, which are connected to a **sound card** via an audio jack. Sound cards are also used to record input from a microphone. Most audio jacks are 3.5 mm (⅛ inch) mono or stereo jacks. These are also referred to as phone plugs or mini tip, ring, sleeve (TRS) connectors.



Audio jacks on a sound card. (Image ©123RF.com)

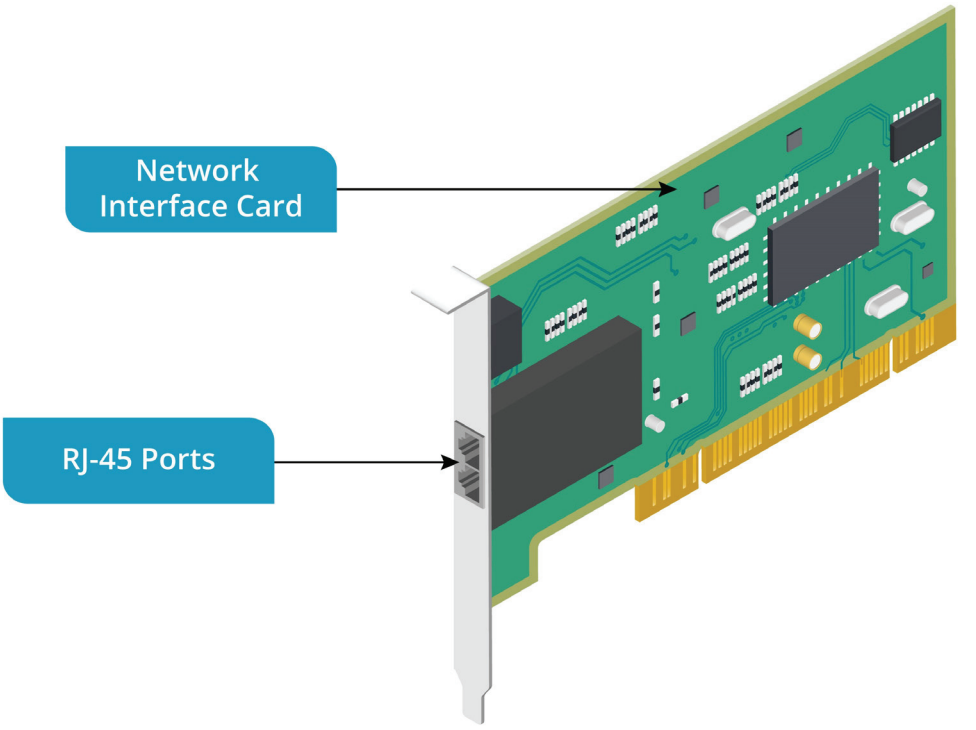
Sound cards supporting multiple output channels with an appropriate speaker system can provide various levels of playback, from mono (on legacy systems) or stereo to some type of surround sound. Surround sound uses multiple speakers positioned around the listener to provide a "cinematic" audio experience.

A basic sound chip may be provided as part of the motherboard chipset, but better-quality audio functions can be provided as a PCIe or PCI expansion card. Pro-level cards may also feature onboard memory, flash memory storing sound samples (wavetables), and additional jack types for different input sources.

Audio hardware built into a computer may be susceptible to noise from other internal components when using recording functionality. Consequently, most audio interfaces designed for professional use are external units connected via USB or Thunderbolt.

Network Interface Cards

Most computers have an Ethernet network adapter already installed as part of the motherboard chipset. However, there may be occasions when you need to install an add-on **network interface card (NIC)** or need to upgrade an adapter to use a different type of network or cabling/connector, such as copper cable versus fiber optic. A dedicated NIC may also provision multiple ports. These can be bonded into a single higher bandwidth link.



RJ45 ports on a Network Interface Card (NIC). (Image ©123RF.com)

A Wi-Fi adapter can be added to connect to a wireless network. Wi-Fi adapters are developed to different 802.11 standards. There are also cards that can connect to cellular data networks.

Review Activity:

Motherboards

Answer the following questions:

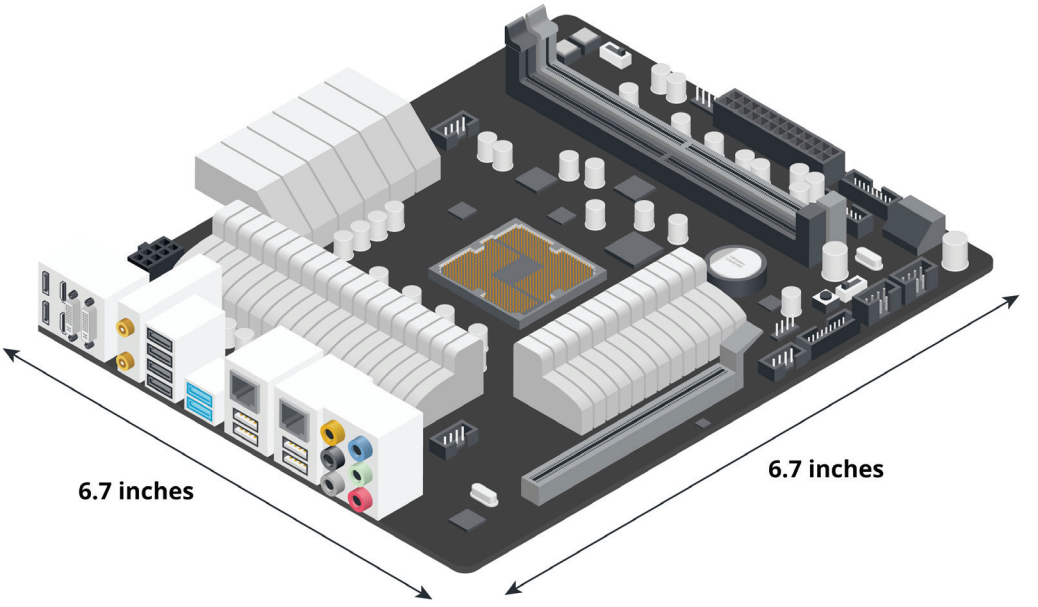
1. **What type of motherboard socket is used to install system memory?**

2. **How many storage devices can be attached to a single SATA port?**

3. **What is the bandwidth of a PCIe v2.0 x16 graphics adapter?**

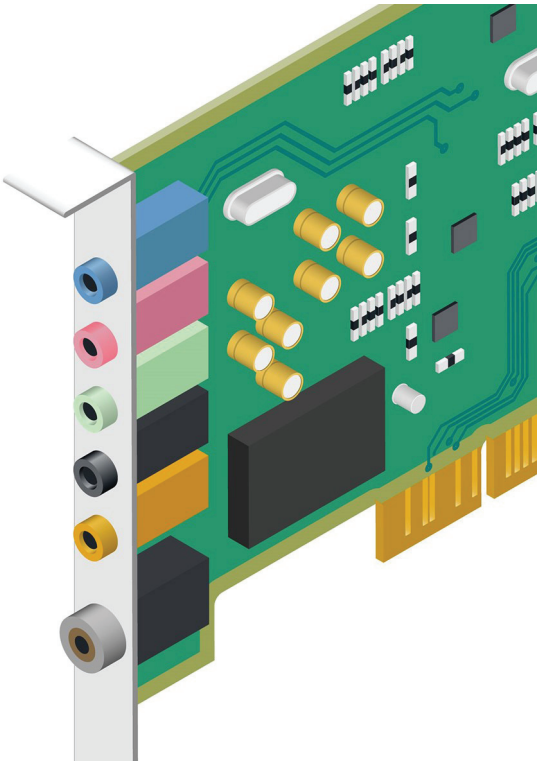
4. **You have a x8 PCIe storage adapter card—can you fit this in a x16 slot?**

5. **You are labelling spare parts for inventory. What type of motherboard is displayed here?**



(Image ©123RF.com)

6. You have another part to label for inventory. What category of adapter card is shown in the exhibit?



(Image ©123RF.com)

Topic 1C

Explain Legacy Cable Types

CORE 1 EXAM OBJECTIVES COVERED

3.1 Explain basic cable types and their connectors, features, and purposes.

As PC designs have evolved over the years, many types of bus interface have been implemented as connectivity solutions for computer components that maximize the performance and functionality at the time. There can be many reasons why computer systems using these older bus types remain in use in the workplace. As you are likely to work in diverse environments over the course of your career, it is important that you be able to support older technologies alongside modern ones.

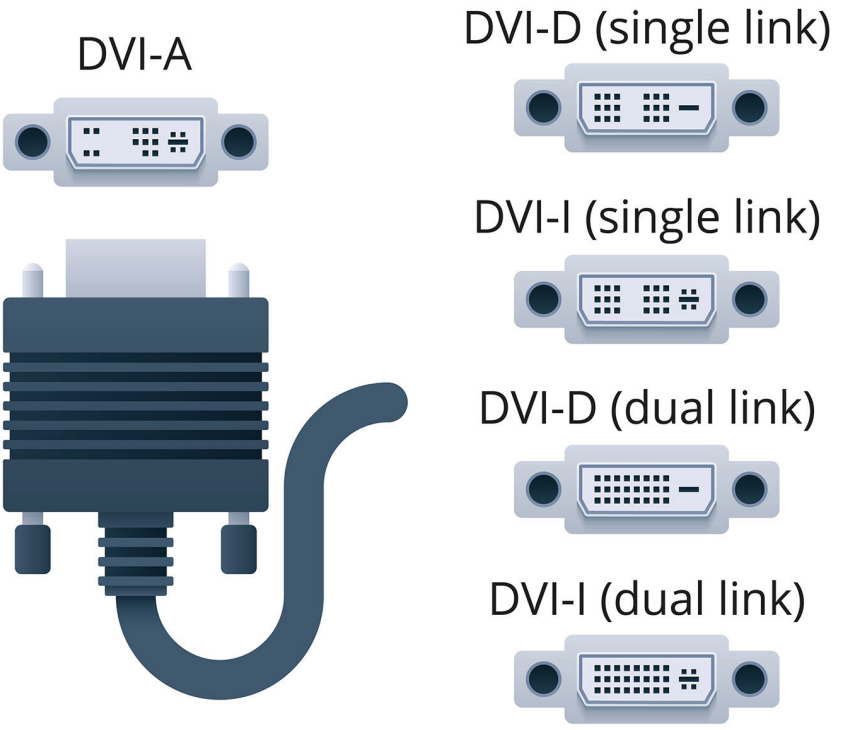
DVI and VGA Video Cables

The HDMI and DisplayPort video interfaces only support digital flat-panel displays. Older video interfaces were used when computer monitors and projectors were predominantly of the cathode ray tube (CRT) type, driven by an analog signal.

Digital Visual Interface

Digital Visual Interface (DVI) is designed to support both analog and digital outputs. While popular for a period after its introduction in 1999, DVI is no longer in active development. You are only likely to encounter DVI on older display devices and video cards.

There are five types of DVI, supporting different configurations for single and dual link (extra bandwidth) and analog/digital output signaling. The pin configuration of the connectors identifies what type of DVI is supported by a particular port.

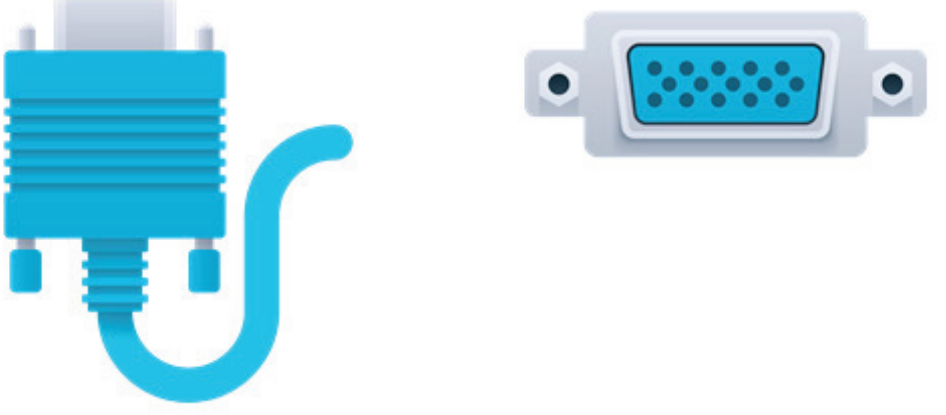


DVI port and connector types. (Image ©123RF.com)

DVI-I supports both analog equipment and digital outputs. DVI-A supports only analog output and DVI-D supports only digital.

Video Graphics Array Interface

The 15-pin **Video Graphics Array (VGA)** port was the standard analog video interface for PC devices for a very long time. Up until a few years ago, most video cards and monitors included a VGA port, though it is starting to be phased out completely now. VGA will usually support resolutions up to HD (1920x1080), depending on cable quality. The connector is a D-shell type with screws to secure it to the port.



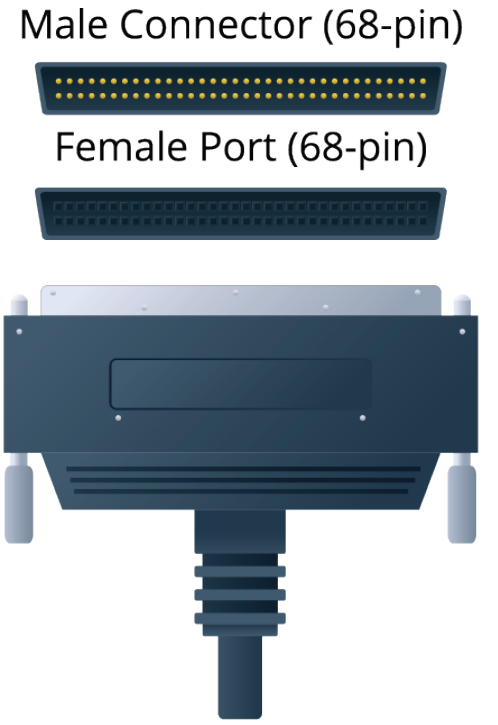
A VGA connector and port. (Image ©123RF.com)

Small Computer System Interface

Modern bus interfaces such as USB and Thunderbolt use serial communications. These serial links can achieve Mbps and Gbps speeds through the use of improved signaling and encoding methods. Back when serial interfaces were much slower, PC vendors used parallel data transmission to support better transfer rates. While a serial interface essentially transfers 1 bit at a time, a parallel interface transfers 8 bits (1 byte) or more. This requires more wires in the cable and more pins in the connectors, meaning parallel interfaces are bulky.

Small computer system interface (SCSI) is one example of a legacy parallel bus. One SCSI host bus adapter (HBA) can control multiple devices attached by internal ribbon cables or external SCSI cables. The SCSI standard also defines a command language that allows the host adapter to identify which devices are connected to the bus and how they are accessed.

SCSI could be used for both internal devices and external peripherals, such as scanners and printers, but you are now unlikely to find it used for any purpose other than the connection of internal hard disk drives. SCSI could support data rates up to 320 MBps. There have been numerous versions of SCSI with many different physical connectors, but you are only likely to come across high density (HD) 68-pin connectors or single connector attachment (SCA) 80-pin connectors. SCA incorporates a power connector, while HD-68 is used with Molex power connectors.



Internal and external male HD connectors. (Image ©123RF.com)

Each device on a wide SCSI bus must be configured with a unique ID, from 0 to 15. The host adapter is usually set to 7 or 15. A bootable hard disk is usually allocated ID 0. The first and last devices on a SCSI bus must be terminated. Termination may either be enabled internally on the device by setting a switch or by physically connecting a terminator pack to a device or the host adapter.

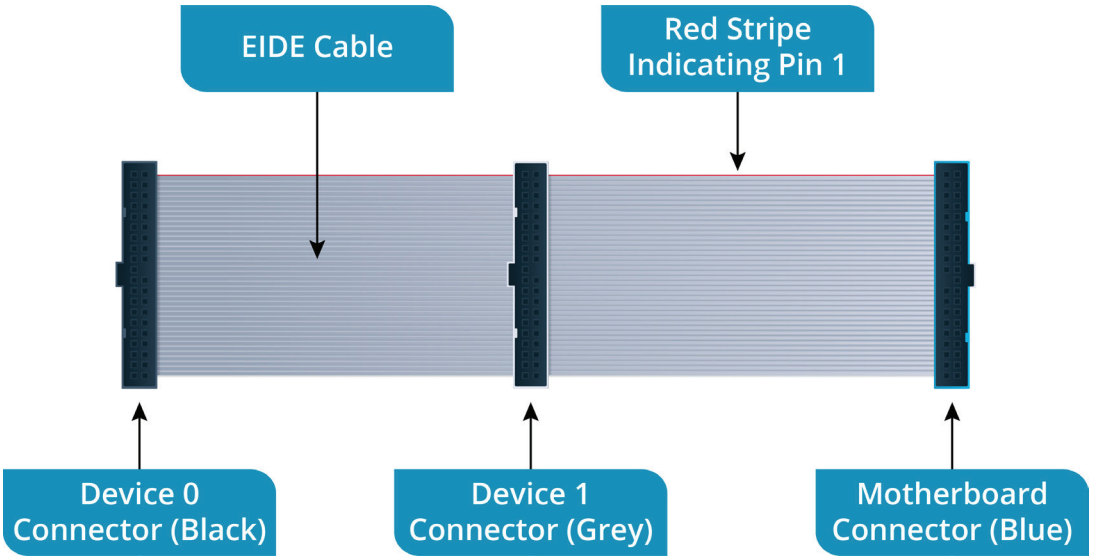
Additionally, you should note that while parallel SCSI as a physical interface has almost completely disappeared, the software interface and command set are used in many other storage technologies, including serial attached SCSI (SAS). SAS is a dominant interface for enterprise-class storage devices in the PC workstation and server market.

Integrated Drive Electronics Interface

The **integrated drive electronics (IDE)** interface was the principal mass storage interface for desktop PCs for many years. The interface is also referred to as parallel advanced technology attachment (PATA). The extended IDE (EIDE) bus interface uses 16-bit parallel data transfers.

A motherboard supporting IDE may come with one or two host adapters, called the IDE1 channel and the IDE2 channel. These may also be labelled primary (PRI IDE) and secondary (SEC IDE). A single IDE channel is now more typical if the motherboard also supports SATA. Each IDE channel supports two devices, 0 and 1.

An EIDE cable typically has three color-coded connectors. The blue connector is for the motherboard port. The black (end) and grey (middle) connectors attach to devices 0 and 1 respectively. When inserting a connector, pin 1 on the cable must be oriented with pin 1 on the port. On the cable, pin 1 is identified with a red stripe. The connectors are also keyed to prevent them from being inserted the wrong way around.

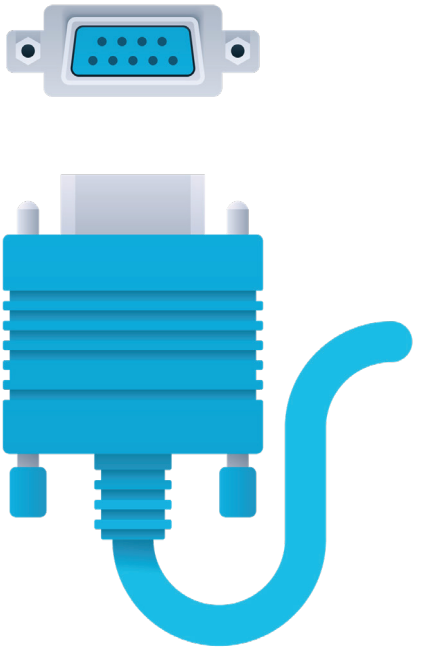


EIDE cable with device 0 (black), device 1 (grey), and motherboard (blue) connectors. The red strip indicates pin 1 on the cable. (Image ©123RF.com)

Unfortunately, the terms master and slave were used to distinguish device 0 and device 1. CompTIA and the computing industry generally are working to eliminate this type of non-inclusive terminology, but you will often still see it used in historical support documentation.

Serial Cables

The **serial** port is a legacy connection interface where data is transmitted over one wire one bit at a time. Start, stop, and parity bits are used to format and verify data transmission. This interface is also referred to as Recommended Standard #232 (RS-232). While modern interfaces like USB are also serial, an RS-232 interface uses much less sophisticated signaling methods. Consequently, an RS-232 serial port supports data rates up to about 115 Kbps only.



9-pin serial connector and port. (Image ©123RF.com)

Serial ports are generally associated with connecting external modems, used to establish dial-up Internet connections, though even this function has largely been superseded by USB. You may also come across serial ports on network equipment, where a serial connection can be used to manage the device.

RS-232 specifies a 25-pin hardware interface, but in practice, PC manufacturers used the cheaper 9-pin D-subminiature (**DB-9**) female port shown above.

In Windows, the serial port is referred to as a Communications (COM) port.

You might also come across PS/2 serial ports. PS/2 i used to attach mice and keyboards. PS/2 ports use a 6-pin mini-DIN format. The green color-coded port is used to attach a mouse, and the purple one is for a keyboard.

Adapter Cables

Given the numerous cable types and connector types, it will often be the case that a basic peripheral cable will not provide a connection between a port available on the PC and the port used on the peripheral device. An adapter cable can often be used to overcome this issue. An **adapter cable** has connectors for two different cable types at each end. An active adapter uses circuitry to convert the signal, while a passive adapter simply converts between two connector form factors.

The following types of adapter cable are typical:

- Video adapters convert between signaling types, such as HDMI to VGA, HDMI to DisplayPort, or HDMI to DVI.
- USB adapters to convert connector types, such as USB-C to USB-A. There are also USB hubs that provide additional ports.
- USB adapters to various kinds of output, including Lightning and HDMI.

Review Activity:

Legacy Cable Types

Answer the following questions:

1. You are labelling systems for inventory. What two types of display cabling can be connected to this laptop?

2. Which ports are present on the graphics card shown below?

3. Which interfaces does the adapter cable shown below support?

Lesson 1

Summary

You should be able to identify and install types of interfaces and their physical connectors on the motherboard and on peripheral devices.

Guidelines for Installing and Configuring Motherboards and Connectors

Follow these guidelines to support the installation and configuration of motherboards, peripheral devices, and connectors:

- Make support documentation available so that technicians can easily identify the features of system cases and motherboards—especially ATX/ITX form factor, CPU socket type, and header configuration—and perform maintenance and upgrades efficiently.
- Identify requirements for peripheral cables and connector types so that missing or faulty cables can be replaced quickly. Consider stocking adapter cables so that use can be made of devices even if the connector type is not directly supported by the motherboard.
- Identify opportunities to upgrade devices that use legacy interfaces—VGA, DVI, PCI, EIDE/PATA, SCSI, and RS-232 serial—with faster and more reliable modern versions—USB/Thunderbolt, HDMI, DisplayPort, PCIe, SATA, and M.2.
- Identify systems that have additional requirements to the controllers and ports provided on the motherboard and research the best model of video, capture, sound, or network card to meet the requirement.

Growing Home IT-Training Curriculum

CompTia Network Certification (Part 3)

6429 S. Honore St, Chicago, IL 60636 | 773.549.1336
www.growinghomeinc.org

CompTIA

The Official CompTIA

Network+ Study Guide

Exam N10-008

Official CompTIA Content Series for CompTIA Performance Certifications

The Official CompTIA Network+ Study Guide (Exam N10-008)

Course Edition: 1.0

Acknowledgments

James Pengelly, Author

Thomas Reilly, Senior Vice President, Learning

Katie Hoenicke, Senior Director, Product Management

Evan Burns, Senior Manager, Learning Technology Operations and Implementation

James Chesterfield, Manager, Learning Content and Design

Becky Mann, Director, Product Development

Katherine Keyes, Content Specialist

Notices

Disclaimer

While CompTIA, Inc. takes care to ensure the accuracy and quality of these materials, we cannot guarantee their accuracy, and all materials are provided without any warranty whatsoever, including, but not limited to, the implied warranties of merchantability or fitness for a particular purpose. The use of screenshots, photographs of another entity's products, or another entity's product name or service in this book is for editorial purposes only. No such use should be construed to imply sponsorship or endorsement of the book by nor any affiliation of such entity with CompTIA. This courseware may contain links to sites on the Internet that are owned and operated by third parties (the "External Sites"). CompTIA is not responsible for the availability of, or the content located on or through, any External Site. Please contact CompTIA if you have any concerns regarding such links or External Sites.

Trademark Notice

CompTIA®, Network+®, and the CompTIA logo are registered trademarks of CompTIA, Inc., in the U.S. and other countries. All other product and service names used may be common law or registered trademarks of their respective proprietors.

Copyright Notice

Copyright © 2021 CompTIA, Inc. All rights reserved. Screenshots used for illustrative purposes are the property of the software proprietor. Except as permitted under the Copyright Act of 1976, no part of this publication may be reproduced or distributed in any form or by any means, or stored in a database or retrieval system, without the prior written permission of CompTIA, 3500 Lacey Road, Suite 100, Downers Grove, IL 60515-5439.

This book conveys no rights in the software or other products about which it was written; all use or licensing of such software or other products is the responsibility of the user according to terms and conditions of the owner. If you believe that this book, related materials, or any other CompTIA materials are being reproduced or transmitted without permission, please call 1-866-835-8020 or visit **help.comptia.org**.

Table of Contents

Lesson 1: Comparing OSI Model Network Functions 1

- Topic 1A: Compare and Contrast OSI Model Layers 2
- Topic 1B: Configure SOHO Networks 10

Lesson 2: Deploying Ethernet Cabling 19

- Topic 2A: Summarize Ethernet Standards 20
- Topic 2B: Summarize Copper Cabling Types 25
- Topic 2C: Summarize Fiber Optic Cabling Types 34
- Topic 2D: Deploy Ethernet Cabling 41

Lesson 3: Deploying Ethernet Switching 51

- Topic 3A: Deploy Networking Devices 52
- Topic 3B: Explain Network Interfaces 58
- Topic 3C: Deploy Common Ethernet Switching Features 65

Lesson 4: Troubleshooting Ethernet Networks 75

- Topic 4A: Explain Network Troubleshooting Methodology 76
- Topic 4B: Troubleshoot Common Cable Connectivity Issues 85

Lesson 5: Explaining IPv4 Addressing 97

- Topic 5A: Explain IPv4 Addressing Schemes 98
- Topic 5B: Explain IPv4 Forwarding 106
- Topic 5C: Configure IP Networks and Subnets 115

Lesson 6: Supporting IPv4 and IPv6 Networks 125

- Topic 6A: Use Appropriate Tools to Test IP Configuration 126
- Topic 6B: Troubleshoot IP Networks 133
- Topic 6C: Explain IPv6 Addressing Schemes 139

Lesson 7: Configuring and Troubleshooting Routers 149

Topic 7A: Compare and Contrast Routing Concepts 150

Topic 7B: Compare and Contrast Dynamic Routing Concepts 156

Topic 7C: Install and Troubleshoot Routers 171

Lesson 8: Explaining Network Topologies and Types 185

Topic 8A: Explain Network Types and Characteristics 186

Topic 8B: Explain Tiered Switching Architecture 194

Topic 8C: Explain Virtual LANs 200

Lesson 9: Explaining Transport Layer Protocols 207

Topic 9A: Compare and Contrast Transport Protocols 208

Topic 9B: Use Appropriate Tools to Scan Network Ports 216

Lesson 10: Explaining Network Services 225

Topic 10A: Explain the Use of Network Addressing Services 226

Topic 10B: Explain the Use of Name Resolution Services 233

Topic 10C: Configure DNS Services 241

Lesson 11: Explaining Network Applications 247

Topic 11A: Explain the Use of Web, File/Print, and Database Services 248

Topic 11B: Explain the Use of Email and Voice Services 256

Lesson 12: Ensuring Network Availability 267

Topic 12A: Explain the Use of Network Management Services 268

Topic 12B: Use Event Management to Ensure Network Availability 274

Topic 12C: Use Performance Metrics to Ensure Network Availability 284

Lesson 13: Explaining Common Security Concepts 295

Topic 13A: Explain Common Security Concepts 296

Topic 13B: Explain Authentication Methods 304

Lesson 14: Supporting and Troubleshooting Secure Networks 317

Topic 14A: Compare and Contrast Security Appliances 318

Topic 14B: Troubleshoot Service and Security Issues 329

Lesson 15: Deploying and Troubleshooting Wireless Networks 341

Topic 15A: Summarize Wireless Standards 342

Topic 15B: Install Wireless Networks 350

Topic 15C: Troubleshoot Wireless Networks 358

Topic 15D: Configure and Troubleshoot Wireless Security 366

Lesson 16: Comparing WAN Links and Remote Access Methods 375

Topic 16A: Explain WAN Provider Links 376

Topic 16B: Compare and Contrast Remote Access Methods 383

Lesson 17: Explaining Organizational and Physical Security Concepts 395

Topic 17A: Explain Organizational Documentation and Policies 396

Topic 17B: Explain Physical Security Methods 408

Topic 17C: Compare and Contrast Internet of Things Devices 416

Lesson 18: Explaining Disaster Recovery and High Availability Concepts 423

Topic 18A: Explain Disaster Recovery Concepts 424

Topic 18B: Explain High Availability Concepts 431

Lesson 19: Applying Network Hardening Techniques 439

Topic 19A: Compare and Contrast Types of Attacks 440

Topic 19B: Apply Network Hardening Techniques 453

Lesson 20: Summarizing Cloud and Datacenter Architecture..... 463

Topic 20A: Summarize Cloud Concepts..... 464

Topic 20B: Explain Virtualization and Storage Area Network Technologies..... 471

Topic 20C: Explain Datacenter Network Architecture..... 478

Appendix A: Mapping Course Content to CompTIA Network+ (N10-008).....A-1

Solutions S-1

Glossary G-1

Index I-1

About This Course

CompTIA is a not-for-profit trade association with the purpose of advancing the interests of IT professionals and IT channel organizations, and its industry-leading IT certifications are an important part of that mission. CompTIA's Network+ Certification is an entry-level certification designed for professionals with 9-12 months' work experience in roles such as a junior network administrator or network support technician.

> The CompTIA Network+ certification exam will verify the successful candidate has the knowledge and skills required to:
>
> - Establish network connectivity by deploying wired and wireless devices.
> - Understand and maintain network documentation.
> - Understand the purpose of network services.
> - Understand basic datacenter, cloud, and virtual networking concepts.
> - Monitor network activity, identifying performance and availability issues.
> - Implement network hardening techniques.
> - Manage, configure, and troubleshoot network infrastructure.
>
> *CompTIA Network+ Exam Objectives*

Course Description

Course Objectives

This course can benefit you in two ways. If you intend to pass the CompTIA Network+ (Exam N10-008) certification examination, this course can be a significant part of your preparation. But certification is not the only key to professional success in the field of network support. Today's job market demands individuals have demonstrable skills, and the information and activities in this course can help you build your network administration skill set so that you can confidently perform your duties in any entry-level network support technician role.

On course completion, you will be able to:

- Deploy and troubleshoot Ethernet networks.
- Support IPv4 and IPv6 networks.
- Configure and troubleshooting routers.
- Support network services and applications.
- Ensure network security and availability.
- Deploy and troubleshooting wireless networks.
- Support WAN links and remote access methods.
- Support organizational procedures and site security controls.
- Summarize cloud and datacenter architecture.

Target Student

The Official CompTIA Network+ Guide (Exam N10-008) is the primary course you will need to take if your job responsibilities include network administration, installation, and security within your organization. You can take this course to prepare for the CompTIA Network+ (Exam N10-008) certification examination.

Prerequisites

To ensure your success in this course, you should have basic IT skills comprising nine to twelve months' experience. CompTIA A+ certification, or the equivalent knowledge, is strongly recommended.

The prerequisites for this course might differ significantly from the prerequisites for the CompTIA certification exams. For the most up-to-date information about the exam prerequisites, complete the form on this page: www.comptia.org/training/resources/exam-objectives.

How to Use The Study Notes

The following sections will help you understand how the course structure and components are designed to support mastery of the competencies and tasks associated with the target job roles and will help you to prepare to take the certification exam.

As You Learn

At the top level, this course is divided into **lessons,** each representing an area of competency within the target job roles. Each lesson is composed of a number of topics. A **topic** contains subjects that are related to a discrete job task, mapped to objectives and content examples in the CompTIA exam objectives document. Rather than follow the exam domains and objectives sequence, lessons and topics are arranged in order of increasing proficiency. Each topic is intended to be studied within a short period (typically 30 minutes at most). Each topic is concluded by one or more activities, designed to help you to apply your understanding of the study notes to practical scenarios and tasks.

Additional to the study content in the lessons, there is a glossary of the terms and concepts used throughout the course. There is also an index to assist in locating particular terminology, concepts, technologies, and tasks within the lesson and topic content.

In many electronic versions of the book, you can click links on key words in the topic content to move to the associated glossary definition, and on page references in the index to move to that term in the content. To return to the previous location in the document after clicking a link, use the appropriate functionality in your eBook viewing software.

Watch throughout the material for the following visual cues.

Student Icon	Student Icon Descriptive Text
	A **Note** provides additional information, guidance, or hints about a topic or task.
	A **Caution** note makes you aware of places where you need to be particularly careful with your actions, settings, or decisions so that you can be sure to get the desired results of an activity or task.

As You Review

Any method of instruction is only as effective as the time and effort you, the student, are willing to invest in it. In addition, some of the information that you learn in class may not be important to you immediately, but it may become important later. For this reason, we encourage you to spend some time reviewing the content of the course after your time in the classroom.

Following the lesson content, you will find a table mapping the lessons and topics to the exam domains, objectives, and content examples. You can use this as a checklist as you prepare to take the exam, and review any content that you are uncertain about.

As A Reference

The organization and layout of this book make it an easy-to-use resource for future reference. Guidelines can be used during class and as after-class references when you're back on the job and need to refresh your understanding. Taking advantage of the glossary, index, and table of contents, you can use this book as a first source of definitions, background information, and summaries.

Lesson 1

Comparing OSI Model Network Functions

LESSON INTRODUCTION

Computer networks are complex systems that incorporate multiple functions, standards, and proprietary technologies. The Open Systems Interconnection (OSI) model is used to try to simplify some of this complexity. It divides network technologies between seven functional layers. This makes it easier to separate and focus on individual concepts and technologies while retaining an understanding of relationships to the functions of technologies placed in other layers.

This lesson uses the OSI model to give you an overview of the technologies that you will be studying in the rest of the course. You will compare the functions of these layers in the OSI model and apply those concepts to the installation and configuration of a small office/home office network.

Lesson Objectives

In this lesson, you will:

- Compare and contrast OSI model layers.
- Configure SOHO networks.

Topic 1A

Compare and Contrast OSI Model Layers

EXAM OBJECTIVES COVERED

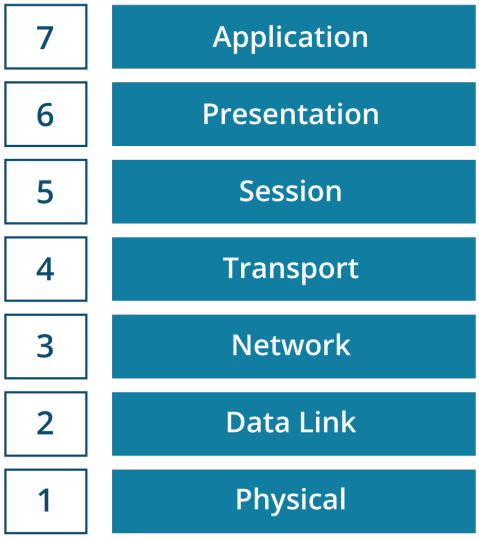
1.1 Compare and contrast the Open Systems Interconnection (OSI) model layers and encapsulation concepts.

Networks are built on common standards and models that describe how devices and protocols interconnect. In this topic, you will identify how the implementation and support of these systems refer to an important common reference model: the Open Systems Interconnection (OSI) model. The OSI model breaks the data communication process into discrete layers. Being able to identify the OSI layers and compare the functions of devices and protocols working at each layer will help you to implement and troubleshoot networks.

Open Systems Interconnection Model

A network is two or more computer systems that are linked by a transmission medium and share one or more protocols that enable them to exchange data. You can think of any network in terms of nodes and links. The nodes are devices that send, receive, and forward data and the links are the communications pathways between them.

The International Organization for Standardization (ISO) developed the **Open Systems Interconnection (OSI) reference model** (iso.org/standard/20269.html) to promote understanding of how components in a network system work. It does this by separating the function of hardware and software components to seven discrete layers. Each layer performs a different group of tasks required for network communication.



The OSI model.

Although not all network systems implement layers using this precise structure, they all implement each task in some way. The OSI model is not a standard or a specification; it serves as a functional guideline for designing network protocols, software, and appliances and for troubleshooting networks.

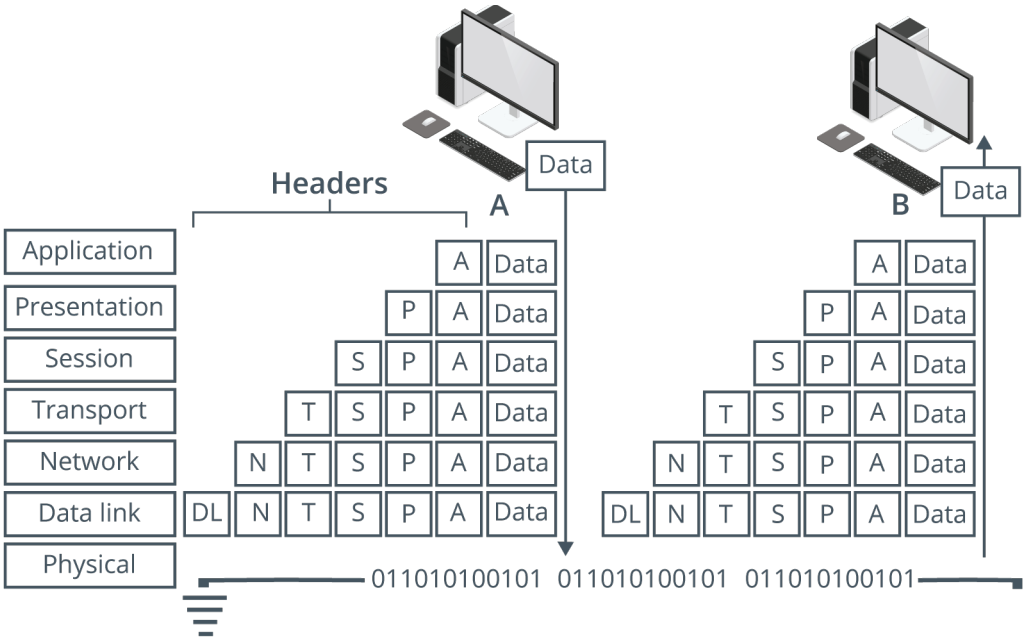
To remember the seven layers, use the following mnemonic: All People Seem To Need Data Processing.

Data Encapsulation and Decapsulation

A network protocol is a set of rules for exchanging data in a structured format. A network protocol has two principal functions:

- **Addressing**—Describing where data messages should go. At each layer, there are different mechanisms for identifying nodes and rules for how they can send and receive messages.
- **Encapsulation**—Describing how data messages should be packaged for transmission. Encapsulation is like an envelope for a letter, with the distinction that each layer requires its own envelope. At each layer, the protocol adds fields in a header to whatever data (payload) it receives from an application or other protocol.

A network will involve the use of many different protocols operating at different layers of the OSI model. At each layer, for two nodes to communicate they must be running the same protocol. The protocol running at each layer communicates with its equivalent (or peer) layer on the other node. This communication *between* nodes at the same layer is described as a same layer interaction. To transmit or receive a communication, *on* each node, each layer provides services for the layer above and uses the services of the layer below. This is referred to as adjacent layer interaction.



Encapsulation and decapsulation. (Images © 123RF.com.)

When a message is sent from one node to another, it travels down the stack of layers on the sending node, reaches the receiving node using the transmission media, and then passes up the stack on that node. At each level (except the physical layer), the sending node adds a header to the data payload, forming a "chunk" of data called a protocol data unit (PDU). This is the process of encapsulation.

For example, on the sending node, data is generated by an application, such as the HyperText Transfer Protocol (HTTP), which will include its own application header. At the transport layer, a Transport Control Protocol (TCP) header is added to this application data. At the network layer, the TCP segment is wrapped in an Internet Protocol (IP) header. The IP packet is encapsulated in an Ethernet frame at the data link layer, then the stream of bits making up the frame is transmitted over the network at the physical layer as a modulated electrical signal.

The receiving node performs the reverse process, referred to as decapsulation. It receives the stream of bits arriving at the physical layer and decodes an Ethernet frame. It extracts the IP packet from this frame and resolves the information in the IP header, then does the same for the TCP and application headers, eventually extracting the HTTP application data for processing by a software program, such as a web browser or web server.

You might notice that this example seems to omit some OSI layers. This is because "real-world" protocols do not conform exactly to the OSI model.

Layer 1—Physical

The **physical layer (PHY)** of the OSI model (layer 1) is responsible for the transmission and receipt of the signals that represent bits of data from one node to another node. Different types of transmission media can be classified as cabled or wireless:

- **Cabled**—A physical signal conductor is provided between two nodes. Examples include cable types such as copper or fiber optic cable. Cabled media can also be described as bounded media.
- **Wireless**—Uses free space between nodes, such as microwave radio. Wireless media can also be described as unbounded media.

The Physical layer specifies the following:

- **Physical topology**—The layout of nodes and links as established by the transmission media. An area of a larger network is called a segment. A network is typically divided into segments to cope with the physical restrictions of the network media used, to improve performance, or to improve security. At the Physical layer, a segment is where all the nodes share access to the same media.
- **Physical interface**—Mechanical specifications for the network medium, such as cable specifications, the medium connector and pin-out details (the number and functions of the various pins in a network connector), or radio transceiver specifications.
- The process of transmitting and receiving signals over the network medium, including modulation schemes and timing/synchronization.

Devices that operate at the Physical layer include:

- **Transceiver**—The part of a network interface that sends and receives signals over the network media.
- **Repeater**—A device that amplifies an electronic signal to extend the maximum allowable distance for a media type.

- **Hub**—A multiport repeater, deployed as the central point of connection for nodes.
- **Media converter**—A device that converts one media signaling type to another.
- **Modem**—A device that performs some type of signal modulation and demodulation, such as sending digital data over an analog line.

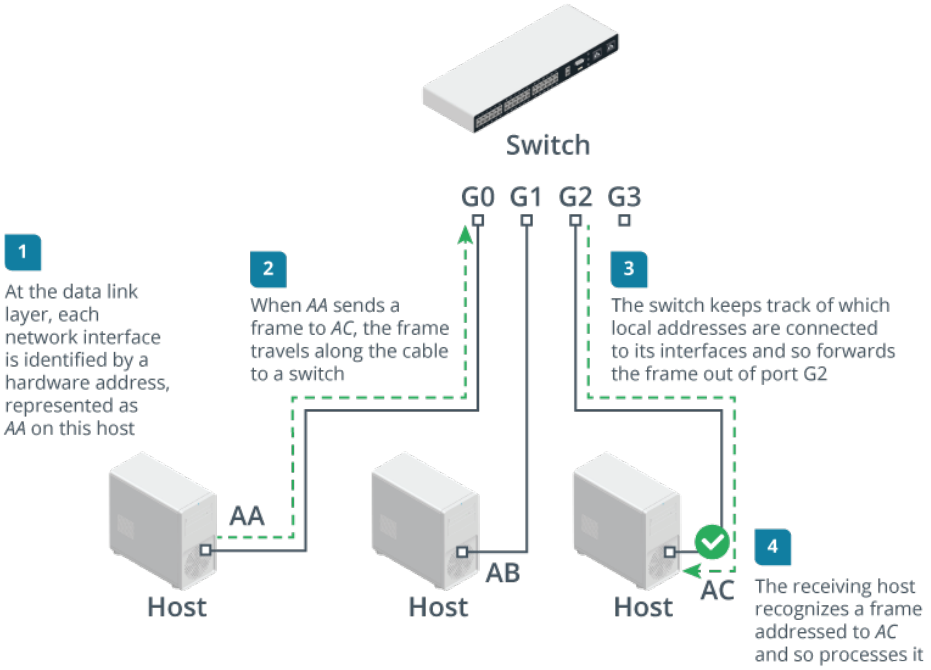
Layer 2—Data Link

The **data link layer (layer 2)** is responsible for transferring data between nodes on the same logical segment. At the Data Link layer, a segment is one where all nodes can send traffic to one another using hardware addresses, regardless of whether they share access to the same media. A layer 2 segment might include multiple physical segments. This is referred to as a logical topology.

Relatively few networks are based on directly connecting hosts together. Rather than making hosts establish direct links with one another, each host is connected to a central node, such as a switch or a wireless access point. The central node provides a forwarding function, receiving the communication from one node and sending it to another. The addresses of interfaces within the same layer 2 segment are described as local addresses or hardware addresses.

Nodes that send and receive information are referred to as end systems or as host nodes. This type of node includes computers, laptops, servers, Voice over IP (VoIP) phones, smartphones, and printers. A node that provides only a forwarding function is referred to as an intermediate system or infrastructure node.

The data link layer organizes the stream of bits arriving from the physical layer into structured units called frames. Each frame contains a network layer packet as its payload. The data link layer adds control information to the payload in the form of header fields. These fields include source and destination hardware addresses, plus a basic error check to test if the frame was received intact.



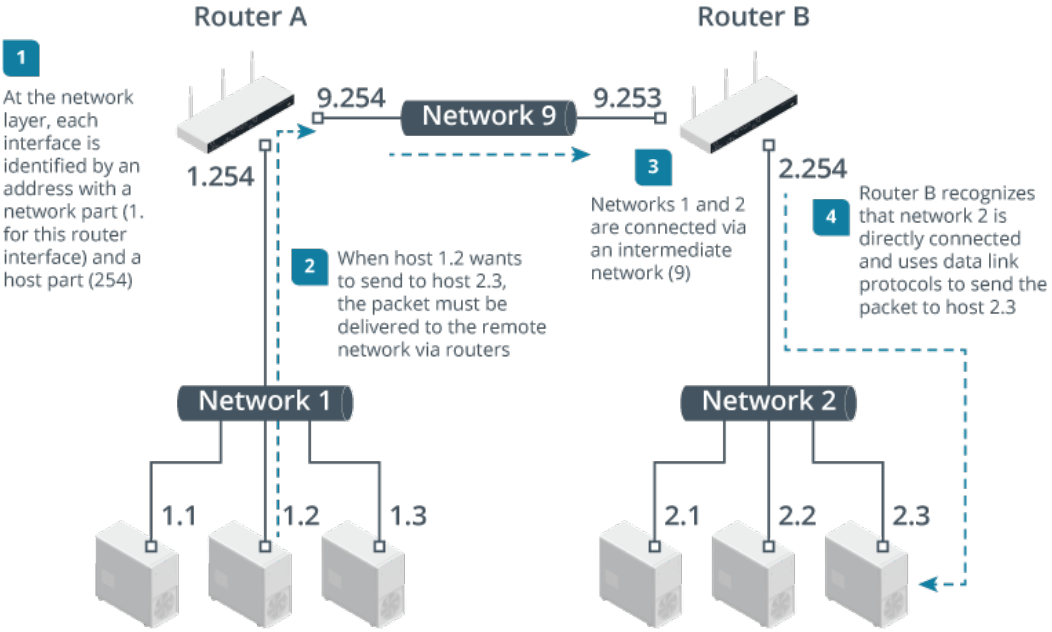
Communications at layer 2 of the OSI model. (Images © 123RF.com)

Devices that operate at the data link layer include:

- **Network adapter or network interface card (NICs)**—An NIC joins an end system host to network media (cabling or wireless) and enables it to communicate over the network by assembling and disassembling frames.
- **Bridge**—A bridge is a type of intermediate system that joins physical network segments while minimizing the performance reduction of having more nodes on the same network. A bridge has multiple ports, each of which functions as a network interface.
- **Switch**—An advanced type of bridge with many ports. A switch creates links between large numbers of nodes more efficiently.
- **Wireless access point (AP)**—An AP allows nodes with wireless network cards to communicate and creates a bridge between wireless networks and wired ones.

Layer 3—Network

The **network layer (layer 3)** is responsible for moving data around a network of networks, known as an internetwork or the Internet. While the data link layer is capable of forwarding data by using hardware addresses within a single segment, the network layer moves information around an internetwork by using logical network and host IDs. The networks are often heterogeneous; that is, they use a variety of physical layer media and data link protocols. The main appliance working at layer 3 is the **router**.



Communications at layer 3 of the OSI model. (Images © 123RF.com)

The network layer forwards information between networks by examining the destination network-layer address or logical network address. The packet is forwarded, router by router (or hop by hop), through the internetwork to the target network. Once it has reached the destination network, the hardware address can be used to deliver the packet to the target node.

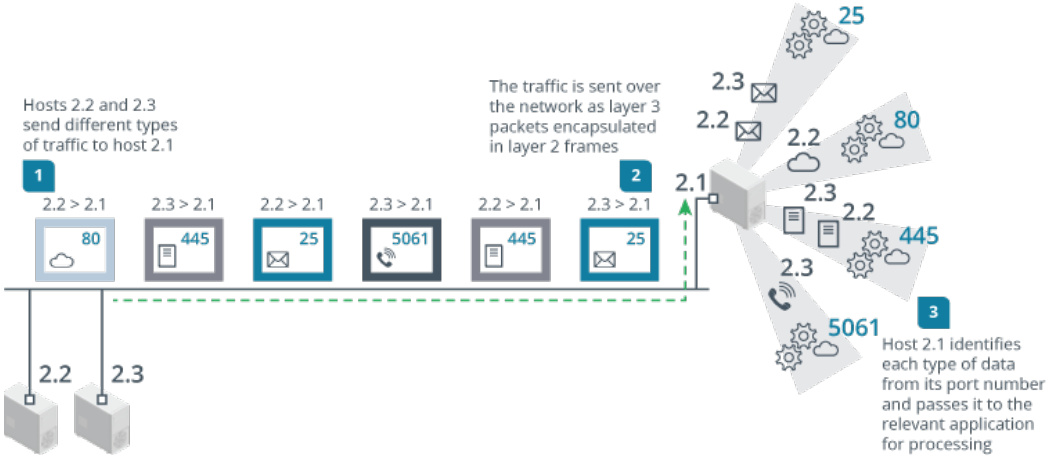
The general convention is to describe PDUs packaged at the network layer as packets or datagrams, and messages packaged at the data link layer as frames. Packet is often used to describe PDUs at any layer, however.

It is usually important for traffic passing between networks to be filtered. A basic firewall operates at layer 3 to enforce an access control list (ACL). A network ACL is a list of the addresses and types of traffic that are permitted or blocked.

Layer 4—Transport

The first three layers of the OSI model are primarily concerned with moving frames and datagrams between nodes and networks. At the **transport layer**—also known as the end-to-end or host-to-host layer—the content of the packets becomes significant. Any given host on a network will be communicating with many other hosts using many different types of networking data. One of the functions of the transport layer is to identify each type of network application by assigning it a port number. For example, data requested from an HTTP web application can be identified as port 80, while data sent to an email server can be identified as port 25.

At the transport layer, on the sending host, data from the upper layers is packaged as a series of layer 4 PDUs, referred to as segments. Each segment is tagged with the application's port number. The segment is then passed to the network layer for delivery. Many different hosts could be transmitting multiple HTTP and email packets at the same time. These are multiplexed using the port numbers along with the source and destination network addresses onto the same link.



Communications at layer 4 (transport) of the OSI model. (Images © 123RF.com)

At the network and data link layers, the port number is ignored—it becomes part of the data payload and is invisible to the routers and switches that implement the addressing and forwarding functions of these layers. At the receiving host, each segment is decapsulated, identified by its port number, and passed to the relevant handler at the application layer. Put another way, the traffic stream is de-multiplexed.

The transport layer can also implement reliable data delivery mechanisms, should the application require it. Reliable delivery means that any lost or damaged packets are resent.

Devices working at the transport layer include multilayer switches—usually working as load balancers—and many types of security appliances, such as more advanced firewalls and intrusion detection systems (IDSs).

Upper Layers

The upper layers of the OSI model are less clearly associated with distinct real-world protocols. These layers collect various functions that provide useful interfaces between software applications and the transport layer.

Layer 5—Session

Most application protocols require the exchange of multiple messages between the client and server. This exchange of such a sequence of messages is called a session or dialog. The **session layer (layer 5)** represents functions that administer the process of establishing a dialog, managing data transfer, and then ending (or tearing down) the session.

Layer 6—Presentation

The **presentation layer (layer 6)** transforms data between the format required for the network and the format required for the application. For example, the presentation layer is used for character set conversion, such as between American Standard Code for Information Interchange (ASCII) and Unicode. The presentation layer can also be conceived as supporting data compression and encryption. However, in practical terms, these functions are often implemented by encryption devices and protocols running at lower layers of the stack or simply within a homogenous application layer.

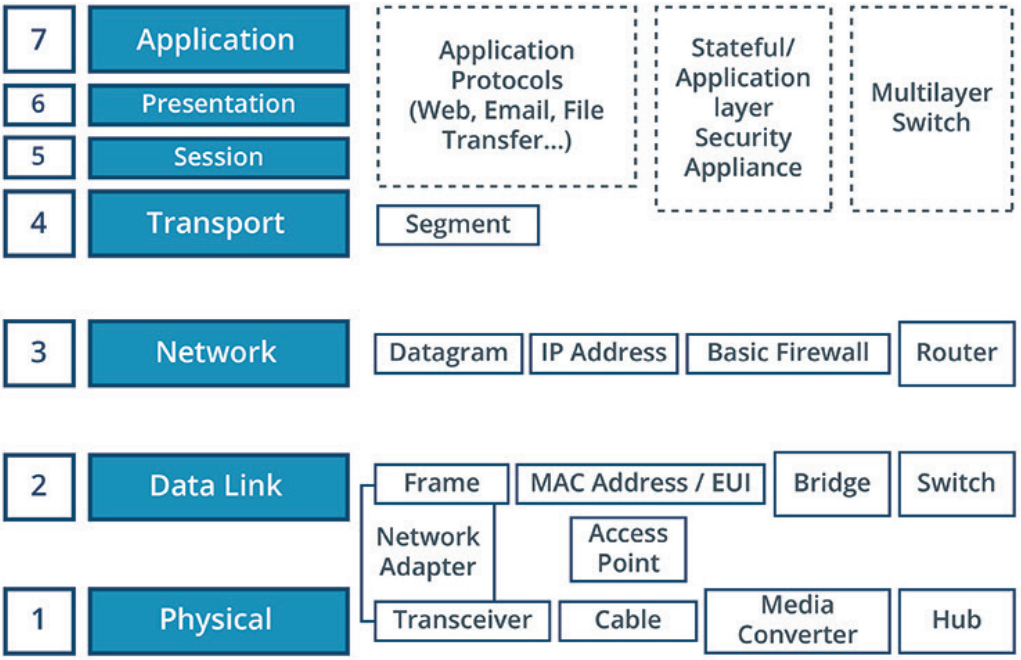
Layer 7—Application

The **application layer (layer 7)** is at the top of the OSI stack. An application-layer protocol doesn't encapsulate any other protocols or provide services to any protocol. Application-layer protocols provide an interface for software programs on network hosts that have established a communications channel through the lower-level protocols to exchange data.

More widely, upper-layer protocols provide most of the services that make a network useful, rather than just functional, including web browsing, email and communications, directory lookup, remote printing, and database services.

OSI Model Summary

The following image summarizes the OSI model, listing the PDUs at each layer, along with the types of devices that work at each layer.



Devices and concepts represented at the relevant OSI model layer.

Review Activity:

OSI Model Layers

Answer the following questions:

1. **At which OSI layer is the concept of a port number introduced?**

2. **At which layer of the OSI model is no header encapsulation applied?**

3. **What component performs signal amplification to extend the maximum allowable distance for a media type?**

4. **Which OSI layer packages bits of data from the Physical layer into frames?**

5. **True or False? The Session layer is responsible for passing data to the Network layer at the lower bound and the Presentation layer at the upper bound.**

Topic 1B

Configure SOHO Networks

EXAM OBJECTIVES COVERED

1.1 Compare and contrast the Open Systems Interconnection (OSI) model layers and encapsulation concepts.

The OSI model involves quite a lot of abstraction. As a practical example, it is worth examining how a basic network is implemented. In this topic, you will learn the connection and configuration options for components within a typical small office/home office (SOHO) router.

SOHO Routers

Networks of different sizes are classified in different ways. A network in a single location is often described as a **local area network (LAN)**. This definition encompasses many different sizes of networks with widely varying functions and capabilities. It can include both residential networks with a couple of computers, and enterprise networks with hundreds of servers and thousands of workstations.

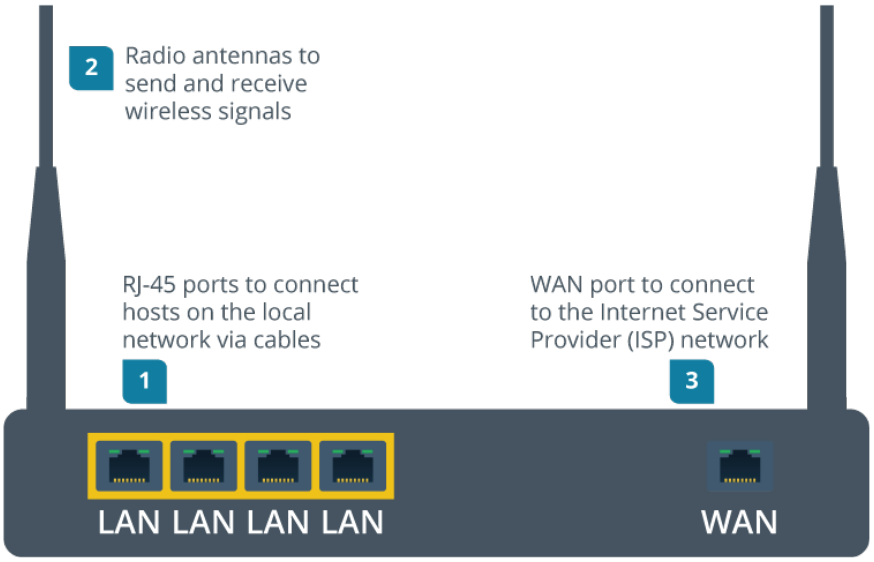
Small office/home office (SOHO) is a category of LAN with a small number of computing hosts that typically rely on a single integrated appliance for local and Internet connectivity.

Networks such as the Internet that are located in different geographic regions but with shared links are called **wide area networks (WANs)**. The intermediate system powering SOHO networks is usually described as a SOHO router because one of its primary functions is to forward traffic between the LAN and the WAN. However, routing is actually just one of its functions. We can use the OSI model to analyze each of these in turn.

Physical Layer Functions

Starting at layer 1, the SOHO router provides the following physical connections:

- A number of RJ-45 ports (typically four) to connect to a local cabled network. These are typically labeled as the LAN ports.
- Radio antennas to transmit and receive wireless signals.
- A type of modem (typically cable or digital subscriber line) to connect to the Internet Service Provider's (ISP's) network. This is typically labeled as the WAN port. On the example in the diagram, the interface is another RJ-45 port, designed to connect to a fiber to the premises Internet service using the same Ethernet technology as the local network. On other SOHO routers, there may be a different type of WAN modem, such as an RJ-11 port to connect to a digital subscriber line (DSL) service.

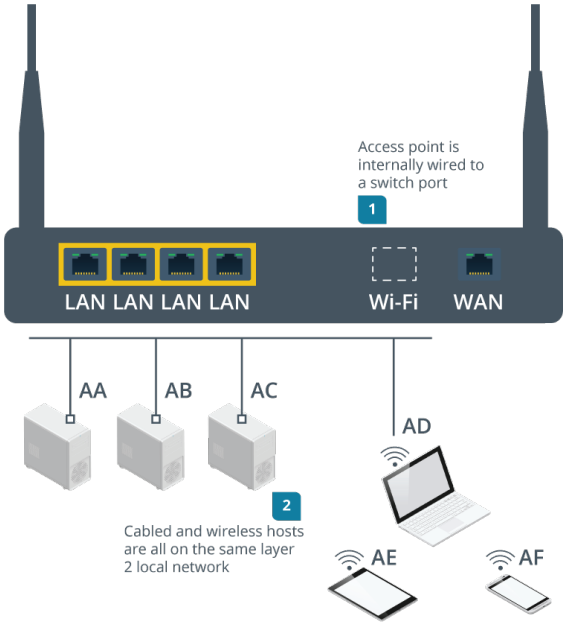


Physical layer connectivity options on a SOHO router.

Data Link Layer Functions

At layer 2, the SOHO router implements the following functions to make use of its physical layer adapters:

- **Ethernet switch**—the RJ-45 jacks are connected internally by an Ethernet switch.
- **Wireless access point**—the radio antennas implement some version of the Wi-Fi standard. The access point functions as a wireless hub, allowing stations (PCs, tablets, smartphones, and printers) to form a wireless network. The access point it also wired to the Ethernet switch via an internal port. This forms a bridge between the cabled and wireless segments, creating a single logical local network.

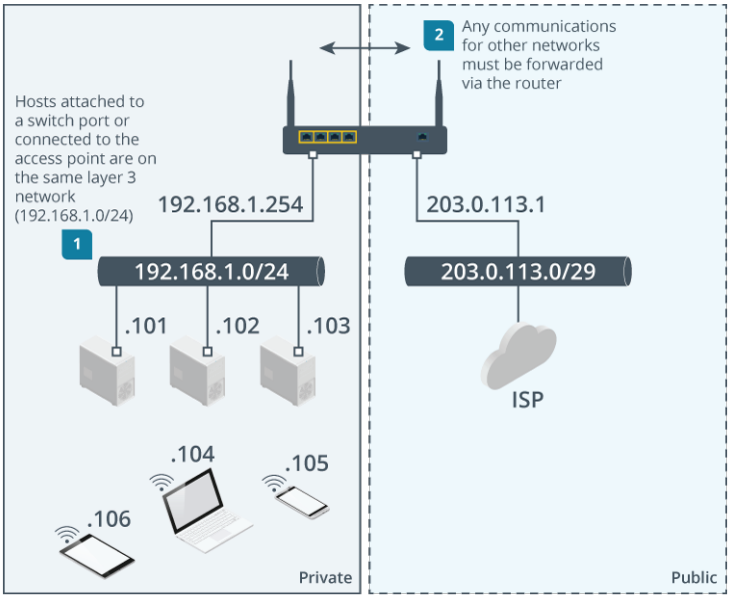


Data link layer local network segment. (Images © 123RF.com)

At this layer, each host interface is identified by a media access control (MAC) address.

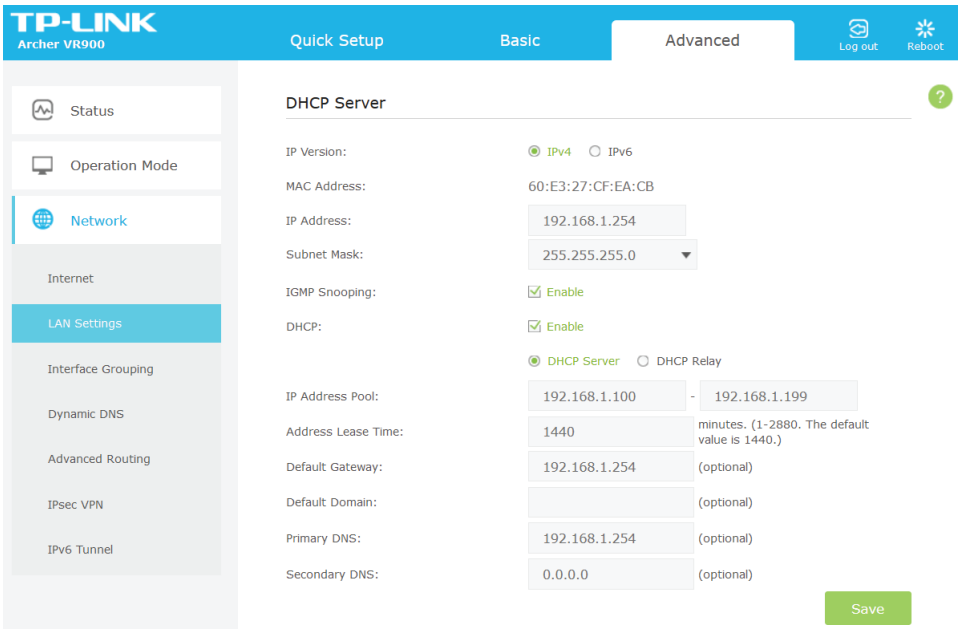
Network Layer Functions

At layer 3, the network layer, the routing part of the SOHO router makes forwarding decisions between the local private network and public Internet. These zones are distinguished by internet protocol (IP) addresses. The local network uses a private IP address range, such as `192.168.1.0/24`. The SOHO router itself is identified by an address in this range, such as `192.168.1.1` or `192.168.1.254`.



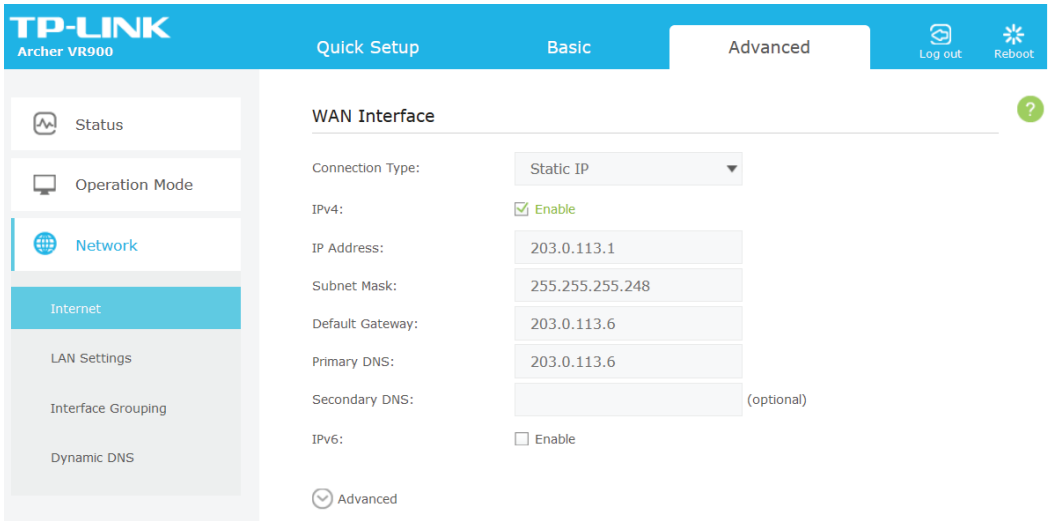
Network layer private and public segments. (Images © 123RF.com)

The router runs a dynamic host configuration protocol (DHCP) server to allocate a unique address to each host that connects to it over either an Ethernet port or via the wireless access point. The addresses assigned to clients use the same first three octets as the router's address: `192.168.1`. The last octet can be any value from 1 to 254, excluding whichever value is used by the router.



Configuring the LAN addresses using DHCP on a wireless router. (Screenshot courtesy of TP-Link Technologies Co., Ltd.)

The SOHO router's WAN interface is allocated a public IP address, say `203.0.113.1`, by the internet service provider. When a host on the local network tries to access any valid IP address outside the `192.168.1.0/24` range, the router forwards that packet over its WAN interface and directs any replies back to the host on the LAN.



Configuring the WAN (internet) interface on a wireless router. These parameters are supplied by the ISP. Many ISP services use DHCP to allocate a dynamic WAN address, but some offer static addressing. (Screenshot courtesy of TP-Link Technologies Co., Ltd.)

Transport and Application Layer and Security Functions

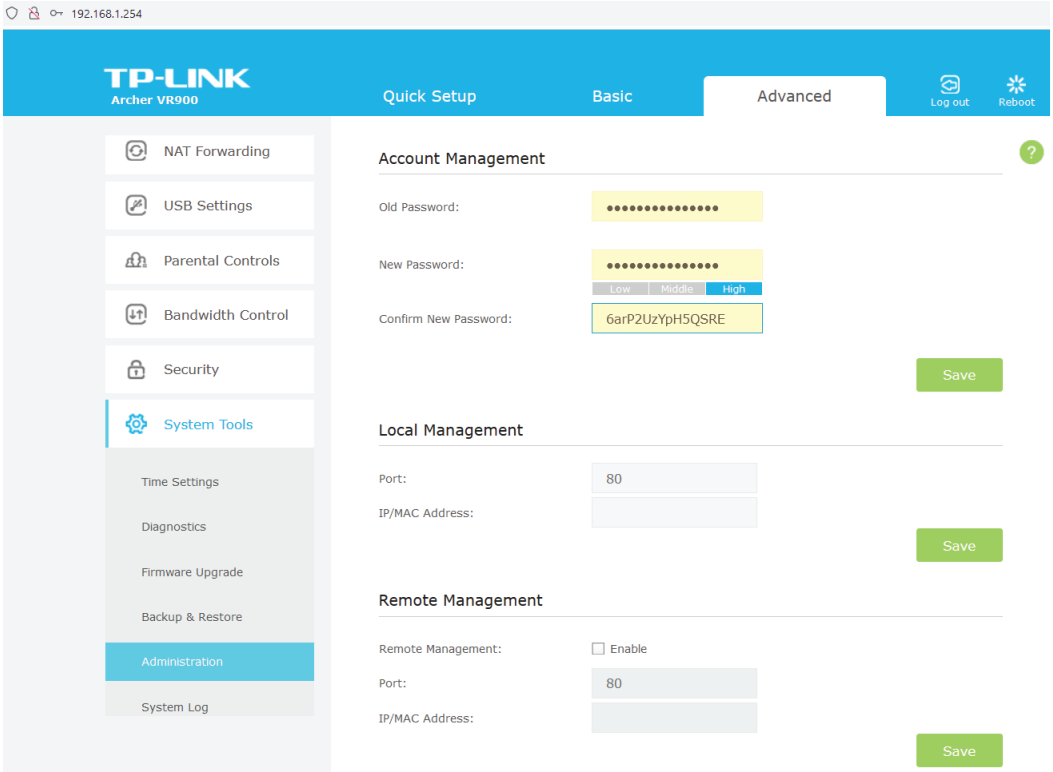
There is no separate OSI model layer for security. Instead, security issues can arise and solutions are needed at every layer. Network security is essentially a matter of allowing or preventing devices, users, and services (applications) from using the network. The WAN interface is the network perimeter. The SOHO router can apply filtering rules to traffic sent between the public and private zones, implementing a firewall. The firewall can be configured to block traffic based on source or destination IP addresses and also on the type of application.

At layer 4, each application is identified by a port number, such as 80 for hypertext transfer protocol (HTTP) web traffic or 25 for Simple Mail Transfer Protocol (SMTP) email traffic.

The firewall in the router can be configured with rules specifying behavior for each port. For example, computers on the network might use the server message block (SMB) protocol to share files. It would not be appropriate for hosts on the Internet to be able to access these shared files, so the SMB port would be blocked by default on the WAN interface but allowed on the LAN and WLAN interfaces.

Any host can connect to the RJ-45 ports on the router and join the network. The wireless network is usually protected by an encryption system that requires each station to be configured with a passphrase-based key to join the network.

Access to the router's management interface and its configuration settings is protected by an administrative account passphrase. As the router is connected to the Internet, it is critical to configure a strong passphrase.



Configuring a management interface on a wireless router. (Screenshot courtesy of TP-Link Technologies Co., Ltd.)

The Internet

The WAN interface of the router connects the SOHO network to the Internet.

The Public Switched Telephone Network

Most SOHO subscriber Internet access is facilitated via the **public switched telephone network (PSTN)**. The SOHO router is described as customer premises equipment (CPE). More widely, this is any termination and routing equipment placed at the customer site. Some of this equipment may be owned or leased from the telecommunications company (or telco); some may be owned by the customer.

The CPE is connected via its modem and WAN port to the local loop. This is cabling from the customer premises to the local exchange. The point at which the telco's cabling enters the customer premises is referred to as the demarcation point (often shortened to demarc).

Internet Service Providers

The major infrastructure of the Internet consists of high bandwidth trunks connecting Internet eXchange Points (IXPs). Within an IXP datacenter, ISPs establish links between their networks, using transit and peering arrangements to carry traffic to and from parts of the internet they do not physically own. There is a tiered hierarchy of ISPs that reflects to what extent they depend on transit arrangements with other ISPs.

Internet Standards

Although no single organization owns the Internet or its technologies, several organizations are responsible for the development of the internet and agreeing common standards and protocols.

- **Internet Assigned Numbers Authority (IANA) (iana.org)**—manages allocation of IP addresses and maintenance of the top-level domain space. IANA is currently run by Internet Corporation for Assigned Names and Numbers (ICANN). IANA allocates addresses to regional registries who then allocate them to local registries or ISPs. The regional registries are Asia/Pacific (APNIC), North America and Southern Africa (ARIN), Latin America (LACNIC), and Europe, Northern Africa, Central Asia, and the Middle East (RIPE NCC).
- **Internet Engineering Task Force (IETF) (ietf.org)**—focuses on solutions to Internet problems and the adoption of new standards, published as Requests for Comments (RFCs). Some RFCs describe network services or protocols and their implementation, while others summarize policies. An older RFC is never updated. If changes are required, a new RFC is published with a new number. Not all RFCs describe standards. Some are designated informational, while others are experimental. The official repository for RFCs is at rfc-editor.org.

References to RFCs in this course are for your information should you want to read more. You do not need to learn them for the certification exam.

The OSI model has a stricter definition of the Session, Presentation, and Application layers than is typical of actual protocols used on networks. The Internet model (tools.ietf.org/html/rfc1122) uses a simpler four layer hierarchy, with a link layer representing OSI layers 1 and 2, layer 3 referred to as the Internet layer, a Transport layer mapping approximately to layers 4 and 5, and an Application layer corresponding to layers 6 and 7.

Hexadecimal Notation

To interpret network addresses, you must understand the concept of base numbering systems. To start with the familiar; decimal numbering is also referred to as base 10. Base 10 means that each digit can have one of ten possible values (0 through 9). A digit positioned to the left of another has 10 times the value of the digit to the right. For example, the number 255 can be written out as follows:

```
(2x10x10)+(5x10)+5
```

Binary is base 2, so a digit in any given position can only have one of two values (0 or 1), and each place position is the next power of 2. The binary value 11111111 can be converted to the decimal value 255 by the following sum:

```
(1x2x2x2x2x2x2x2)+(1x2x2x2x2x2x2)+(1x2x2x2x2x2)+
(1x2x2x2x2)+(1x2x2x2)+(1x2x2)+(1x2)+1
```

As you can see, it takes 8 binary digits to represent a decimal value up to 255. This number of bits is called a byte or an octet. The four decimal numbers in the SOHO router's WAN IP address 203.0.113.1 are octets.

While computers process everything in binary, the values make for very long strings if they have to be written out or entered into configuration dialogs. Hexadecimal notation (or hex) is a convenient way of referring to the long sequences of bytes used in some other types of network addresses. Hex is base 16 with the possible values of each digit represented by the numerals 0 through 9 and the characters A, B, C, D, E, and F.

Use the following table to help to convert between decimal, binary, and hexadecimal values.

Decimal	Hexadecimal	Binary
0	0	0000
1	1	0001
2	2	0010
3	3	0011
4	4	0100
5	5	0101
6	6	0110
7	7	0111

Decimal	Hexadecimal	Binary
8	8	1000
9	9	1001
10	A	1010
11	B	1011
12	C	1100
13	D	1101
14	E	1110
15	F	1111

As you can see from the table, every hex digit lines up neatly with four binary digits (a nibble). Each byte or octet can be expressed as two hex digits. For example, the decimal value 255 is FF in hex. This would sometimes be written as 0xFF for clarity.

Review Activity:

SOHO Networks

Answer the following questions:

1. **True or false? The WAN port on a SOHO router is connected to the LAN ports by an internal switch.**

2. **What type of address is used by the switch to forward transmissions to the appropriate host?**

3. **True or false? The DHCP server in the SOHO router assigns an IP address to the WAN interface automatically.**

4. **What function or service prevents an Internet host from accessing servers on the LAN without authorization?**

5. **How is the decimal value 12 expressed in hex?**

6. **How is the decimal value 171 expressed in hex?**

Lesson 1

Summary

You should be able to compare and contrast OSI model layers and encapsulation concepts and apply them to analyzing the function of networks and networking components.

Guidelines for Comparing OSI Model Network Functions

Follow these guidelines to make effective use of the OSI model:

- Use characteristics of physical layer media and devices to plan wiring topologies and identify potential performance issues.
- Use the data link layer to plan logical segments to isolate groups of hosts for performance or security reasons.
- At the network layer, map data link segments to logical network IDs and work out rules for how hosts in one network should be permitted or denied access to other networks.
- Evaluate service requirements at the transport layer to determine which ports a host should expose.
- Use the session, presentation, and application layers to determine performance and security requirements for the services that the network is providing.

Growing Home IT-Training Curriculum

CompTia Security+ Certification (Part 4)

6429 S. Honore St, Chicago, IL 60636 | 773.549.1336
www.growinghomeinc.org

CompTIA

The Official CompTIA

Security+ Study Guide

Exam SY0-601

Official CompTIA Content Series for CompTIA Performance Certifications

The Official CompTIA Security+ Study Guide (Exam SY0-601)

Course Edition: 1.0

Acknowledgments

James Pengelly, Author

Thomas Reilly, Vice President, Learning

Katie Hoenicke, Director of Product Management

Evan Burns, Senior Manager, Learning Technology Operations and Implementation

James Chesterfield, Manager, Learning Content and Design

Becky Mann, Senior Manager, Product Development

Katherine Keyes, Content Specialist

Notices

Disclaimer

While CompTIA, Inc., takes care to ensure the accuracy and quality of these materials, we cannot guarantee their accuracy, and all materials are provided without any warranty whatsoever, including, but not limited to, the implied warranties of merchantability or fitness for a particular purpose. The use of screenshots, photographs of another entity's products, or another entity's product name or service in this book is for editorial purposes only. No such use should be construed to imply sponsorship or endorsement of the book by nor any affiliation of such entity with CompTIA. This courseware may contain links to sites on the Internet that are owned and operated by third parties (the "External Sites"). CompTIA is not responsible for the availability of, or the content located on or through, any External Site. Please contact CompTIA if you have any concerns regarding such links or External Sites.

Trademark Notice

CompTIA®, Security+®, and the CompTIA logo are registered trademarks of CompTIA, Inc., in the U.S. and other countries. All other product and service names used may be common law or registered trademarks of their respective proprietors.

Copyright Notice

Copyright © 2020 CompTIA, Inc. All rights reserved. Screenshots used for illustrative purposes are the property of the software proprietor. Except as permitted under the Copyright Act of 1976, no part of this publication may be reproduced or distributed in any form or by any means, or stored in a database or retrieval system, without the prior written permission of CompTIA, 3500 Lacey Road, Suite 100, Downers Grove, IL 60515-5439.

This book conveys no rights in the software or other products about which it was written; all use or licensing of such software or other products is the responsibility of the user according to terms and conditions of the owner. If you believe that this book, related materials, or any other CompTIA materials are being reproduced or transmitted without permission, please call 1-866-835-8020 or visit https://help.comptia.org.

Table of Contents

Lesson 1: Comparing Security Roles and Security Controls 1

Topic 1A: Compare and Contrast Information Security Roles 2

Topic 1B: Compare and Contrast Security Control and Framework Types 8

Lesson 2: Explaining Threat Actors and Threat Intelligence 17

Topic 2A: Explain Threat Actor Types and Attack Vectors 18

Topic 2B: Explain Threat Intelligence Sources 25

Lesson 3: Performing Security Assessments 35

Topic 3A: Assess Organizational Security with Network Reconnaissance Tools 36

Topic 3B: Explain Security Concerns with General Vulnerability Types 50

Topic 3C: Summarize Vulnerability Scanning Techniques 57

Topic 3D: Explain Penetration Testing Concepts 67

Lesson 4: Identifying Social Engineering and Malware 73

Topic 4A: Compare and Contrast Social Engineering Techniques 74

Topic 4B: Analyze Indicators of Malware-Based Attacks 82

Lesson 5: Summarizing Basic Cryptographic Concepts 95

Topic 5A: Compare and Contrast Cryptographic Ciphers 96

Topic 5B: Summarize Cryptographic Modes of Operation 104

Topic 5C: Summarize Cryptographic Use Cases and Weaknesses 111

Topic 5D: Summarize Other Cryptographic Technologies 120

Lesson 6: Implementing Public Key Infrastructure 125

Topic 6A: Implement Certificates and Certificate Authorities 126

Topic 6B: Implement PKI Management 137

Lesson 7: Implementing Authentication Controls 147
Topic 7A: Summarize Authentication Design Concepts 148
Topic 7B: Implement Knowledge-Based Authentication 154
Topic 7C: Implement Authentication Technologies 164
Topic 7D: Summarize Biometrics Authentication Concepts 172

Lesson 8: Implementing Identity and Account Management Controls 179
Topic 8A: Implement Identity and Account Types 180
Topic 8B: Implement Account Policies 191
Topic 8C: Implement Authorization Solutions 199
Topic 8D: Explain the Importance of Personnel Policies 208

Lesson 9: Implementing Secure Network Designs 215
Topic 9A: Implement Secure Network Designs 216
Topic 9B: Implement Secure Switching and Routing 227
Topic 9C: Implement Secure Wireless Infrastructure 235
Topic 9D: Implement Load Balancers 247

Lesson 10: Implementing Network Security Appliances 255
Topic 10A: Implement Firewalls and Proxy Servers 256
Topic 10B: Implement Network Security Monitoring 268
Topic 10C: Summarize the Use of SIEM 275

Lesson 11: Implementing Secure Network Protocols 283
Topic 11A: Implement Secure Network Operations Protocols 284
Topic 11B: Implement Secure Application Protocols 292
Topic 11C: Implement Secure Remote Access Protocols 301

Lesson 12: Implementing Host Security Solutions 317
Topic 12A: Implement Secure Firmware 318
Topic 12B: Implement Endpoint Security 325
Topic 12C: Explain Embedded System Security Implications 331

Lesson 13: Implementing Secure Mobile Solutions 343

Topic 13A: Implement Mobile Device Management 344

Topic 13B: Implement Secure Mobile Device Connections 356

Lesson 14: Summarizing Secure Application Concepts 365

Topic 14A: Analyze Indicators of Application Attacks 366

Topic 14B: Analyze Indicators of Web Application Attacks..... 372

Topic 14C: Summarize Secure Coding Practices 383

Topic 14D: Implement Secure Script Environments 390

Topic 14E: Summarize Deployment and Automation Concepts 399

Lesson 15: Implementing Secure Cloud Solutions 407

Topic 15A: Summarize Secure Cloud and Virtualization Services 408

Topic 15B: Apply Cloud Security Solutions..... 418

Topic 15C: Summarize Infrastructure as Code Concepts 429

Lesson 16: Explaining Data Privacy and Protection Concepts..... 437

Topic 16A: Explain Privacy and Data Sensitivity Concepts..... 438

Topic 16B: Explain Privacy and Data Protection Controls..... 447

Lesson 17: Performing Incident Response 455

Topic 17A: Summarize Incident Response Procedures..... 456

Topic 17B: Utilize Appropriate Data Sources for Incident Response 465

Topic 17C: Apply Mitigation Controls..... 475

Lesson 18: Explaining Digital Forensics..... 483

Topic 18A: Explain Key Aspects of Digital Forensics Documentation 484

Topic 18B: Explain Key Aspects of Digital Forensics Evidence Acquisition 490

Lesson 19: Summarizing Risk Management Concepts 499

Topic 19A: Explain Risk Management Processes and Concepts 500

Topic 19B: Explain Business Impact Analysis Concepts..... 508

Lesson 20: Implementing Cybersecurity Resilience 515

Topic 20A: Implement Redundancy Strategies..... 516

Topic 20B: Implement Backup Strategies 522

Topic 20C: Implement Cybersecurity Resiliency Strategies..... 530

Lesson 21: Explaining Physical Security 539

Topic 21A: Explain the Importance of Physical Site Security Controls 540

Topic 21B: Explain the Importance of Physical Host Security Controls..... 548

Appendix A: Mapping Course Content to CompTIA Security+ (Exam SY0-601) A-1

Solutions S-1

Glossary.....G-1

Index.....I-1

About This Course

CompTIA is a not-for-profit trade association with the purpose of advancing the interests of IT professionals and IT channel organizations and its industry-leading IT certifications are an important part of that mission. CompTIA's Security+ certification is a foundation-level certificate designed for IT administrators with two years' experience whose job role is focused on system security.

The CompTIA Security+ exam will certify the successful candidate has the knowledge and skills required to assist with cybersecurity duties in small and large organizations. These duties include assessments and monitoring; secure network, host, app, and cloud provisioning; data governance; and incident analysis and response.

> *CompTIA Security+ is the first security certification IT professionals should earn. It establishes the core knowledge required of any cybersecurity role and provides a springboard to intermediate-level cybersecurity jobs. Security+ incorporates best practices in hands-on troubleshooting to ensure security professionals have practical security problem-solving skills. Cybersecurity professionals with Security+ know how to address security incidents—not just identify them.*
>
> *Security+ is compliant with ISO 17024 standards and approved by the US DoD to meet directive 8140/8570.01-M requirements. Regulators and government rely on ANSI accreditation because it provides confidence and trust in the outputs of an accredited program.*
>
> comptia.org/certifications/security

Course Description

Course Objectives

This course can benefit you in two ways. If you intend to pass the CompTIA Security+ (Exam SY0-601) certification examination, this course can be a significant part of your preparation. But certification is not the only key to professional success in the field of computer security. Today's job market demands individuals with demonstrable skills, and the information and activities in this course can help you build your cybersecurity skill set so that you can confidently perform your duties in any entry-level security role.

On course completion, you will be able to:

- Compare security roles and security controls
- Explain threat actors and threat intelligence
- Perform security assessments and identify social engineering attacks and malware types
- Summarize basic cryptographic concepts and implement public key infrastructure
- Implement authentication controls
- Implement identity and account management controls
- Implement secure network designs, network security appliances, and secure network protocols
- Implement host, embedded/Internet of Things, and mobile security solutions
- Implement secure cloud solutions

- Explain data privacy and protection concepts
- Perform incident response and digital forensics
- Summarize risk management concepts and implement cybersecurity resilience
- Explain physical security

Target Student

The Official CompTIA Security+ Guide (Exam SY0-601) is the primary course you will need to take if your job responsibilities include securing network services, devices, and data confidentiality/privacy in your organization. You can take this course to prepare for the CompTIA Security+ (Exam SY0-601) certification examination.

Prerequisites

- To ensure your success in this course, you should have basic Windows and Linux administrator skills and the ability to implement fundamental networking appliances and IP addressing concepts. CompTIA A+ and Network+ certifications, or equivalent knowledge, and six to nine months' experience in networking, including configuring security parameters, are strongly recommended.

The prerequisites for this course might differ significantly from the prerequisites for the CompTIA certification exams. For the most up-to-date information about the exam prerequisites, complete the form on this page: comptia.org/training/resources/exam-objectives

How to Use the Study Notes

The following notes will help you understand how the course structure and components are designed to support mastery of the competencies and tasks associated with the target job roles and help you to prepare to take the certification exam.

As You Learn

At the top level, this course is divided into **lessons,** each representing an area of competency within the target job roles. Each lesson is composed of a number of topics. A **topic** contains subjects that are related to a discrete job task, mapped to objectives and content examples in the CompTIA exam objectives document. Rather than follow the exam domains and objectives sequence, lessons and topics are arranged in order of increasing proficiency. Each topic is intended to be studied within a short period (typically 30 minutes at most). Each topic is concluded by one or more activities, designed to help you to apply your understanding of the study notes to practical scenarios and tasks.

Additional to the study content in the lessons, there is a glossary of the terms and concepts used throughout the course. There is also an index to assist in locating particular terminology, concepts, technologies, and tasks within the lesson and topic content.

In many electronic versions of the book, you can click links on key words in the topic content to move to the associated glossary definition, and on page references in the index to move to that term in the content. To return to the previous location in the document after clicking a link, use the appropriate functionality in your eBook viewing software.

Watch throughout the material for the following visual cues.

Student Icon	Student Icon Descriptive Text
	A **Note** provides additional information, guidance, or hints about a topic or task.
	A **Caution** note makes you aware of places where you need to be particularly careful with your actions, settings, or decisions so that you can be sure to get the desired results of an activity or task.

As You Review

Any method of instruction is only as effective as the time and effort you, the student, are willing to invest in it. In addition, some of the information that you learn in class may not be important to you immediately, but it may become important later. For this reason, we encourage you to spend some time reviewing the content of the course after your time in the classroom.

Following the lesson content, you will find a table mapping the lessons and topics to the exam domains, objectives, and content examples. You can use this as a checklist as you prepare to take the exam, and review any content that you are uncertain about.

As a Reference

The organization and layout of this book make it an easy-to-use resource for future reference. Guidelines can be used during class and as after-class references when you're back on the job and need to refresh your understanding. Taking advantage of the glossary, index, and table of contents, you can use this book as a first source of definitions, background information, and summaries.

Lesson 1

Comparing Security Roles and Security Controls

LESSON INTRODUCTION

Security is an ongoing process that includes assessing requirements, setting up organizational security systems, hardening them, monitoring them, responding to attacks in progress, and deterring attackers. As a security professional, it is important that you understand how the security function is implemented as departments or units and professional roles within different types of organizations. You must also be able to explain the importance of compliance factors and best practice frameworks in driving the selection of security controls.

Lesson Objectives

In this lesson, you will:

- Compare and contrast information security roles.
- Compare and contrast security control and framework types.

Topic 1A

Compare and Contrast Information Security Roles

EXAM OBJECTIVES COVERED

This topic provides background information about the role of security professionals and does not cover a specific exam objective.

To be successful and credible as a security professional, you should understand security in business starting from the ground up. You should also know the key security terms and ideas used by other security experts in technical documents and in trade publications. Security implementations are constructed from fundamental building blocks, just like a large building is constructed from individual bricks. This topic will help you understand those building blocks so that you can use them as the foundation for your security career.

Information Security

Information security (or infosec) refers to the protection of data resources from unauthorized access, attack, theft, or damage. Data may be vulnerable because of the way it is stored, the way it is transferred, or the way it is processed. The systems used to store, transmit, and process data must demonstrate the properties of security. Secure information has three properties, often referred to as the **CIA Triad**:

- **Confidentiality** means that certain information should only be known to certain people.
- **Integrity** means that the data is stored and transferred as intended and that any modification is authorized.
- **Availability** means that information is accessible to those authorized to view or modify it.

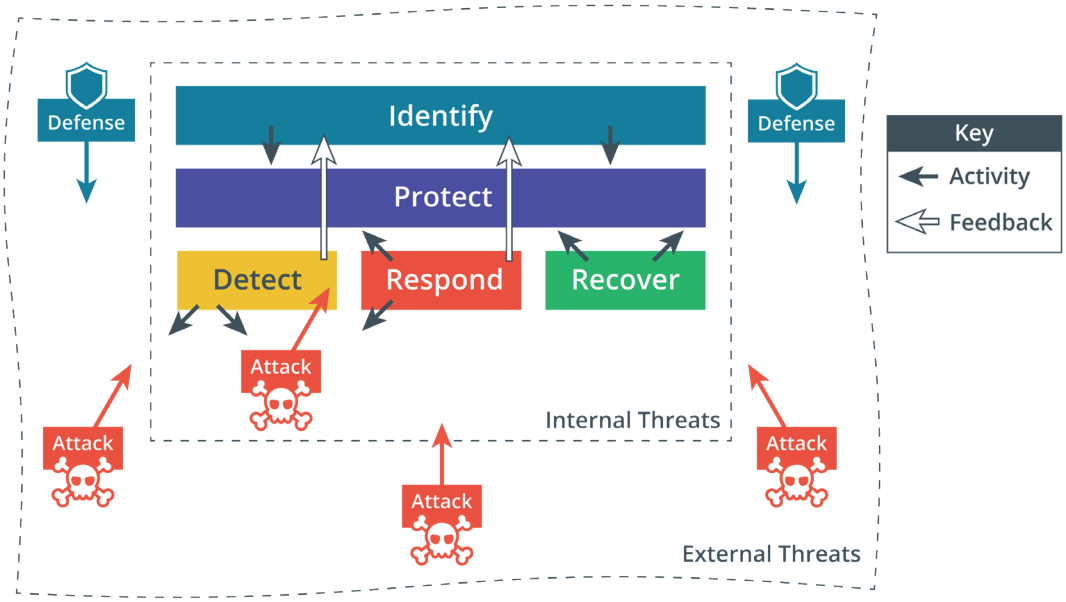
The triad can also be referred to as "AIC" to avoid confusion with the Central Intelligence Agency.

Some security models and researchers identify other properties that secure systems should exhibit. The most important of these is non-repudiation. **Non-repudiation** means that a subject cannot deny doing something, such as creating, modifying, or sending a resource. For example, a legal document, such as a will, must usually be witnessed when it is signed. If there is a dispute about whether the document was correctly executed, the witness can provide evidence that it was.

Cybersecurity Framework

Within the goal of ensuring information security, cybersecurity refers specifically to provisioning secure processing hardware and software. Information security and cybersecurity tasks can be classified as five functions, following the framework developed by the **National Institute of Standards and Technology (NIST)** (nist.gov/cyberframework/online-learning/five-functions):

- Identify—develop security policies and capabilities. Evaluate risks, threats, and vulnerabilities and recommend security controls to mitigate them.
- Protect—procure/develop, install, operate, and decommission IT hardware and software assets with security as an embedded requirement of every stage of this operations life cycle.
- Detect—perform ongoing, proactive monitoring to ensure that controls are effective and capable of protecting against new types of threats.
- Respond—identify, analyze, contain, and eradicate threats to systems and data security.
- Recover—implement cybersecurity resilience to restore systems and data if other controls are unable to prevent attacks.



Core cybersecurity tasks.

Information Security Competencies

IT professionals working in a role with security responsibilities must be competent in a wide range of disciplines, from network and application design to procurement and human resources (HR). The following activities might be typical of such a role:

- Participate in risk assessments and testing of security systems and make recommendations.
- Specify, source, install, and configure secure devices and software.
- Set up and maintain document access control and user privilege profiles.

- Monitor audit logs, review user privileges, and document access controls.
- Manage security-related incident response and reporting.
- Create and test business continuity and disaster recovery plans and procedures.
- Participate in security training and education programs.

Information Security Roles and Responsibilities

A security policy is a formalized statement that defines how security will be implemented within an organization. It describes the means the organization will take to protect the confidentiality, availability, and integrity of sensitive data and resources. It often consists of multiple individual policies. The implementation of a security policy to support the goals of the CIA triad might be very different for a school, a multinational accountancy firm, or a machine tool manufacturer. However, each of these organizations, or any other organization (in any sector of the economy, whether profit-making or non-profit-making) should have the same interest in ensuring that its employees, equipment, and data are secure against attack or damage.

As part of the process of adopting an effective organizational security posture, employees must be aware of their responsibilities. The structure of security responsibilities will depend on the size and hierarchy of an organization, but these roles are typical.

- Overall internal responsibility for security might be allocated to a dedicated department, run by a Director of Security, Chief Security Officer (CSO), or **Chief Information Security Officer (CISO)**. Historically, responsibility for security might have been allocated to an existing business unit, such as Information and Communications Technology (ICT) or accounting.

  However, the goals of a network manager are not always well-aligned with the goals of security; network management focuses on availability over confidentiality. Consequently, security is increasingly thought of as a dedicated function or business unit with its own management structure.

- Managers may have responsibility for a domain, such as building control, ICT, or accounting.
- Technical and specialist staff have responsibility for implementing, maintaining, and monitoring the policy. Security might be made a core competency of systems and network administrators, or there may be dedicated security administrators. One such job title is **Information Systems Security Officer (ISSO)**.
- Non-technical staff have the responsibility of complying with policy and with any relevant legislation.
- External responsibility for security (due care or liability) lies mainly with directors or owners, though again it is important to note that all employees share some measure of responsibility.

NIST's National Initiative for Cybersecurity Education (NICE) categorizes job tasks and job roles within the cybersecurity industry (gov/itl/applied-cybersecurity/nice/nice-framework-resource-center).

Information Security Business Units

The following units are ofen used to represent the security function within the organizational hierarchy.

Security Operations Center (SOC)

A **security operations center (SOC)** is a location where security professionals monitor and protect critical information assets across other business functions, such as finance, operations, sales/marketing, and so on. Because SOCs can be difficult to establish, maintain, and finance, they are usually employed by larger corporations, like a government agency or a healthcare company.

IBM Security Headquarters in Cambridge MA. (Image credit: John Mattern/Feature Photo Service for IBM.)

DevSecOps

Network operations and use of cloud computing make ever-increasing use of automation through software code. Traditionally, software code would be the responsibility of a programming or development team. Separate development and operations departments or teams can lead to silos, where each team does not work effectively with the other.

Development and operations (DevOps) is a cultural shift within an organization to encourage much more collaboration between developers and system administrators. By creating a highly orchestrated environment, IT personnel and developers can build, test, and release software faster and more reliably. Many consider a DevOps approach to administration as the only way organizations can take full advantage of the potential benefits offered by cloud service providers.

DevSecOps extends the boundary to security specialists and personnel, reflecting the principle that security is a primary consideration at every stage of software development and deployment. This is also known as shift left, meaning that security considerations need to be made during requirements and planning phases, not grafted on at the end. The principle of DevSecOps recognizes this and shows that security expertise must be embedded into any development project. Ancillary to this is the recognition that security operations can be conceived of as software development projects. Security tools can be automated through code. Consequently, security operations need to take on developer expertise to improve detection and monitoring.

Incident Response

A dedicated **cyber incident response team (CIRT)**/computer security incident response team (CSIRT)/computer emergency response team (CERT) as a single point-of-contact for the notification of security incidents. This function might be handled by the SOC or it might be established as an independent business unit.

Review Activity:

Information Security Roles

Answer the following questions:

1. **What are the properties of a secure information processing system?**

2. **What term is used to describe the property of a secure network where a sender cannot deny having sent a message?**

3. **A multinational company manages a large amount of valuable intellectual property (IP) data, plus personal data for its customers and account holders. What type of business unit can be used to manage such important and complex security requirements?**

4. **A business is expanding rapidly and the owner is worried about tensions between its established IT and programming divisions. What type of security business unit or function could help to resolve these issues?**

Topic 1B

Compare and Contrast Security Control and Framework Types

EXAM OBJECTIVES COVERED

5.1 Compare and contrast various types of controls
5.2 Explain the importance of applicable regulations, standards, or frameworks that impact organizational security posture

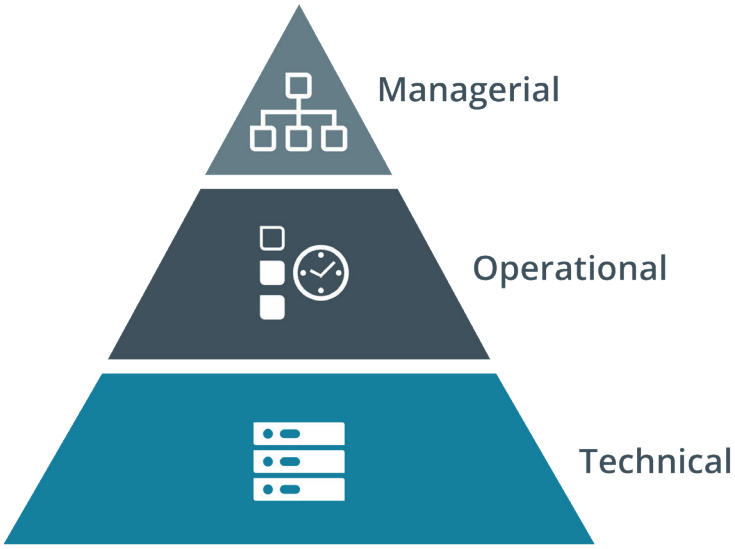
Information security and cybersecurity assurance is met by implementing security controls. As an information security professional, you must be able to compare types of security controls. You should also be able to describe how frameworks influence the selection and configuration of controls. By identifying basic security control types and how key frameworks and legislation drive compliance, you will be better prepared to select and implement the most appropriate controls for a given scenario.

Security Control Categories

Information and cybersecurity assurance is usually considered to take place within an overall process of business risk management. Implementation of cybersecurity functions is often the responsibility of the IT department. There are many different ways of thinking about how IT services should be governed to fulfill overall business needs. Some organizations have developed IT service frameworks to provide best practice guides to implementing IT and cybersecurity. These frameworks can shape company policies and provide checklists of procedures, activities, and technologies that should ideally be in place. Collectively, these procedures, activities, and tools can be referred to as security controls.

A **security control** is something designed to make give a system or data asset the properties of confidentiality, integrity, availability, and non-repudiation. Controls can be divided into three broad categories, representing the way the control is implemented:

- **Technical**—the control is implemented as a system (hardware, software, or firmware). For example, firewalls, anti-virus software, and OS access control models are technical controls. Technical controls may also be described as logical controls.
- **Operational**—the control is implemented primarily by people rather than systems. For example, security guards and training programs are operational controls rather than technical controls.
- **Managerial**—the control gives oversight of the information system. Examples could include risk identification or a tool allowing the evaluation and selection of other security controls.



Categories of security controls.

Although it uses a more complex scheme, it is worth being aware of the way the National Institute of Standards and Technology (NIST) classifies security controls (nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf).

Security Control Functional Types

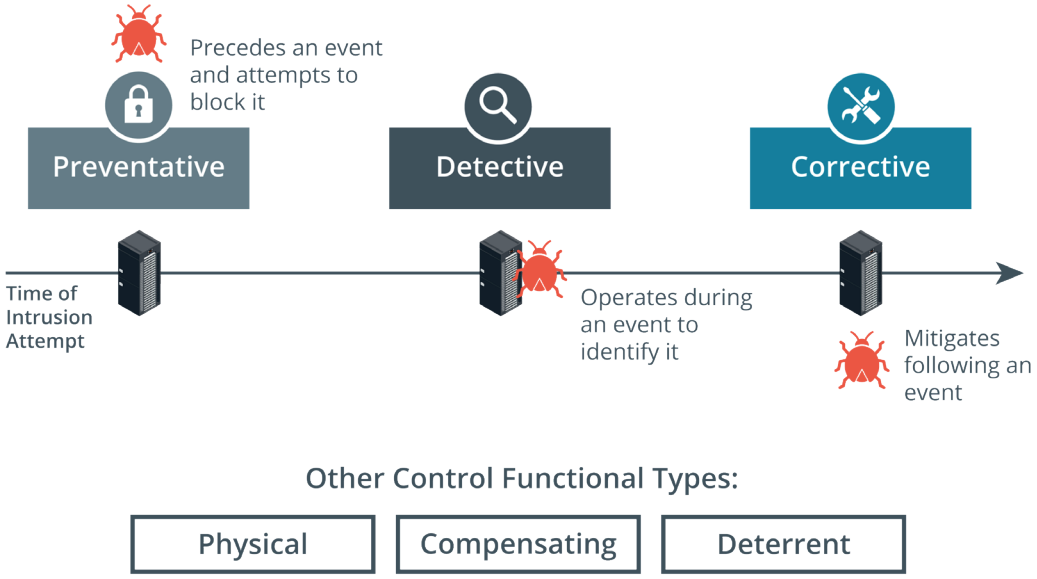
Security controls can also be classified in types according to the goal or function they perform:

- Preventive—the control acts to eliminate or reduce the likelihood that an attack can succeed. A preventative control operates before an attack can take place. **Access control lists (ACL)** configured on firewalls and file system objects are preventative-type controls. Anti-malware software also acts as a preventative control, by blocking processes identified as malicious from executing. Directives and standard operating procedures (SOPs) can be thought of as administrative versions of preventative controls.
- **Detective**—the control may not prevent or deter access, but it will identify and record any attempted or successful intrusion. A detective control operates during the progress of an attack. Logs provide one of the best examples of detective-type controls.
- **Corrective**—the control acts to eliminate or reduce the impact of an intrusion event. A corrective control is used after an attack. A good example is a backup system that can restore data that was damaged during an intrusion. Another example is a patch management system that acts to eliminate the vulnerability exploited during the attack.

While most controls can be classed functionally as preventative, detective, or corrective, a few other types can be used to define other cases:

- **Physical**—Controls such as alarms, gateways, locks, lighting, security cameras, and guards that deter and detect access to premises and hardware are often classed separately.

- **Deterrent**—The control may not physically or logically prevent access, but psychologically discourages an attacker from attempting an intrusion. This could include signs and warnings of legal penalties against trespass or intrusion.
- **Compensating**—The control serves as a substitute for a principal control, as recommended by a security standard, and affords the same (or better) level of protection but uses a different methodology or technology.



Functional types of security controls. (Images © 123RF.com.)

NIST Cybersecurity Framework

A **cybersecurity framework (CSF)** is a list of activities and objectives undertaken to mitigate risks. The use of a framework allows an organization to make an objective statement of its current cybersecurity capabilities, identify a target level of capability, and prioritize investments to achieve that target. This is valuable for giving a structure to internal risk management procedures and provides an externally verifiable statement of regulatory compliance. Frameworks are also important because they save an organization from building its security program in a vacuum, or from building the program on a foundation that fails to account for important security concepts.

There are many different frameworks, each of which categorize cybersecurity activities and controls in slightly different ways. These frameworks are non-regulatory in the sense that they do not attempt to address the specific regulations of a specific industry but represent "best practice" in IT security governance generally. Most organizations will have historically chosen a particular framework; some may use multiple frameworks in conjunction.

Most frameworks are developed for an international audience; others are focused on a domestic national audience. Most of the frameworks are associated with certification programs to show that staff and consultants can apply the methodologies successfully.

The National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) is a relatively new addition to the IT governance space and distinct from other frameworks by focusing exclusively on IT security, rather than IT service provision more generally (nist.gov/cyberframework). It is developed for a US audience and focuses somewhat on US government, but its recommendations can be adapted for other countries and types of organizations.

NIST's Risk Management Framework (RMF) pre-dates the CSF. Where the CSF focuses on practical cybersecurity for businesses, the RMF is more prescriptive and principally intended for use by federal agencies (csrc.nist.gov/projects/risk-management/rmf-overview).

As well as its cybersecurity and risk frameworks, NIST is responsible for issuing the Federal Information Processing Standards (FIPS) plus advisory guides called Special Publications (csrc.nist.gov/publications/sp). Many of the standards and technologies covered in CompTIA Security+ are discussed in these documents.

ISO and Cloud Frameworks

International Organization for Standardization (ISO) 27K

The International Organization for Standardization (ISO) has produced a cybersecurity framework in conjunction with the International Electrotechnical Commission (IEC). The framework was established in 2005 and revised in 2013. Unlike the NIST framework, the ISO 27001 Information Security Management standard must be purchased (iso.org/standard/54534.html). **ISO 27001** is part of an overall 27000 series of information security standards, also known as 27K. Of these, 27002 classifies security controls, 27017 and 27018 reference cloud security, and 27701 focuses on personal data and privacy.

ISO 31K

Where ISO 21K is a cybersecurity framework, **ISO 31K** (iso.org/iso-31000-risk-management.html) is an overall framework for enterprise risk management (ERM). ERM considers risks and opportunities beyond cybersecurity by including financial, customer service, competition, and legal liability factors. ISO 31K establishes best practices for performing risk assessments.

Cloud Security Alliance

The not-for-profit organization **Cloud Security Alliance (CSA)** produces various resources to assist cloud service providers (CSP) in setting up and delivering secure cloud platforms. These resources can also be useful for cloud consumers in evaluating and selecting cloud services.

- Security Guidance (cloudsecurityalliance.org/research/guidance)—a best practice summary analyzing the unique challenges of cloud environments and how on-premises controls can be adapted to them.
- Enterprise reference architecture (ea.cloudsecurityalliance.org)—best practice methodology and tools for CSPs to use in architecting cloud solutions. The solutions are divided across a number of domains, such as risk management and infrastructure, application, and presentation services.
- Cloud controls matrix (cloudsecurityalliance.org/research/working-groups/cloud-controls-matrix)—lists specific controls and assessment guidelines that should be implemented by CSPs. For cloud consumers, the matrix acts as a starting point for cloud contracts and agreements as it provides a baseline level of security competency that the CSP should meet.

Statements on Standards for Attestation Engagements (SSAE) Service Organization Control (SOC)

The **Statements on Standards for Attestation Engagements (SSAE)** are audit specifications developed by the American Institute of Certified Public Accountants

(AICPA). These audits are designed to assure consumers that service providers—notably cloud providers, but including any type of hosted or third-party service—meet professional standards (aicpa.org/interestareas/frc/assuranceadvisoryservices/serviceorganization-smanagement.html). Within SSAE No. 18 (the current specification), there are several levels of reporting:

- Service Organization Control (SOC2)— evaluates the internal controls implemented by the service provider to ensure compliance with Trust Services Criteria (TSC) when storing and processing customer data. TSC refers to security, confidentiality, integrity, availability, and privacy properties. An SOC2 Type I report assesses the system design, while a Type II report assesses the ongoing effectiveness of the security architecture over a period of 6-12 months. SOC2 reports are highly detailed and designed to be restricted. They should only be shared with the auditor and regulators and with important partners under non disclosure agreement (NDA) terms.
- SOC3—a less detailed report certifying compliance with SOC2. SOC3 reports can be freely distributed.

Benchmarks and Secure Configuration Guides

Although a framework gives a "high-level" view of how to plan IT services, it does not generally provide detailed implementation guidance. At a system level, the deployment of servers and applications is covered by benchmarks and secure configuration guides.

Center for Internet Security (CIS)

The **Center for Internet Security** (cisecurity.org) is a not-for-profit organization (founded partly by The SANS Institute). It publishes the well-known "The 20 CIS Controls." The CIS-RAM (Risk Assessment Method) can be used to perform an overall evaluation of security posture (learn.cisecurity.org/cis-ram).

CIS also produces **benchmarks** for different aspects of cybersecurity. For example, there are benchmarks for compliance with IT frameworks and compliance programs, such as **PCI DSS**, NIST 800-53, SOX, and ISO 27000. There are also product-focused benchmarks, such as for Windows Desktop, Windows Server, macOS, Linux, Cisco, web browsers, web servers, database and email servers, and VMware ESXi. The CIS-CAT (Configuration Access Tool) can be used with automated vulnerability scanners to test compliance against these benchmarks (cisecurity.org/cybersecurity-tools/cis-cat-pro/cis-cat-faq).

OS/Network Appliance Platform/Vendor-specific Guides

Operating system (OS) best practice configuration lists the settings and controls that should be applied for a computing platform to work in a defined roles, such as client workstation, authentication server, network switch/router/firewall, web/application server, and so on.

Most vendors will provide guides, templates, and tools for configuring and validating the deployment of network appliances, operating systems, web servers, and application/database servers. The security configurations for each of these devices will vary not only by vendor but by device and version as well. The vendor's support portal will host the configuration guides (along with setup/install guides and software downloads and updates) or they can be easily located using a web search engine.

There is also detailed guidance available from several organizations to cover both vendor-neutral deployments and to provide third-party assessment and advice on deploying vendor products. Apart from the CIS controls, some notable sources include:

- Department of Defense Cyber Exchange provides Security Technical Implementation Guides (STIGs) with hardening guidelines for a variety of software and hardware solutions (public.cyber.mil).

- National Checklist Program (NCP) by NIST provides checklists and benchmarks for a variety of operating systems and applications (nvd.nist.gov/ncp/repository).

Application Servers

Most application architectures use a client/server model. This means that part of the application is a client software program, installed and run on separate hardware to the server application code. The client interacts with the server over a network. Attacks can therefore be directed at the local client code, at the server application, or at the network channel between them. As well as coding issues, the applications need to take account of platform issues. The client application might be running in a computing host alongside other, potentially malicious, software. Code that runs on the client should not be trusted. The server-side code should implement routines to verify that input conforms to what is expected.

Web Server Applications

A web application is a particular type of client/server architecture. A web application leverages existing technologies to simplify development. The application uses a generic client (a web browser), and standard network protocols and servers (HTTP/HTTPS). The specific features of the application are developed using code running on the clients and servers. Web applications are also likely to use a multi-tier architecture, where the server part is split between application logic and data storage and retrieval. Modern web applications may use even more distributed architectures, such as microservices and serverless.

The **Open Web Application Security Project (OWASP)** is a not-for-profit, online community that publishes several secure application development resources, such as the Top 10 list of the most critical application security risks (owasp.org/www-project-top-ten). OWASP has also developed resources, such as the Zed Attack Proxy and Juice Shop (a deliberately unsecure web application), to help investigate and understand penetration testing and application security issues.

Regulations, Standards, and Legislation

The key frameworks, benchmarks, and configuration guides may be used to demonstrate compliance with a country's legal/regulatory requirements or with industry-specific regulations. *Due diligence* is a legal term meaning that responsible persons have not been negligent in discharging their duties. Negligence may create criminal and civil liabilities. Many countries have enacted legislation that criminalizes negligence in information management. In the US, for example, the **Sarbanes-Oxley Act (SOX)** mandates the implementation of risk assessments, internal controls, and audit procedures. The Computer Security Act (1987) requires federal agencies to develop security policies for computer systems that process confidential information. In 2002, the Federal Information Security Management Act (FISMA) was introduced to govern the security of data processed by federal government agencies.

Some regulations have specific cybersecurity control requirements; others simply mandate "best practice," as represented by a particular industry or international framework. It may be necessary to perform mapping between different industry frameworks, such as NIST and ISO 27K, if a regulator specifies the use of one but not another. Conversely, the use of frameworks may not be mandated as such, but auditors are likely to expect them to be in place as a demonstration of a strong and competent security program.

Personal Data and the General Data Protection Regulation (GDPR)

Where some types of legislation address cybersecurity due diligence, others focus in whole or in part on information security as it affects privacy or personal data. Privacy

is a distinct concept from security. Privacy requires that collection and processing of personal information be both secure and fair. Fairness and the right to privacy, as enacted by regulations such as the European Union's **General Data Protection Regulation (GDPR)**, means that personal data cannot be collected, processed, or retained without the individual's informed consent. *Informed consent* means that the data must be collected and processed only for the stated purpose, and that purpose must be clearly described to the user in plain language, not legalese. GDPR (ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr) gives data subjects rights to withdraw consent, and to inspect, amend, or erase data held about them.

National, Territory, or State Laws

Compliance issues are complicated by the fact that laws derive from different sources. For example, the GDPR does not apply to American data subjects, but it does apply to American companies that collect or process the personal data of people in EU countries. In the US, there are national federal laws, state laws, plus a body of law applying to US territories (Puerto Rico, the US Virgin Islands, Guam, and American Samoa). Federal laws tend to focus either on regulations like FISMA for federal departments or as "vertical" laws affecting a particular industry. Examples of the latter include the **Gramm–Leach–Bliley Act (GLBA)** for financial services, and the Health Insurance Portability and Accountability Act (HIPAA).

Some states have started to introduce "horizontal" personal data regulations, similar to the approach taken by the GDPR. One high-profile example of state legislation is the California Consumer Privacy Act (CCPA) (csoonline.com/article/3292578/california-consumer-privacy-act-what-you-need-to-know-to-be-compliant.html).

Varonis' blog contains a useful overview of privacy laws in the US (varonis.com/blog/us-privacy-laws).

Payment Card Industry Data Security Standard (PCI DSS)

Compliance issues can also arise from industry-mandated regulations. For example, the Payment Card Industry Data Security Standard (PCI DSS) defines the safe handling and storage of financial information (pcisecuritystandards.org/pci_security).

Review Activity:

Security Control and Framework Types

Answer the following questions:

1. **You have implemented a secure web gateway that blocks access to a social networking site. How would you categorize this type of security control?**

2. **A company has installed motion-activated floodlighting on the grounds around its premises. What class and function is this security control?**

3. **A firewall appliance intercepts a packet that violates policy. It automatically updates its Access Control List to block all further packets from the source IP. What TWO functions is the security control performing?**

4. **If a security control is described as operational and compensating, what can you determine about its nature and function?**

5. **If a company wants to ensure it is following best practice in choosing security controls, what type of resource would provide guidance?**

Lesson 1

Summary

You should be able to compare and contrast security controls using categories and functional types. You should also be able to explain how regulations, frameworks, and benchmarks are used to develop and validate security policies and control selection.

Guidelines for Comparing Security Roles and Security Controls

Follow these guidelines when you assess the use of security controls, frameworks, and benchmarks in your organization:

- Create a security mission statement and supporting policies that emphasizes the importance of the CIA triad: confidentiality, integrity, availability.
- Assign roles so that security tasks and responsibilities are clearly understood and that impacts to security are assessed and mitigated across the organization.
- Consider creating business units, departments, or projects to support the security function, such as a SOC, CSIRT, and DevSecOps.
- Identify and assess the laws and industry regulations that impose compliance requirements on your business.
- Select a framework that meets compliance requirements and business needs.
- Create a matrix of security controls that are currently in place to identify categories and functions—consider deploying additional controls for any unmatched capabilities.
- Use benchmarks, secure configuration guides, and development best practices as baselines for deploying assets.
- Evaluate security capabilities against framework tiers and identify goals for developing additional cybersecurity competencies and improving overall information security assurance.