EXAM CRAM

CompTIA A+

220-801
220-802

Sixth Edition

PEARSON IT CERTIFICATION

DAVID L. PROWSE

EXAM CRAM

CompTIA® A+

220-801 and 220-802

Sixth Edition

David L. Prowse

CompTIA A+® 220-801 and 220-802 Exam Cram, Sixth Edition

ISBN-13: 978-0-7897-4971-0
ISBN-10: 0-7897-4971-8

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

Fourth Printing: May 2013

Trademarks

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

Warning and Disclaimer

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

Bulk Sales

Que Publishing offers excellent discounts on this book when ordered in quantity for bulk purchases or special sales. For more information, please contact

U.S. Corporate and Government Sales
1-800-382-3419
corpsales@pearsontechgroup.com

For sales outside of the U.S., please contact

International Sales
international@pearson.com

Associate Publisher
David Dusthimer

Acquisitions Editor
Betsy Brown

Development Editor
Eleanor C. Bru

Managing Editor
Sandra Schroeder

Project Editor
Seth Kerney

Copy Editor
Apostrophe Editing Services

Indexer
Lisa Stumpf

Proofreader
Leslie Joseph

Technical Editor
Aubrey Adams

Publishing Coordinator
Vanessa Evans

Multimedia Developer
Tim Warner

Designer
Gary Adair

Composition
Trina Wurst

Contents at a Glance

Table of Contents

About the Author

David L. Prowse is an author, a computer network specialist, and a technical trainer. Over the past several years he has authored several titles for Pearson Education, including the well-received *CompTIA A+ Exam Cram* and *CompTIA Security+ Cert Guide*. As a consultant, he installs and secures the latest in computer and networking technology. Over the past decade he has also taught CompTIA A+, Network+, and Security+ certification courses, both in the classroom and via the Internet. He runs the website www.davidlprowse.com, where he gladly answers questions from students and readers.

About the Tech Editor

Aubrey Adams (CCNA, Security+) is an electronic and computer system engineering lecturer and Cisco Networking Academy instructor at Central Institute of Technology in Perth, Western Australia. Coming from a background in telecommunications design, with qualifications in electronic engineering and management and graduate diplomas in computing and education, he teaches across a range of computer systems and networking vocational education and training areas. Aubrey also authors Networking Academy curriculum and assessments and is a Cisco Press author and Pearson Education technical editor.

Dedication

To my wife Georgia, for dealing with my absurd deadlines…again.

Acknowledgments

First, I'd like to thank David Dusthimer and Betsy Brown who put their faith in me for yet another A+ Exam Cram project.

Special thanks to Aubrey Adams. Your wisdom during this project has kept me on track and is a key component in the flow and technical accuracy of this book.

Thanks to Eleanor Bru, Andrew Cupp, Seth Kerney, and everyone else at Pearson that was involved in this project.

I'd also like to acknowledge my previous and current readers, students, and visitors to my website. Thank you very much for all your kind words, input, and feedback.

We Want to Hear from You!

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

As an associate publisher for Pearson IT Certification, I welcome your comments. You can email or write me directly to let me know what you did or didn't like about this book—as well as what we can do to make our books better.

Please note that I cannot help you with technical problems related to the topic of this book. We do have a User Services group, however, where I will forward specific technical questions related to the book.

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

Email: feedback@pearsonitcertification.com

Mail: David Dusthimer
Associate Publisher
Pearson IT Certification
800 East 96th Street
Indianapolis, IN 46240 USA

Reader Services

Visit our website and register this book at http://www.pearsonitcertification.com/ store/product.aspx?isbn=9780789749710 for convenient access to any updates, downloads, or errata that might be available for this book.

It Pays to Get Certified

In a digital world, digital literacy is an essential survival skill.

Certification proves you have the knowledge and skill to solve business problems in virtually any business environment. Certifications are highly-valued credentials that qualify you for jobs, increased compensation and promotion.

Certification Advances Your Career

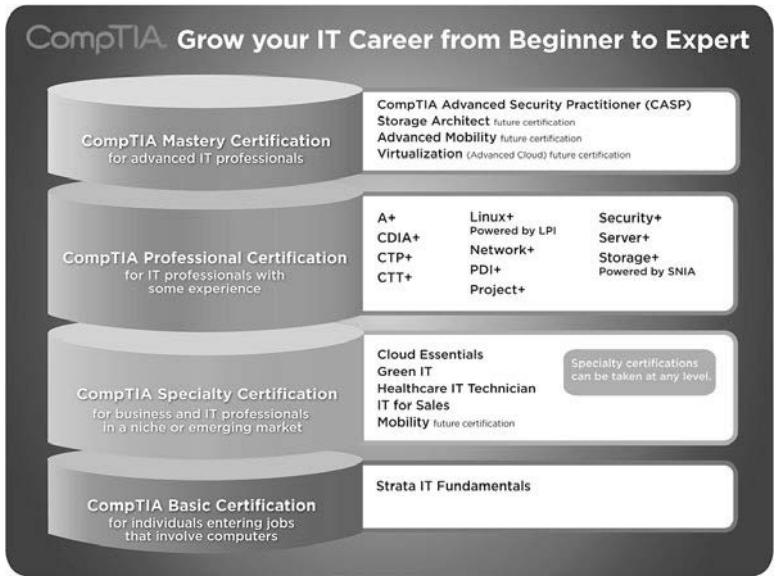
- The CompTIA A+ credential—provides foundation-level knowledge and skills necessary for a career in PC repair and support.
- Starting Salary—CompTIA A+ Certified individuals can earn as much as $65,000 per year.
- Career Pathway—CompTIA A+ is a building block for other CompTIA certifications such as Network+, Security+ and vendor specific technologies.
- More than 850,000—Individuals worldwide are CompTIA A+ certified.
- Mandated/Recommended by organizations worldwide—Such as Cisco and HP and Ricoh, the U.S. State Department, and U.S. government contractors such as EDS, General Dynamics, and Northrop Grumman.

Some of the primary benefits individuals report from becoming A+ certified are:

- More efficient troubleshooting
- Improved career advancement
- More insightful problem solving

CompTIA Career Pathway

CompTIA offers a number of credentials that form a foundation for your career in technology and allows you to pursue specific areas of concentration. Depending on the path you choose to take, CompTIA certifications help you build upon your skills and knowledge, supporting learning throughout your entire career.



Steps to Certification

Steps to Getting Certified and Staying Certified	
Review Exam Objectives	Review the certification objectives to make sure you know what is covered in the exam. http://www.comptia.org/certifications/testprep/examobjectives.aspx
Practice for the Exam	After you have studied for the certification, take a free assessment and sample test to get an idea what type of questions might be on the exam. http://www.comptia.org/certifications/testprep/practicetests.aspx
Purchase an Exam Voucher	Purchase your exam voucher on the CompTIA Marketplace, which is located at: www.comptiastore.com.
Take the Test!	Select a certification exam provider and schedule a time to take your exam. You can find exam providers at the following link: http://www.comptia.org/certifications/testprep/testingcenters.aspx

Join the Professional Community

Join IT Pro Community

http://itpro.comptia.org

The free IT Pro online community provides valuable content to students and professionals.

Career IT Job Resources

- Where to start in IT
- Career Assessments
- Salary Trends
- US Job Board

Forums on Networking, Security, Computing and Cutting Edge Technologies

Access to blogs written by Industry Experts

Current information on Cutting Edge Technologies

Access to various industry resource links and articles related to IT and IT careers

Content Seal of Quality

This courseware bears the seal of **CompTIA Approved Quality Content**. This seal signifies this content covers 100% of the exam objectives and implements important instructional design principles. CompTIA recommends multiple learning tools to help increase coverage of the learning objectives.

Why CompTIA?

- **Global Recognition**—CompTIA is recognized globally as the leading IT non-profit trade association and has enormous credibility. Plus, CompTIA's certifications are vendor-neutral and offer proof of foundational knowledge that translates across technologies.
- **Valued by Hiring Managers**—Hiring managers value CompTIA certification because it is vendor- and technology-independent validation of your technical skills.
- **Recommended or Required by Government and Businesses**—Many government organizations and corporations either recommend or require technical staff to be CompTIA certified. (For example, Dell, Sharp, Ricoh, the U.S. Department of Defense, and many more.)
- **Three CompTIA Certifications ranked in the top 10**—In a study by DICE of 17,000 technology professionals, certifications helped command higher salaries at all experience levels.

How to obtain more information

Visit CompTIA online: www.comptia.org to learn more about getting CompTIA certified.

Contact CompTIA: Call 866-835-8020 ext. 5 or email questions@comptia.org

Connect with us :

Introduction

Welcome to the *CompTIA A+ Exam Cram*, Sixth Edition, my name is David L. Prowse. This book prepares you for the CompTIA A+ 220-801 and 220-802 Certification Exams. Imagine that you are at a testing center and have just been handed the passing scores for these exams. The goal of this book is to make that scenario a reality. I am happy to have the opportunity to serve you in this endeavor. Together, we can accomplish your goal to attain the CompTIA A+ certification.

Target Audience

The CompTIA A+ exams measure the necessary competencies for an entry-level IT professional with the equivalent knowledge of at least 12 months of hands-on experience in the lab or field.

This book is for persons who have experience working with desktop PCs and mobile devices and want to cram for the A+ certification exam—*cram* being the key word. This book does not cover everything in the PC world; how could you in such a concise package? However, this guide is fairly thorough and should offer you a lot of insight…and a whole lot of test preparation.

If you do not feel that you have the required experience, have never attempted to troubleshoot a computer, or are new to the field, then I recommend the *CompTIA A+ Cert Guide*, which goes into much more depth than this text. On a side note, another great reference book that should be on every PC technician's shelf is the latest edition of *Upgrading and Repairing PCs* by Scott Mueller.

Essentially two types of people will read this book: those who want a job in the IT field, and those who want to keep their job. For those of you in the first group, the new CompTIA A+ certification can have a powerful career impact, increasing the chances of securing a position in the IT world. For those in the second group, preparing for the exams serves to keep your skills sharp, and your knowledge up-to-date, making you a well-versed and well-sought-after technician.

Of course, I know that some of you are picking up this book solely for the practice exams, which are by the way located directly after Chapter 19, "Taking the Real Exams." But I recommend against solely studying the practice questions. This book was designed from the ground up to build your

knowledge in such a way that when you get to the practice exams, they can act as the final key to passing the real exams. The knowledge in the chapters is the cornerstone, whereas the practice exam questions are the battlements. Complete the entire book, and you will have built yourself an impenetrable castle of knowledge.

About the CompTIA A+ 220-801 and 220-802 Exams

The 2012 version of the A+ exams are known as the CompTIA A+ 220-801 and 220-802 exams. There are quite a few changes and additions to these versions of the A+ exams including the following:

- Increased Windows 7 content.
- Windows 2000 operating system has been removed.
- Newer multicore processor technologies such as Core i7 have been added.
- Custom PC configurations have been included.
- Mobile devices such as tablets and smartphones have been added.
- Increased amount of networking and security topics, with increased difficulty.
- Additional operational procedures.

This book covers all these changes and more within its covers.

For more information about how the A+ certification can help your career, or to download the latest official objectives, access CompTIA's webpage at www.comptia.org.

About This Book

This book is broken down into 19 chapters, each pertaining to particular objectives on the exam. Because the official CompTIA objectives can have long names that sometimes deal with multiple subjects, the chapters are divided into more manageable (and memorable) topics. All the questions in this book refer to these topics. Chapter topics and the corresponding CompTIA objectives are listed in the beginning of each chapter.

For the most part, the exam topics in this book are structured to build on one another. Because of this, you should read this entire book in order to best prepare for the CompTIA A+ exams. In the case that you want to review a particular topic, for example if your CD practice exam identifies a topic deficiency, those topics are listed at the end of this introduction. In addition, you can use the index or the table of contents to quickly find the concept you are after.

Chapter Format and Conventions

Every Exam Cram chapter follows a standard structure and contains graphical clues about important information. The structure of each chapter includes the following:

- **Opening topics list:** This defines the topics to be covered in the chapter; it also lists the corresponding CompTIA A+ objective numbers.
- **Topical coverage:** The heart of the chapter. Explains the topics from a hands-on and a theory-based standpoint. This includes in-depth descriptions, tables, and figures geared to build your knowledge so that you can pass the exam. The chapters are broken down into between two to five topics each.
- **Cram Quiz questions:** At the end of each topic is a quiz. The quizzes, and ensuing explanations, are meant to gauge your knowledge of the subjects. If the answers to the questions don't come readily to you, consider reviewing individual topics or the entire chapter. In addition to being in the chapters, you can find the Cram Quiz questions on the disc. The questions are separated into their respective 220-801 and 220-802 categories for easier studying when you approach the exam.
- **Exam Alerts, Sidebars, and Notes:** These are interspersed throughout the book. Watch out for them!

ExamAlert

This is what an Exam Alert looks like. Normally, an alert stresses concepts, terms, hardware, software, or activities that are likely to relate to one or more certification test questions.

Additional Elements

Beyond the chapters, there are a few more elements that I've thrown in for you. They include

- **Practice Exams:** These are located directly after Chapter 19 within the book. There is one for each CompTIA A+ exam. These exams are also available on the disc.
- **Cram Sheet:** The tear-out Cram Sheet is located in the beginning of the book. This is designed to jam some of the most important facts you need to know for the exam into one small sheet, allowing for easy memorization. It is also in PDF format on the disc.

The Hands-On Approach

This book refers to two different computers as the following:

- **Media PC:** I built this desktop computer new for this sixth edition in January 2012. It is an Intel Core i5 system.
- **Tower PC:** This tower computer was built in 2009. It is an Intel Core 2 system. I refer to this computer to show older PC technologies still covered within the A+ objectives and to make comparisons with the newer *Media PC*.

I built *Media PC* using components that are a good example of what you will see in the field today, and for a while to come. These components are representative of the types of technologies that will be covered in the exams. I refer to the components in this system from Chapter 2, "Motherboards," onward. I like to put things into context whenever possible. By referencing the parts in the computer during each chapter, I hope to infuse some real-world knowledge and to solidify the concepts you need to learn for the exam. This more hands-on approach can help you to visualize concepts better. I recommend that every PC technician build their own PC at some point (if you haven't already). This can help to reinforce the ideas and concepts expressed in the book. You should also work with multiple computers while going through this book: one with Windows 7, one with Windows Vista, and one with Windows XP. Or you might attempt to create a dual-boot or three-way-boot on a single hard drive. Another option is to run one computer with one of the operating systems mentioned and virtual machines running the other operating systems. Finally, Windows 7 users might opt to include Windows XP mode, in addition to other solutions.

These pages refer to various ancillary websites, most notably

- **Microsoft TechNet:** http://technet.microsoft.com
- **Microsoft Support:** http://support.microsoft.com

As an IT technician, you will be visiting these sites often; they serve to further illustrate and explain concepts covered in this text.

Goals for This Book

I have three main goals in mind while preparing you for the CompTIA A+ exams.

My first goal is to help you understand A+ topics and concepts quickly and efficiently. To do this, I try to get right to the facts necessary for the exam. To drive these facts home, the book incorporates figures, tables, real-world scenarios, and simple to-the-point explanations. Also, in Chapter 19, you can find test-taking tips and a preparation checklist that gives you an orderly step-by-step approach to taking the exam. Be sure to complete every item on the checklist! For students of mine that truly complete every item, there is an extremely high pass rate for the exams.

My second goal for this book is to provide you with more than 500 *unique* questions to prepare you for the exam. Between the Cram Quizzes and the practice exams, that goal has been met, and I think it will benefit you greatly. Because CompTIA reserves the right to change test questions at any time, it is difficult to foresee exactly what you will be asked on the exam; however I think you will find that a good amount of the questions in this book are similar to the real questions. Regardless, to become a good technician, you must know the *concept*, not just memorize questions. To this effect each question has an explanation and maps back to the topic (and chapter) covered in the text. I've been using this method for more than a decade with my students (more than 2,000 of them) with great results.

My final goal is to provide support for this and all my titles, completing the life cycle of learning. I do this through my personal website: www.DavidLProwse.com/220-801, which has additional resources for you, an errata page (which you should check as soon as possible) and is set up to take questions from you about this book. I'll try my best to get to your questions ASAP. All personal information is kept strictly confidential.

Good luck in your certification endeavors. I hope you benefit from this book. Enjoy!

Sincerely,

David L. Prowse

Exam Topics

Table I.1 lists the exam topics covered in each chapter of the book.

TABLE I.1 **Exam Cram CompTIA A+ Exam Topics**

Exam Topic	Chapter
The Six-Step A+ Troubleshooting Process	1
Troubleshooting Examples and PC Tools	
Motherboard Components and Form Factors	2
The BIOS	
Installing and Troubleshooting Motherboards	
CPU 101	3
Installing and Troubleshooting CPUs	
RAM Basics and Types of RAM	4
Installing and Troubleshooting DRAM	
Understanding and Testing Power	5
Power Devices	
Power Supplies	
Magnetic Storage Media	6
Optical Storage Media	
Solid State Storage Media	
Installing, Configuring, and Troubleshooting Visible Laptop Components	7
Installing, Configuring, and Troubleshooting Internal Laptop Components	
Installing and Upgrading to Windows 7	8
Installing and Upgrading to Windows Vista	
Installing and Upgrading to Windows XP	
Windows User Interfaces	9
System Tools and Utilities	
Files, File Systems, and Disks	
Updating Windows	10
Maintaining Hard Disks	
Repair Environments and Boot Errors	11
Windows Tools and Errors	
Command-Line Tools	
The Video Subsystem	12
The Audio Subsystem	

TABLE I.1 **Continued**

Exam Topic	Chapter
Input/Output Devices, and Peripherals	13
Custom PC Configurations	
Printer Types and Technologies	14
Installing, Configuring, and Troubleshooting Printers	
Types of Networks and Network Devices	15
Cables, Connectors, and Tools	
TCP/IP	
SOHO Windows Networking	
Troubleshooting Networks	
Security Threats and Prevention	16
Windows Security	
SOHO Security	
Mobile Hardware and Operating Systems	17
Mobile Networking and Synchronization	
Mobile Security	
Safety	18
Procedures and Environmental Controls	
Professionalism and Communication Skills	
Getting Ready and the Exam Preparation Checklist	19
Tips for Taking the Real Exam	
Beyond the CompTIA A+ Certification	

This page intentionally left blank

CHAPTER 17

Mobile Devices

This chapter covers the following A+ exam topics:

- Mobile Hardware and Operating Systems
- Mobile Networking and Synchronization
- Mobile Security

You can find a master list of A+ exam topics in the "Introduction."

This chapter covers CompTIA A+ 220-802 objectives 3.1 through 3.5.

Mobile devices have simply exploded on to the mainstream scene. Especially since 2010, the amount of mobile devices in use has been growing exponentially. Now, it seems that everywhere you look there is someone tapping away on a tablet computer, smartphone, or other mobile device. As of 2012, half a million Android and Apple devices are activated daily—and that number is increasing! Because of this CompTIA has added an entire mobile devices section to the A+ 220-802 exam. As an A+ technician you need to know the basic hardware of these devices, the differences between the two main mobile operating systems, how to network and synchronize the devices, and how to secure them.

In this chapter we'll pay the most attention to Apple devices and Android-based devices, but we'll also briefly discuss some of the other players in the market. For this edition of the book I will refer to an Apple iPad2 tablet computer and an Android HTC Evo smartphone. I do this so that you can see some important configurations on the two most-used platforms in the mobile device market. So enough talk…let's get mobile!

Mobile Hardware and Operating Systems

Mobile devices are computers, smaller and lighter than desktops and laptops, but computers nonetheless. There are similarities and differences in hardware between the two. You will find there are new players on the software side, and these too have similarities and differences compared to PCs and laptops. But remember that at their core, mobile devices are still computers, and many of the principles and rules that you have learned earlier in this book regarding hardware and software still apply.

Mobile Hardware Examples

A common device as of the writing of this book is the Apple iPad2. It is known as a tablet computer and is manufactured by Foxconn, who also constructs the iPhone, Kindle, Playstation 3, and Xbox 360. Table 17.1 gives a list of the hardware the iPad2 uses.

TABLE 17.1 **Apple iPad2 Hardware**

Hardware Component	Description
1 GHz ARM CPU	▶ 32-bit *A*dvanced *R*ISC *M*achine Processor ▶ Designed for simplicity and low-power
512 MB DDR2 RAM	▶ Similar DDR standard to what PCs use ▶ Smaller form factor
16 GB Flash Memory	▶ Similar to solid-state flash memory in a USB flash drive ▶ Used for permanent storage instead of an SATA or IDE hard drive
Multitouch touchscreen	▶ Capacitive touchscreen that responds to fingers and stylus devices
Lithium-ion polymer battery	▶ Similar to lithium-ion batteries in laptops ▶ Can be made into any shape ▶ Lasts for 10 hours on a full charge

ExamAlert

Memorize the basic types of hardware used by a tablet computer.

As you can see from the table, the basic components of CPU, RAM, and so on are the same as desktop/laptop computers. But the *types* of components are different. The whole concept of this hardware configuration is based on

portability and ease of use. Therefore, tablet computers will be less powerful than desktop computers and laptops; but, the hardware is matched to the type of applications the device will be used for.

Similar tablets (but with different software) include the Motorola Xoom, Samsung Galaxy, and Asus Transformer. These will often be less proprietary than an Apple device; for example, they might use Micro-USB ports for charging and synchronization of data, whereas the Apple iPad2 has a proprietary charging port. You might also see different names for the touch interface of a device. For example, the company HTC developed a user interface called TouchFLO for its smartphones that enabled the user to drag the screen up, left, or right. This has been replaced by HTC Sense, which is a multitouch-enabled touch screen similar to the Apple multitouch technology. As of 2012, most new smartphones and tablets feature multitouch touch screens.

Hardware Differences Between Tablets and Laptops

One of the big distinctions between tablets and laptops is the lack of field serviceable parts. Another difference is that tablets and other similar devices are usually not upgradeable. Some mobile devices, such as smartphones, can have upgraded memory cards and/or batteries, but that's about it, and these are usually not serviceable in the field because it is difficult to protect yourself from ESD when working on these devices. (But that doesn't mean it isn't done.) Many organizations recommend you bring the device back to the lab for upgrades or parts swaps. Other devices such as the iPad2 are not user-serviceable whatsoever; and any attempt at doing so voids the warranty. If repair, upgrade, or replacement is necessary, most organizations utilize the warranties built in to these products, instead of trying to do the work in-house.

Exam Alert

Know the basic differences between tablets and laptops.

A laptop is actually just a smaller, portable version of a desktop computer. Like the desktop computer, it contains a similar processor, similar DDR RAM, and a hard drive that could possibly be solid-state, but regardless will most likely be plugged into an SATA port. It also has a keyboard, and a touchpad similar to a mouse. All this hardware is designed to make the best use of operating systems that you would normally find on a desktop computer. Tablets on the other

hand use ARM-based processors and use nonvolatile flash memory hard-wired to the system instead of a magnetic or solid-state hard drive. So, as you can imagine, the tablet has a loss of performance when compared to a laptop. In addition, the tablet utilizes an on-screen keyboard and doesn't require any type of mouse due to the touchscreen capability. All this hardware is designed to run mobile device software such as Android or iOS.

Mobile Operating Systems

Currently, mobile device software comes in one of two forms: open-source, which is effectively free to download and modify; and closed-source, otherwise known as *vendor-specific*, which cannot be modified without express permission and licensing. There are benefits and drawbacks to each type of system. Because you will see both in the field, you should know each one equally. Let's go over these two systems.

Open-Source: Android

Android is an example of open source software. It is a Linux-based operating system used mostly on smartphones and tablet computers and is developed by the Open Handset Alliance, a group directed by Google. Google releases the Android OS code as open-source, allowing developers to modify it, and freely create applications for it. Google also commissioned the Android Open-Source Project (AOSP); its mission is to maintain and further develop Android. You'll know when you are dealing with the Android open-source OS and related applications when you see the little robot caricature, usually in green.

Android OS versions are dubbed with names such as Cupcake, Gingerbread, and the two latest: Honeycomb (version 3) and Ice Cream Sandwich (version 4). To find out the version you are currently running, start at the Home screen; this is the main screen that boots up by default. Then tap the Menu button, and then tap Settings. (Settings is used often in this chapter as a starting point, so remember how to get there!) Scroll to the bottom and tap the About Phone (or just About) option. Then tap Software Information or similar option. This displays the version of Android. Figure 17.1 shows a smartphone using Android version 2.3.3 (Gingerbread)

Say a company wanted to create a custom version of the Android OS for a handheld computer that it was developing. According to the license, the company would be allowed to do this and customize the OS to its specific hardware. Some companies opt to use Android for this purpose, whereas others use Windows CE or Windows Mobile (for a fee), both designed for handheld computers.

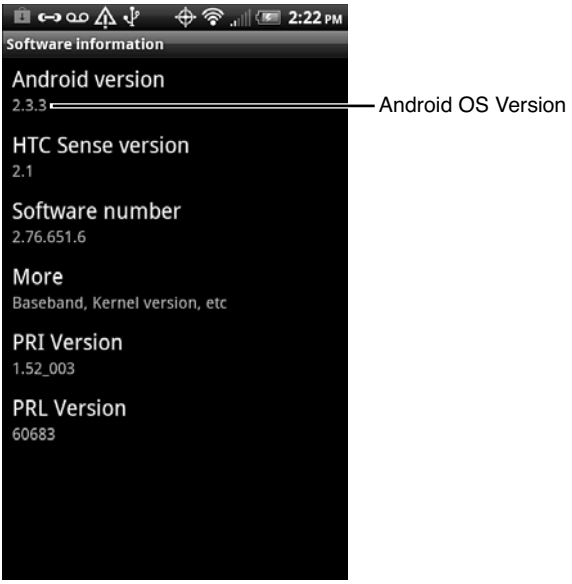


FIGURE 17.1 **Typical smartphone using Android version 2.3.3**

Closed-Source: iOS

Apple's iOS is an example of closed-source software. It is found on iPhones and iPads as well. It is based off Mac OS X (used on Mac desktops and laptops) and is Unix-based.

To find out the version of iOS you are running go to the Home screen, and then tap Settings. Tap General and then tap About. You see the Version number. For example, Figure 17.2 shows an iPad2 running Version 5.0 (9A334). 9A334 is the build number; this was the public release of version 5.0.

Unlike Android, iOS is not open-source, and is not available for download to developers. Only Apple hardware uses this operating system. This is an example of vendor-specific software. However, if a developer wants to create an application for iOS, they can download the iOS software development kit (SDK). Apple license fees are required when a developer is ready to go live with the application.

ExamAlert

Understand the difference between open-source and closed-source.

FIGURE 17.2 **iPad2 using version 5.0 of iOS**

Obtaining Applications

Mobile devices are nothing without applications. To this end, both Android and iOS have application sources where you can download free and paid applications (also known as *apps*).

Android users download applications from the Android Market (also accessible through Google Play.) This can be done directly from the mobile device. Or if a mobile device is connected via USB to a computer, the user can browse apps on the Google Play website while working on the computer and download directly from the site to the phone, passing through the computer.

iOS users download applications from the App Store. This was originally an update to the iTunes store, but on newer iOS mobile devices, it is now a separate icon on the Home screen. Apps can also be downloaded from a Mac or from a PC through the iTunes application.

ExamAlert

Know where to obtain applications for Apple and Android devices.

Regardless of the OS, users would search for the name of the application they want, download it, start the installation process, agree to a license, and then finally make use of the app.

Some applications don't work unless a person was to hack the OS and gain "superuser" privileges. In the Android world this is known as *rooting* the phone or other mobile device. In the iOS world it is *jailbreaking*. Note that performing either of these could be a breach of the user license agreement. It can also be dangerous. These types of hacks often require a person to wipe out the device completely, and install a special application that may or may not be trustworthy. Many phones are rendered useless or are compromised when attempting this procedure. Applications that have anything to do with rooting or jailbreaking should generally be avoided.

Screen Configurations

Mobile device displays rotate by default if the user turns the device, allowing the screen to be viewed vertically or horizontally. This aids when looking at pictures, movies, or viewing websites. But in some cases, a user might want to lock the rotation of the device so that it stays as either vertical or horizontal, without moving. On an Android device this can be done by accessing Settings, then tapping Display, and then deselecting Auto-rotate screen. On an iOS device (version 4 or 5) this can be done by double-tapping the Home button (which brings up the multitasking bar on the bottom) and then swiping the bar all the way to the right. Finally, a circular arrow is shown to the far left; tap this, and rotation will be locked. Some iPads (such as the iPad2) also have a side switch that can be configured to enable/disable rotation lock; this feature can be turned on in Settings > General > Use side switch to: Lock Rotation.

Screen orientation is a simple concept to understand and use. But it can be more complicated when it comes to applications. For example, Apple mobile devices make use of the *Accelerometer*: a combination of hardware and software that measure velocity; they detect rotation, shaking of the device and so on. It's the accelerometer that enables a mobile device to automatically adjust from portrait (vertical) to landscape (horizontal) mode using the three axes: the X-axis (left to right), the Y-axis (up and down), and the Z-axis (back to front). These are manipulated by developers for applications and games so that the program can recognize particular movements of the device and translate them to specific application functions. Newer Apple devices include a *gyroscope*, which adds the measurements of pitch, roll, and yaw, just like in the concept of flight dynamics. You won't need a pilot's license to use an iPad, but this additional measurement of movement has a great impact on the development of

newer applications and especially games. Of course, if the accelerometers or gyroscope of the mobile device fail and a reset of the device doesn't fix the problem, it must be repaired at an authorized service center.

ExamAlert

Understand the concepts of *accelerometer* and *gyroscope*.

Android devices have a screen calibration utility called G-Sensor calibration. It is found in Settings > Display. To make sure that the three axes are calibrated properly, this program is run while the mobile device is laid on a flat surface. You can tell if the surface is level by the horizontal and vertical leveling bubbles on the display. Then press the Calibrate button to reset the G-sensor, as shown in Figure 17.3.

FIGURE 17.3 **G-Sensor calibration on a typical smartphone**

Other mobile devices' calibration programs show a crosshair or similar image in the center of the screen. You need to tap with a stylus as close to the center of the display as possible. If a stylus is not available, use the pointed end of a pen cap.

ExamAlert

Know how to calibrate the screen of an Android device.

A reset can also fix problems with calibration (as well as other types of problems). There are two types of resets: soft and hard. A soft reset is usually performed simply by powering the device off and then powering it back on again. This can fix temporary problems quickly and easily. It is similar to rebooting a PC. However, more advanced problems require a hard reset. Warning! A hard reset may remove all data and applications and return the device to its original factory state. Do not perform a hard reset without backing up the contents of the memory card in the mobile device, and any additional settings you require. You can find more information on resets in the section titled "Mobile Security."

Today's Apple devices do not offer a calibration utility. Sometimes, issues that appear to be calibration problems are actually something else with an easy fix. For example, cheaper screen protectors can bubble and otherwise cause problems when tapping on the screen. Removing the protector and installing a new one properly can fix this problem. When installing a screen protector, use a long, flat surface to squeeze all the bubbles out; there are shims that can be purchased for just this purpose. Use a decent screen protector such as Ghost Armor or something similar. Good quality screen protectors will not only protect the display, but they will also reduce glare, smudging, and fingerprints, without reducing sensitivity. Dirty screens can also be a culprit when a user is having difficulty tapping on icons or smaller items. Clean the display with a lint-free cloth. If the screen is very dirty, mix 50% isopropyl alcohol and 50% water, apply conservatively to the cloth, and then clean the display with the cloth. Make sure all traces of liquid are removed when you are done. If none of these steps work, the device needs to be brought in to an authorized service center for repair.

GPS and Geotracking

The Global Positioning System (GPS), developed by the U.S. DoD is a worldwide system of satellites that provide location information for anything with a GPS receiver. Any mobile device with a GPS receiver can use this system to identify its location and utilize mapping programs and any other applications that rely on GPS. Some mobile devices do not have a GPS receiver, and instead use cell tower triangulation, or Location Services that uses crowdsourced Wi-Fi locations to determine the approximate location of the device.

To enable/disable GPS on an Android-based device go to Settings > Location, and select Use GPS satellites. To enable/disable GPS on an Apple device such as an iPad, go to Settings > Location Services.

ExamAlert

Memorize how to enable GPS for Android and Apple devices.

Geotracking is the practice of tracking and recording the location of a mobile device over time. This location tracking is done by Apple and Google as well as other organizations and governments. Privacy issues aside, this practice *is* being done, so if a user doesn't want their location known, simply disable the GPS setting.

ExamAlert

Understand the definition of geotracking for the exam.

Cram Quiz

Answer these questions. The answers follow the last question. If you cannot answer these questions correctly, consider reading this section again until you can.

220-802 Questions

1. A user is having difficulty tapping on icons. What should you do to help the user? (Select the two best answers.)
   - ❍ **A.** Clean the display.
   - ❍ **B.** Tap the Home button.
   - ❍ **C.** Install a screen protector.
   - ❍ **D.** Initiate a soft reset.
   - ❍ **E.** Initiate a hard reset.

2. Which of the following can aid a mobile user in finding the nearest coffee shop? (Select the best answer.)
   - ❍ **A.** Geotracking
   - ❍ **B.** iOS
   - ❍ **C.** GPS
   - ❍ **D.** GSM

3. A user wants to stop his tablet from shifting horizontally when he turns it. Which of the following should you enable?

- ❍ **A.** Lock Rotation
- ❍ **B.** Accelerometer
- ❍ **C.** Gyroscope
- ❍ **D.** Screen Calibration

4. What kind of display would an iPad2 use?

- ❍ **A.** CRT
- ❍ **B.** Multitouch
- ❍ **C.** Tap screen
- ❍ **D.** Singletouch

5. What are two common operating systems used by mobile devices? (Select the two best answers.)

- ❍ **A.** Blueberry OS
- ❍ **B.** iOS
- ❍ **C.** Google OS
- ❍ **D.** Android OS

6. What type of CPU do mobile devices use?

- ❍ **A.** Core i7
- ❍ **B.** Phenom II
- ❍ **C.** ARM
- ❍ **D.** Pentium

7. Which OS is considered to be closed-source?

- ❍ **A.** Android OS
- ❍ **B.** Bluetooth
- ❍ **C.** Linux
- ❍ **D.** iOS

8. What are a couple of differences between a tablet computer and a laptop? (Select the two best answers.)

- ❍ **A.** Tablets have little or no field serviceable parts.
- ❍ **B.** Tablets are upgradeable.
- ❍ **C.** Laptops don't use touch screens.
- ❍ **D.** Tablets use flash memory as the hard drive.
- ❍ **E.** Tablets use RAM.

Cram Quiz Answers

220-802 Answers

1. **A** and **D.** A dirty display can cause issues when trying to manipulate a multi-touch screen. By cleaning it, the user might find that is it easier to use. A soft reset (turning the device off and on) can sometimes fix the problem as well. Tapping the Home button simply brings the person to the Home screen. Screen protectors are a good idea, but if installed incorrectly, they could actually be the reason that a user has issues tapping icons. After the screen is cleaned, a decent quality screen protector should be installed. Hard resets often initiate a complete wipe of the system. Use this only as a last resort.
2. **C.** GPS is used to locate the mobile user. From that information, one of several programs can locate that all-important nearest coffee shop. Geotracking is the practice of tracking and recording the location of a mobile device. However, geo-tracking is done by organizations, whereas GPS is something installed to the mobile device. iOS is the operating system used by Apple mobile devices. GSM is a cellular standard.
3. **A.** Enable Lock Rotation on Apple devices. On Android devices disable Auto-rotate. The Accelerometer is a term used by Apple to describe the hardware/software that controls the three axes of movement. The Gyroscope is another term used by Apple to describe the device that measures the additional three movements (pitch, roll, and yaw) of newer Apple devices. Screen calibration is used to reset the device that measures the three axes.
4. **B.** iPad2 devices use multitouch screens, which allow more than one contact point. Cathode ray tube (CRT) is an older technology monitor used by desktop computers. You would "tap" the screen, but it is known as a touchscreen. Singletouch screens are an older technology; you won't see much of that in the field.
5. **B** and **D**. Two common operating systems used by mobile devices are iOS and Android OS. *Black*berry OS is the OS used on Blackberry devices. Android is effectively controlled by Google. There is a Google Chrome OS designed to work with web applications that is also open-source.
6. **C.** Most commonly, mobile devices use ARM (Advanced RISC Machine) CPUs. Core i7, Phenom II and the older Pentium are used by desktop and laptop computers.
7. **D.** The Apple iOS is a closed-source vendor specific operating system. Android is a type of Linux that is open-source. Bluetooth is a wireless standard, not an operating system.
8. **A** and **D**. Unlike laptops, tablets are not field-serviceable. They use flash memory instead of an SATA hard drive. Tablets are for the most part not upgradeable. Some laptops do come with touchscreens. Both tablets and laptops use RAM.

Mobile Networking and Synchronization

Now that we've discussed mobile hardware and software, let's go ahead and harness their power through networking and synchronization.

From cellular GSM connections to Wi-Fi and Bluetooth, a mobile device can create connections to computers and networks, download e-mail, and work with headsets and remote printers.

Synchronization is the matching up of files, e-mail, and other types of data between one computer and another. We use synchronization to bring files in line with each other and to force devices to coordinate their data. When dealing with synchronization, a mobile device can connect to a PC via USB (the most common), RS-232 serial connections (less common), Wi-Fi, and Bluetooth.

GSM Cellular Connectivity

Cellular phones use the Global System for Mobile Communications (GSM) to make voice calls, and GSM or the general packet radio service (GPRS) to send data at 2G speeds through the cellular network. Extensions of these standards, 3GPP and EDGE are used to attain 3G speeds. 4G speeds can be attained only if a mobile device complies with the International Mobile Telecommunications Advanced (IMT-Advanced) requirements, has a 4G antenna, and is in range of a 4G transmitter, which as of the writing of this book, are only common in urban areas.

Most devices cannot shut off the cellular antenna by itself (unless shutting down the whole device.) However, every device manufactured now is required to have an "airplane mode," which turns off any wireless antenna in the device including GSM, Wi-Fi, GPS, and Bluetooth. On a typical Android device, this can be done by going to Settings > Wireless & Networks > and check marking Airplane Mode. You will find that some airlines don't consider this to be acceptable and will still ask you to turn off your device, either for the duration of the flight or at least during takeoff and landing. Android devices can also access Airplane Mode by pressing and holding the power button. To enable airplane mode on an Apple tablet you would go to Settings > Airplane Mode.

ExamAlert

Know how to configure airplane mode for Android and Apple devices.

Wi-Fi Network Connectivity

Using a cellular connection can be slow when transmitting data (unless you happen to get a 4G signal). That's why all mobile devices are equipped with an embedded wireless antenna to connect to wireless LANs. This WLAN antenna (often referred to as a Wi-Fi antenna) can allow access to 802.11a, b, g, and n networks. The wireless configuration works similar to a wireless connection on a PC or laptop. See Chapter 15, "Networking," for a detailed description of connecting to wireless networks.

In general, the mobile device must first search for wireless networks before connecting. On a typical Android smartphone, this can be done in the following steps:

1. Go to Settings > Wireless & Networks > Wi-Fi Settings.
2. From there, most devices usually scan for wireless networks automatically, or you could tap Add Wi-Fi Network to add one manually.
3. If adding a network manually, enter the SSID of the wireless access point in the Add Wi-Fi Network window, as shown in Figure 17.4.

FIGURE 17.4 **Android OS Prompting for the user to enter an SSID**

4. Enter the passcode for the network. If the code is correct, then the wireless adapter in the mobile device gets an IP address allowing it to communicate with the network. If a wireless network uses WPA2, and the mobile device isn't compatible, you should search for an update to the operating system to make it WPA2-compliant.

Follow these steps to access wireless networks on an iPad or similar device:

1. Go to Settings > Wi-Fi.
2. The device usually scans for networks automatically. To connect to a network manually, tap Other.
3. If adding a network manually, type the SSID of the network in the Name field.
4. Type the passcode for the network. If adding the network manually, you can select the type of security, for example WPA2, as shown in Figure 17.5.

FIGURE 17.5 **iOS Prompting for the user to enter an SSID for a WPA2-secured network**

ExamAlert

Understand how to configure Wi-Fi connections for Android and Apple devices.

Almost all types of devices display the universal wireless icon when connected to a wireless network, as shown in Figure 17.6. This icon not only let's you know when you are connected, but also how strong the connection is. The more curved lines you see, the better the connection.

FIGURE 17.6 **Universal wireless symbol**

Some mobile devices can also perform *Wi-Fi tethering*. This is when the mobile device shares its Internet connection with other Wi-Fi capable devices. For example, if one user had a smartphone that could access the Internet through 3G or GPRS networks, then it could be configured to become a portable Wi-Fi hotspot for other mobile devices that are Wi-Fi capable but have no cellular or GPRS option. Another option in Android is *USB tethering*. When an Android phone is connected to a desktop computer via USB, the desktop (Windows or MAC) can share the phone's mobile network.

A lot of devices can also be configured for *Internet pass-through* as well. This means that the phone or other device connects to a PC via USB and accesses the Internet using the PC's Internet connection.

ExamAlert

Know the terms Wi-Fi tethering, USB tethering, and Internet pass-through.

Wi-Fi Troubleshooting

When troubleshooting mobile device wireless connections, always make sure of the following basic wireless troubleshooting techniques:

- Device is within range.
- The correct SSID was entered (if manually connecting).
- The device supports the encryption protocol of the wireless network.
- Wi-Fi tethering or Internet pass-through is not conflicting with the wireless connection.

If you still have trouble, here are a few more methods that can help to connect, or reconnect to a wireless network:

- Power cycle the mobile device.
- Power cycle Wi-Fi.
- Remove or "forget" the particular wireless network and then attempt to connect to it again.
- Access the advanced settings and check if there is a proxy configuration, if a static IP is used, or if there is a Wi-Fi sleep policy. Any of these could possibly cause a conflict. You might also try renewing the lease of an IP address, if the device is obtaining one from a DHCP server (which it most likely will be.) Some devices also have an option for Best Wi-Fi Performance, which uses more power but might help when connecting to distant WAPs. Advanced settings can be found on an Android device by going to Settings >

Wireless and Networks > Wi-Fi Settings; then tap the Menu button and select Advanced. This is shown in Figure 17.7. On an Apple iPad advanced settings can be located at Settings > Wi-Fi; then tap on the arrow of an individual wireless network. This is shown in Figure 17.8.

FIGURE 17.7 **Advanced wireless settings in Android**

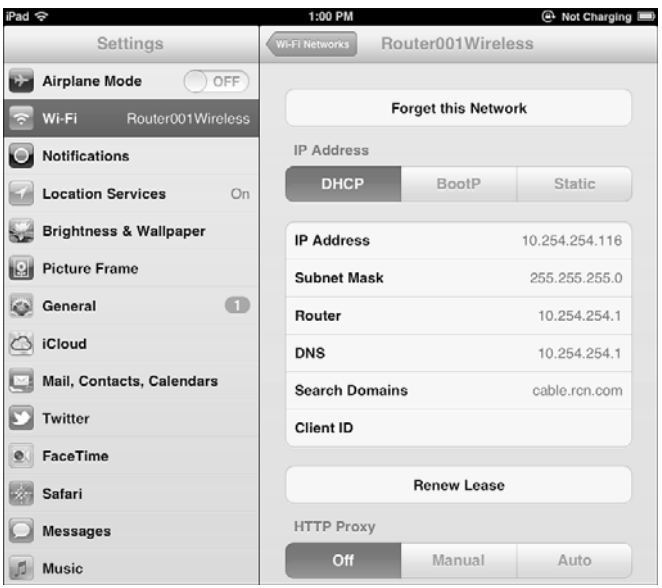


FIGURE 17.8 **Advanced wireless settings in iOS**

One of these methods usually works when troubleshooting a wireless connection but if all else fails; a hard reset can bring the device back to factory settings. (Always back up all data and settings before performing a hard reset.) And if the mobile device still can't connect to any of several known good wireless networks, bring the device to an authorized service center.

ExamAlert

Know your Wi-Fi troubleshooting techniques for the exam!

Bluetooth Configuration

Bluetooth is a wireless standard for transmitting data over short distances. It is commonly implemented in the form of a headset or printer connection by mobile users. It is also used to create wireless personal area networks (WPANs) consisting of multiple Bluetooth-enabled mobile devices.

By default, Bluetooth is usually disabled on Android devices but is enabled on devices such as iPads. To connect a Bluetooth device to a mobile device, Bluetooth first needs to be enabled. Then the Bluetooth device needs to be synchronized to the mobile device. This is known as *pairing* or *linking*. It sometimes requires a pin code. When synchronized, the device needs to be connected. Finally, the Bluetooth connection should be tested. Following are the steps involved in connecting a Bluetooth headset to a typical Android-based device and to an iPad. Before you begin, make sure the Bluetooth headset is charged.

Steps to Configure a Bluetooth Headset on an Android-based Device

1. Go to Settings > Wireless & Networks > and check the box for Bluetooth. This enables Bluetooth on the mobile device.
2. Tap Bluetooth Settings. This displays the Bluetooth Setting screen.
3. Prepare the headset. This can vary from headset to headset. For example, on a typical Motorola Bluetooth headset, you press and hold the button while opening the microphone. Keep holding the button.
4. Tap Scan for Devices on the Android device. Keep holding the button on the headset until the Android device finds it.

5. On the Android device, under the Bluetooth device tap Pair with This Device. Most Android devices pair the Bluetooth headset to the mobile device and then complete the connection automatically, allowing full use of the device.
6. Enter a pin code if necessary. Many devices come with a default pin of 0000.

When finished, the screen on the Android device will look similar to Figure 17.9. Note the Bluetooth icon at the top of the screen. This icon tells you if Bluetooth is running on the device. It will remain even if you disconnect the Bluetooth device. For this headset device we would test it simply by making a phone call. To disconnect it, simply tap the device on the screen and tap OK. It will remain paired but nonfunctional until a connection is made again.

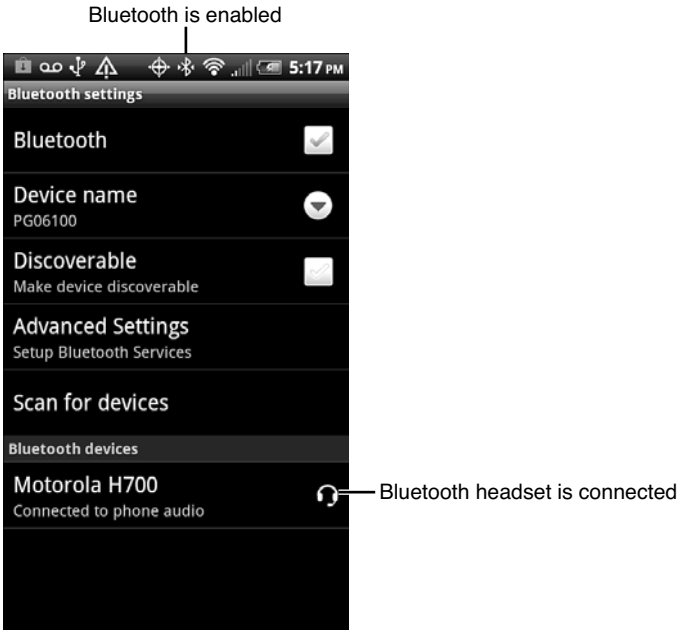


FIGURE 17.9 **Installed Bluetooth device on an Android phone**

Mobile devices can also connect to other Bluetooth-enabled devices (forming a PAN), or to a computer equipped with a Bluetooth dongle. To do this, you must set the mobile device to discoverable (which generally lasts for only 2 minutes). In the same fashion that the headset was discovered by the mobile device in the previous procedure, so can a mobile device be discovered by a

computer or other mobile device. When connecting a mobile device to another mobile device or PC, it can be identified by its name. For example, the mobile device in Figure 17.9 is listed as PG06100. You can modify this name if you want. It is authenticated by a pin code chosen at the PC or other mobile device. We would test these types of connections by sending data or by initiating communications.

Steps to Configure a Bluetooth Headset on an iOS-based Device

This exercise refers to an iPad2.

1. Go to Settings > General > and tap Bluetooth. This displays the Bluetooth screen.
2. Tap Bluetooth to enable it (if it isn't enabled already). This automatically starts searching for devices and continues to do so.
3. Prepare the headset. This can vary from headset to headset. For example, on a typical Motorola Bluetooth headset, you press and hold the button while opening the mic. Keep holding the button. The iPad2 will automatically recognize the device and list it as discoverable.
4. Tap the device name, and it should automatically connect, as shown in Figure 17.10.
5. Enter a pin code if necessary.

To remove the device, click it, and on the next screen click Forget.

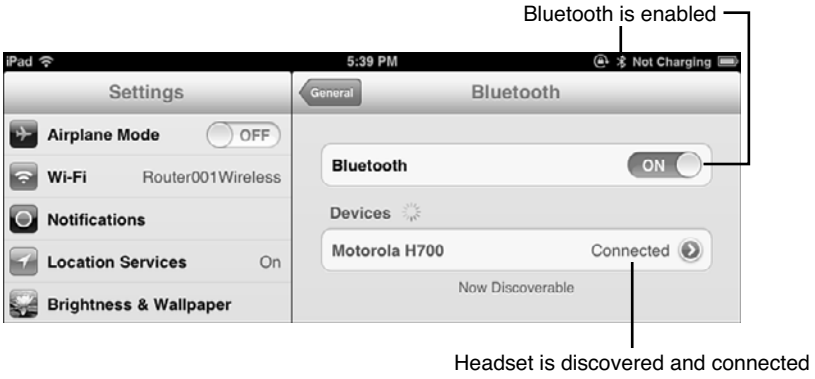


FIGURE 17.10 Installed Bluetooth device on an iPad2

Bluetooth devices can be connected to only one mobile device at a time. If you need to switch the Bluetooth device from one mobile device to another, be sure to disconnect it or "forget" it from the current connection before making a new one.

ExamAlert

Know how to configure Bluetooth devices on Android and Apple devices.

Bluetooth Troubleshooting

If you have trouble pairing a Bluetooth device, and connecting or reconnecting to Bluetooth devices or PANs, try some of the following methods:

- Make sure the phone or other mobile device is Bluetooth-capable.
- Verify that your devices are fully charged, especially Bluetooth headsets.
- Check if you are within range. For example Class 2 Bluetooth devices have a range of 10 meters.
- Try restarting the mobile device and attempt to reconnect.
- Check for conflicting Wi-Fi frequencies. Consider changing the channel used by the Wi-Fi network.
- Try using a known good Bluetooth device with the mobile device to make sure that the mobile device's Bluetooth is functional.
- Remove or "forget" the particular Bluetooth device; then turn off Bluetooth in general, restart the mobile device, and attempt to reconnect.

ExamAlert

Know your Bluetooth troubleshooting techniques for the exam!

E-Mail Configurations

Though there are many other types of communication available to mobile users, e-mail still accounts for an important percentage. You should know how to configure a mobile device for web-based e-mail services such as Gmail, Yahoo, and so on. You should also know how to configure POP3, IMAP, and connections to Microsoft Exchange Servers.

Web-Based E-Mail for Mobile Devices

Mobile devices can access web-based e-mail through a browser, but this is not necessary nowadays due to the "app." For example, Android devices come with a Gmail application built in, allowing a user to access Gmail directly without having to use the browser. Apple iOS devices allow connectivity to Gmail, Yahoo, and a host of other e-mail providers as well.

Connecting to these services is simple and works in a similar fashion as when working on a desktop or laptop computer. Choose the type of provider you use, enter a username (the e-mail address) and password (on Apple devices an Apple ID is also required), and the user will have access to web-based e-mail.

When troubleshooting issues with e-mail, make sure that the username and password are typed correctly. Using onscreen keyboards often leads to mistyped passwords. Also make sure that the mobile device is currently connected to the Internet.

POP3, IMAP, and Exchange

If you need to connect your mobile device to a specific organization's e-mail system, it gets a little bit more complicated. You need to know the server that you want to connect to, the port you need to use, and whether security is employed.

Here's a step-by step process on how to connect a typical Android smartphone to a POP3 account.

1. Go to Home and tap the menu button. Then select All apps.
2. Scroll down until you see the Mail app, and tap it. (This might also be listed as E-mail.)
3. Select whether you want POP3, IMAP, or Exchange. (For this exercise select POP3.)
4. Type the e-mail address and the password of the account and tap Next.
5. Configure the incoming settings. Change the username if desired to something different than the e-mail address. Then type the POP3 server name. By default it will be the domain name portion of the e-mail address, which is usually correct. If security is used select SSL or TLS. This information should be supplied by the network administrator. Type the port number. For POP3 this is 110 by default. If port numbers are different, they will also be supplied to you by the network administrator. Then tap Next.

6. Configure the outgoing settings. Type the SMTP server. Organizations will often use the same server name as the POP3 server. However, small office and home users might have to use their ISP's SMTP server. If security is used, select SSL or TLS. Type the port number for SMTP, which is 25. (Again, this is a default.) Then tap Next.
7. Configure account options. From here you can tell the mobile device how often to check for mail and whether to notify you when it arrives. Tap Next. At this point, new e-mail should start downloading.
8. Finally, you can give the account an easier name for you to remember it by. Tap Done.

Adding an e-mail account to an iOS-based device works essentially the same, but the navigation will be slightly different. For example, to add an e-mail account to an iPad2, go to Home > Settings > Mail, Contact, Calendars > Add Account > Other > Add Mail Account. Then type the information in the same manner you would in the previous steps.

Exam Alert

Know how to add e-mail accounts in Android and iOS.

Now, if you instead have to connect an IMAP account, you have to type the IMAP server (for downloading mail) which uses port 143 by default, and the outgoing SMTP server (for sending mail). If you connect to a Microsoft Exchange mail server, that server name often takes care of both downloading and uploading of e-mail. You might need to know the domain that the Exchange server is a member of. Secure e-mail sessions require the use of SSL or TLS on port 443. Check with the network administrator to find out which protocol to use. POP3 also has a secure derivative known as APOP, a challenge/response protocol which uses a hashing function to prevent replay attacks during an e-mail session. This protocol can be chosen from the Android platform, and is also used by Mozilla Thunderbird, Windows Live Mail and Apple Mail.

Configuring e-mail accounts for other devices, such as the Blackberry, works in a similar fashion to other smartphones. However, you also have the option to connect to a Blackberry Enterprise Server, which is similar to Microsoft Exchange. These Blackberry servers are at the core of "pushed" e-mail, which Blackberry pioneered for users to get their e-mail immediately when it reaches the mail server.

Troubleshooting E-mail Connections

If you have trouble connecting an e-mail account, try some of the following methods:

- Make sure the mobile device has Internet access. If connecting through the cellular network, make sure there is a decent reception.
- Verify that the username, password, and server names are typed correctly. Remember that the username is often the e-mail address itself.
- Check the port numbers. By default POP3 is 110, SMTP is 25, and IMAP is 143. However, network administrators might decide to use nondefault port numbers!

Note

There is a newer SMTP mail submission port, 587, that can be used by e-mail clients. Due to security concerns with port 25, you will likely see more of port 587 in the future.

- Double-check whether security is required in the form of SSL or TLS. For nonstandard port numbers and security configurations, check with your network administrator.

Exam Alert

Double-check all e-mail settings such as username, password, server name, and port number.

Synchronizing an Android Device to a PC

If you connect an Android-based mobile device to a PC via USB, Windows will most likely recognize it, and you will have a few options display on the Android screen, as shown in Figure 17.11.

The first option is Charge Only. Aside from charging the Android device by connecting it to an AC outlet, a PC's USB port can charge it. (Though it will probably take longer to charge.) This first option is the default, so if you need to charge a device only, you won't have to change this setting. We'll skip the second option for now and come back to it later. The third option is Disk Drive. If you want to display the contents of the mobile device's memory card within Windows you have to select this. Then, the device shows up as a

Removable Disk in Windows Explorer. From there, data can be copied back and forth between the PC and the mobile device as you usually would within Windows. Older Android devices required you to tap "mount" to have the phone show as a Removable Disk.

FIGURE 17.11 **PC Connection Options on Android**

ExamAlert

Know how to connect a mobile device to a PC and read its data.

You will also note USB tethering on the list. This allows you to share the mobile device's cellular network with the PC. The last item on the list is Internet Pass-through, which as mentioned previously allows you to use the PC's Internet connection on the mobile device.

Now, none of these so far allow you to synchronize information from the mobile device to the PC. Only the second option HTC Sync allows this synchronization, but with a caveat: The PC must have the appropriate synchronization software installed. Keep in mind that this software (and connection name) will be different depending on the manufacturer of the device. This example shows an HTC Evo smartphone.

Most synchronization software requires the PC have Windows XP or higher, 1 GB of RAM or more, USB 2.0 ports minimum, and 300 MB of free space on the hard drive. Syncing software is freely downloadable from the manufacturer's website.

HTC Sync for example can synchronize music, pictures, the calendar, bookmarks and more. This synchronization can be initiated from the mobile device or from the program on the PC. Documents, music, pictures and video will be synchronized by default to the Windows Libraries of the same names.

If you use the mobile device's built-in contacts and e-mail programs, the information within those programs will be transferred to the PC's corresponding programs. For example the Calendar and Contacts will be synchronized with Microsoft Outlook. However, for this mobile device, Gmail or Exchange contacts information will not be synchronized, nor will any other third-party data besides data that originates from, or is destined for, a Microsoft application.

However, not everyone uses synchronization software. Some people exclusively use Gmail on the Android platform. Google automatically synchronizes mail, contacts, and the Calendar so that you can view the information on the mobile device or on the PC (when connected to the Gmail website). However, because the data is stored on a Google server, security can be compromised. If you choose to do this, you should use an extremely strong password, change it every month or so, and use a secure browser when connecting to Gmail from your PC. The same people who use Gmail usually transfer data by simply mounting the mobile device as a disk drive in Windows. This effectively renders the synchronization software unnecessary for those people.

Third-party tools (such as Mark/Space) are available if a person wants to synchronize an Android device with a PC or MAC via Bluetooth or Wi-Fi. Standard Microsoft ActiveSync is not used to synchronize data between Android and Windows. However, Exchange ActiveSync can be used to synchronize e-mail, contacts, and calendars between an Android 2.0 mobile device and higher with an Exchange Server.

ExamAlert

Know the various ways to synchronize data between an Android and a PC.

Synchronizing an iPad2 to a PC

Before getting into synchronizing, let's talk about charging. The best way to charge an iPad is by plugging the AC adapter into an outlet. If the iPad is connected to a desktop computer via USB and is turned on, it will not charge.

However, if it is connected by USB and it is sleeping or off, it will slowly charge. If the computer is not equipped with a high-power USB port, this could take a long time. Regardless, Apple recommends plugging these devices into the AC outlet to charge.

If you plug an iPad into a PC via USB, Windows should automatically recognize it and install the driver for it. At that point you can move files between the PC and the iPad's memory card. The iPad shows up in Windows Explorer as Apple iPad directly inside of Computer.

To synchronize data such as contacts, calendars, and so on, PC users need to use iTunes for Windows. From iTunes a user would select Sync Contacts or Sync Calendars, for example. This information can be synchronized to Microsoft Outlook 2003 or higher, Windows Address Book (in Windows XP), and Windows Contacts (in Windows 7/Vista). Mac users benefit from the simplicity of synchronization across all Apple products. They can use iTunes or can use the iCloud to store, backup, and synchronize information across all Apple devices. This can be done by USB or via Wi-Fi if the various Apple devices are on the same wireless network. Calendar items can also be synced from the iPad itself by going to Settings > Mail, Contacts, Calendars. Then scroll down and select Sync, as shown in Figure 17.12.

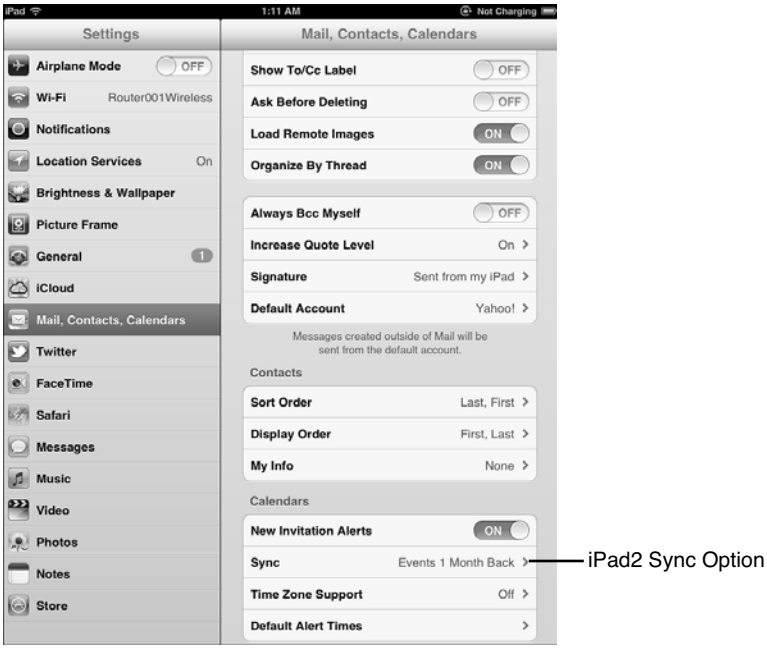


FIGURE 17.12 **Apple iPad2 synchronization example**

ExamAlert

Know the various ways to synchronize data between an Apple mobile device and a PC or Mac.

Synchronizing Other Devices

The two operating systems the CompTIA objectives are concerned with are Android and iOS. However, these are not the only players on the field! Let's mention a few other devices.

First of all, the Blackberry deserves some mention. For the longest time, this was the standard device a business person would use. It has lost some momentum, but you still see plenty of them in the field. Blackberry offers Desktop Software. Separate versions for PC and Mac are available at this link:

http://us.blackberry.com/apps-software/desktop/

The software works in a similar fashion to other synchronization software for Android or iOS.

And let's not forget about Microsoft mobile operating systems. Windows CE and Windows Mobile are commonly found in the transportation, medical, and surveying fields, as well as other niche markets that require rugged, waterproof devices. These devices synchronize to the PC by way of Microsoft ActiveSync (for Windows XP or earlier) and the Windows Mobile Device Center (Windows Vista or newer.) The Windows Mobile Device Center is available at this link:

http://www.microsoft.com/download/en/details.aspx?id=14

These programs can synchronize data between the mobile device and the PC via USB or Bluetooth connections. Microsoft does not allow synchronization over Wi-Fi as it is deemed a security issue.

Cram Quiz

Answer these questions. The answers follow the last question. If you cannot answer these questions correctly, consider reading this section again until you can.

220-802 Questions

1. Which of the following are valid Wi-Fi troubleshooting methods? (Select the two best answers.)
   - ❍ **A.** Power cycle the device.
   - ❍ **B.** Restart Bluetooth.
   - ❍ **C.** Use a static IP.
   - ❍ **D.** Make sure the device is within range.
   - ❍ **E.** Rename the SSID.

2. Which of the following connections requires a username, password, and SMTP server? (Select the two best answers.)

- ❍ **A.** Bluetooth connection
- ❍ **B.** Wi-Fi connection
- ❍ **C.** POP3 connection
- ❍ **D.** Exchange connection
- ❍ **E.** IMAP connection

3. What is the most common connection method when synchronizing data from a mobile device to a PC?

- ❍ **A.** Wi-Fi
- ❍ **B.** Bluetooth
- ❍ **C.** USB
- ❍ **D.** FireWire

4. When configuring a Wi-Fi connection what step occurs after successfully entering the SSID?

- ❍ **A.** Select POP3.
- ❍ **B.** Check if the device is within range of the WAP.
- ❍ **C.** Enter a passcode for the network.
- ❍ **D.** Scan for networks.

5. Which technology would you use if you want to connect a headset to your mobile phone?

- ❍ **A.** Bluetooth
- ❍ **B.** GSM
- ❍ **C.** Wi-Fi
- ❍ **D.** Exchange

6. Which of the following allows other mobile devices to share your mobile device's Internet connection?

- ❍ **A.** Internet pass-through
- ❍ **B.** Locator application
- ❍ **C.** IMAP
- ❍ **D.** Wi-Fi tethering

7. What would a user need to synchronize contacts from an iPad to a PC?

- ❍ **A.** Android Synchronization Application
- ❍ **B.** Google Play
- ❍ **C.** iTunes
- ❍ **D.** ActiveSync

Cram Quiz Answers

220-802 Answers

1. **A** and **D.** Valid Wi-Fi troubleshooting methods include power cycling the device and making sure that the mobile device is within range of the wireless access point. Bluetooth could possibly cause a conflict with Wi-Fi. If you suspect this, Bluetooth should simply be turned off. Static IP addresses are one thing you can check for when troubleshooting. Normally, the mobile device should obtain an IP address from a DHCP server. Renaming the SSID of the access point could cause problems for all clients trying to connect. However, you should make sure that the correct SSID was typed (if the connection were made manually.)
2. **C** and **E**. POP3 and IMAP e-mail connections require an incoming mail server (either POP3 or IMAP), and an outgoing mail server (SMTP.) Bluetooth and Wi-Fi connections do not require a username or SMTP server. Exchange connections require a username and password, but no SMTP server. The Exchange server acts as the incoming and outgoing mail server.
3. **C.** USB is the most common connection method used when synchronizing data from a mobile device to a PC. Though Wi-Fi and Bluetooth are also possible, they are less common. Few mobile devices have FireWire connections.
4. **C.** After you enter the SSID (if it's correct) you would enter the passcode for the network. POP3 has to do with configuring an e-mail account. If you have already entered the SSID, then you should be within range of the wireless access point (WAP). Scanning for networks is the first thing you do when setting up a Wi-Fi connection.
5. **A.** The Bluetooth standard is used to connect a headset and other similar devices over short range to a mobile device. GSM is used to make voice calls over cellular networks. Wi-Fi is used to connect mobile devices to the Internet. Exchange is a Microsoft E-mail server; some mobile devices have the capability to connect to e-mail accounts stored on an Exchange server.
6. **D.** Wi-Fi tethering allows a mobile device to share its Internet connection with other Wi-Fi capable devices. Internet pass-through is when the mobile device connects to a PC to share the PC's Internet connection. Locator applications are used to find lost or stolen mobile devices through GPS. IMAP is another e-mail protocol similar to POP3.
7. **C.** PC users need iTunes to synchronize contacts and other data from an iPad to a PC. There are many Android sync programs, but they do not work on Apple devices. Google Play is a place to get applications and other items. ActiveSync is the older Microsoft sync program used to synchronize Windows CE and Mobile to PCs.

Mobile Security

Mobile devices need to be secure just like any other computing devices. But due to their transportable nature, some of the security techniques will be a bit different. I recommend that you prepare for the possibility of a stolen, lost, damaged, or compromised device. The following methods can help you to recover from these problems and also aid you in preventing them from happening.

Stolen and Lost Devices

Because mobile devices are expensive and could contain confidential data, they become a target for thieves. Plus, they are small and easy to conceal, making them easier to steal. But there are some things you can do to protect your data and attempt to get the mobile device back.

The first thing a user should do when receiving a mobile device is to set a *passcode*, which is a set of numbers. This is one of several types of *screenlocks*. Locking the device makes it inaccessible to everyone except experienced hackers. The screen lock can be a pattern that is drawn on the display, a PIN (passcode), or a password. A strong password will usually be the strongest form of screenlock.

This can be accessed on an Android device by going to Settings > Security. This screen on a typical Android smartphone is shown in Figure 17.13.

FIGURE 17.13 **Android security screen**

You can also select how long the phone will wait after inactivity to lock. Generally this is set to 3 or 5 minutes or so, but in a confidential environment you might set this to Immediate.

The next option on the Security screen is Visible Passwords. If check marked, this shows the current letter of the password being typed by the user. This type of setting is vulnerable to shoulder surfers (people looking over your shoulder to find out your password) and should be deselected. When deselected, only asterisks (*) are shown when the user types a password.

ExamAlert

Know how to configure a screenlock in Android and how to disable visible passwords.

Passcode locking can be accessed on an iPad device by going to Settings > General > and tapping Passcode Lock. This displays the Passcode Lock screen. Tap Turn Passcode On to set a passcode, as shown in Figure 17.14. Be sure that the Auto-Lock on the previous screen is set to an amount of minutes. If it is set to Never, the device never sleeps, negating the security of the passcode, and using valuable battery power. The default setting is 2 minutes. You'll also note in Figure 17.14 that Simple Passcode is enabled. This allows 4-digit numeric passcodes only. As this is probably not going to be secure enough for an organization, you should turn the Simple Passcode option off; that will allow alphanumeric passwords to be entered.

FIGURE 17.14 iPad2 passcode lock screen

ExamAlert

Know how to configure a passcode in iOS.

Aside from the default timeout, devices can also be locked by pressing the power button quickly. If configured, the passcode must be supplied whenever a mobile device comes out of a sleep or lock state and whenever it is first booted.

If a person fails to enter the correct passcode after a certain amount of attempts, the device locks temporarily and the person has to wait a certain amount of time before attempting the passcode again. For example, by default on the Android this is 5 attempts; if they all fail the user has to wait 30 seconds. If the person fails to enter the correct passcode again, the timeout increases on most devices. After a certain amount of attempts, the device either needs to be connected to the computer it was last synced to, or has to be restored to factory condition with a hard reset (which can wipe the data.)

ExamAlert

Understand the consequences of entering an incorrect passcode too many times.

Some devices (such as the iPhone) have a setting where the device will be erased after a certain amount of incorrect password attempts (10 in the case of the iPhone). There are also third-party apps available for download for most mobile devices that can wipe the data after x number of attempts. Some apps configure the device to automatically take a picture after 3 failed attempts and e-mail the picture to the owner.

There's an app for virtually everything. For example, say the device was lost or stolen. If the user had previously installed a locator application, such as Where's my Droid, Lookout Mobile Security, or Find iPhone, and the GPS/Location Services was enabled on the device, then the user would track where the device is. At that point, the organization would decide whether to get the police involved.

ExamAlert

Know what locator applications are.

Now, even if you track your mobile device and find it, it might be too late. A hacker can get past passcodes and other screen locks. It's just a matter of time

before the hacker has access to the data. So, an organization with confidential information should consider a remote wipe program. As long as the mobile device still has access to the Internet, the remote wipe program can be initiated from a desktop computer, which will delete all the contents of the remote mobile device. Examples of software that can accomplish this include: Google Sync, Google Apps Device Policy, Apple's Data Protection, and third-party apps such as Mobile Defense. In some cases, such as Apple's Data Protection, the command that starts the remote wipe must be issued from an Exchange server or Mobile Device Management server.

ExamAlert

Know the remote wipe programs available for mobile devices.

You should also have a backup plan in place as well so that data on the mobile device is backed up to a secure location at regular intervals. This way, if the data needs to be wiped, you are secure in the fact that most of the data can be recovered. The type of remote wipe program, backup program, and policies regarding how these are implemented will vary from one organization to the next. Be sure to read up on your organization's policies to see exactly what is allowed from a mobile security standpoint.

Compromised and Damaged Devices

Theft and loss aren't the only risks a mobile device faces. We should protect against the chance that a mobile device is damaged, or if the device's security is compromised.

Many organizations implement backup and remote backup policies. iOS devices can be backed up to a PC via USB connection and by using iTunes. Also, they can be backed up remotely to the iCloud. In addition, there are other third-party apps for remote backup such as iDrive and Mozy. Information can even be restored to newer, upgraded iOS devices. Android (as of the writing of this book) doesn't allow a complete backup without rooting the phone (which I don't recommend.) However, almost all the data and settings can be backed up in a collection of ways. First, the Android Cloud backup can be used to backup e-mail, contacts, and other information. However, if you use Gmail, then e-mail, contacts, and calendars are backed up (and synchronized) to Google servers. If a mobile device is lost, the information can be quickly accessed from a desktop computer or other mobile device. Unlike Apple, Android applications can be backed up, as long as they are not copy-protected, with an app such as

Astro. Android settings can be backed up and restored from Settings > Privacy. If you choose not to use the Android cloud to backup files, or the synchronization program that came with the device, then there are plenty of third-party apps (such as iDrive, Mozy, HandyBackup, and so on) that can be used to backup via USB to a PC, or to backup to the cloud.

One way to protect mobile devices from compromise is to patch or update the operating system. By default, you will be notified automatically about available updates on Android and iOS-based devices. However, you should know where to go to manually update these devices as well. For Android go to Settings > System Updates > Software Update (or similar path). From here tap Check Now. If you have a connection to the Internet, you will receive any information concerning system updates; an example is shown in Figure 17.15.

FIGURE 17.15 **Android system update available**

ExamAlert

Know how to check for, and perform, Android OS updates.

As you can see in the figure, the system update has an important new security feature that should be installed right away (which I will do when I finish writing this sentence!) Security patches are a large percentage of system updates because there are a lot of attackers around the world that want to compromise

the Android operating system. But let's be real—attackers will go for any OS if it catches their fancy, be it Android, iOS or even Windows!

Updates for iOS can be located at Settings > General > Software Update. As shown in Figure 17.16, this iOS needs to be updated from 5.0 to 5.1 and should be done as soon as possible to patch up any security flaws, and make the best use of the system.

FIGURE 17.16 **iOS system update available**

ExamAlert

Know how to check for, and perform, iOS updates.

Updates are great, but they are not created to specifically battle viruses and other malware. So, just like there is antivirus software for PCs, there is also AV software for mobile devices. These are third-party applications that need to be paid for, downloaded, and installed to the mobile device. Some common examples for Android include McAfee's Virusscan Mobile, AVG, Lookout, Dr. Web, and NetQin.

iOS works a bit differently. iOS is a tightly controlled operating system. One of the benefits of being a closed-source OS is that it can be more difficult to write viruses for, making it somewhat more difficult to compromise. But there is no OS that can't be compromised. For the longest time there was no

antivirus software for iOS. That is until 2011 when a type of jailbreaking software called jailbreakme used a simple PDF to move insecure code to the root of the device causing a jailbreak.

iOS *jailbreaking* is the process of removing the limitations that Apple imposes on its devices that run iOS. This enables users to gain root access to the system and allows the download of previously unavailable applications and software not authorized by Apple.

ExamAlert

Understand the term jailbreaking for the exam.

Jailbreakme is used to gain root level access and take control of the device without the user's consent. Finally, Apple consented to the first antivirus software for iOS, Intego's VirusBarrier, a paid download through the App Store. Any AV software for Android or iOS should be checked regularly for updates.

For large organizations that have many mobile devices, a *Mobile Device Management (MDM)* suite can be implemented. McAfee, and many other companies from AirWatch to LANDesk Mobility Manager to Sybase, have Mobile Device Management software suites that can take care of pushing updates and configuring hundreds of mobile devices from a central location. Decent quality MDM software will secure, monitor, manage, and support multiple different types of mobile devices across the enterprise.

Stopping Applications

Applications that are opened on a mobile device will continue to run in the background unless they are specifically turned off within the app or within the OS.

To turn off apps (or services) that are running on an Android-based system, go to Settings > Applications > Running Services. That displays all the currently running services and applications, as shown in Figure 17.17.

You can see in the figure that there are several apps and services running including the droid VNC server, Calendar, and a GPS program. To see all the services and apps, just scroll down. As with PCs, mobile device apps use RAM. The bottom of the figure shows that 194 MB of RAM is currently being used, and 139 MB of RAM is free. The more RAM that is used by the mobile device,

the worse it will perform: it will slow it down, and eat up battery power. So, to close an app, you would simply tap it and tap Stop. You can also stop services or processes in this manner (for example HTC DM in the figure), but this might require a Force Stop. If you are not absolutely sure what the service is, do not initiate a Force Stop, as it can possibly cause system instability.

FIGURE 17.17 **Services and apps running on an Android**

To force quit an app on an iOS-based device, press and hold the Sleep/Wake button for a few seconds until a red slider appears. Then press and hold the home button until the app quits.

ExamAlert

Understand how to stop apps on Android and Apple devices.

There are third-party apps that can close down all of the apps in one shot if you need to save time. These include Task Manager, TasKiller, and AppControl.

If an application is causing the device to lock up and you can't stop the app, a soft reset or a hard reset will be necessary.

Initiating Resets

A soft reset is done by simply powering off the mobile device and powering it back on. This resets the drivers and the OS. So, soft resets are similar to shutting down a PC and powering it back up. Some technicians will also call this a power cycle. The soft reset can help when certain applications are not functioning properly, or if network connectivity is failing. If a smartphone is still locked up when it is restarted, try pulling the battery, replacing it, and restarting the phone again. In fact, for Blackberry devices, soft resets *require* a battery pull.

iOS-based devices can do a variety of more advanced software resets beyond a simple power-cycle, such as Reset All Settings, Erase All Content, Reset Networking settings, and so on. These are available by tapping Settings > General > Reset.

Hard resets should be initiated only when things have gone terribly wrong. For example, if hardware or software has been compromised, or has failed, and a soft reset does not fix the problem. You want to make sure that all data is backed up before performing a hard reset, as some hard resets will reset the mobile device back to the original factory condition.

Exam Alert

Warning!! All data will be wiped when a hard reset is initiated on an Android device!

Hard resets vary from one device to the next. For example, most Android-based systems such as the HTC smartphone mentioned previously use the following steps:

1. Turn the power off. If the device is locked (frozen), pull the battery out and reinsert it.
2. Hold the Volume Down button, and press and release the Power button.
3. This displays a menu that allows for Fastbook, Recovery, Clear Storage, and Simlock. Select Clear Storage by pressing the Volume Down button.
4. Press and release the Power button.
5. Confirm by pressing Volume Up for Yes or Volume Down for No.

At this point, the device will be reset and you will have to restore data and settings from backup.

Exam Alert

Know how to perform soft and hard resets on Android devices.

Unlike many other mobile devices, hard resets on iOS-based devices do not delete data. They instead stop all apps, and reset the OS and drivers. This can be accomplished with the following steps:

1. Make sure that the device has at least 20 percent battery life remaining. (This process could take some time, and you don't want the battery to discharge completely in the middle of it.)
2. Press the Sleep/Wake and Home buttons simultaneously for 10 seconds or until the Apple logo appears. (Ignore the red slider).
3. When the logo appears, the hard reset has been initiated. It may take several minutes to complete.

To fully reset an iOS-based device such as the iPad2 to factory condition, you need to go to Settings > General > Reset > Erase all Content and Settings. Another way to do this is to connect the iOS device to a computer via USB and open iTunes on the computer. Then, select the iPad2 option, Summary, and click Restore. Regardless of the method you choose, next, initiate a hard reset to complete the procedure.

ExamAlert

Remember how to reset settings and erase all content on iOS devices.

As you have seen with Android and Apple, the types of resets vary from one device to the next, so be sure to go to the manufacturer's website to find out exactly what the various resets do for your mobile device, and how you can perform them.

Cram Quiz

Answer these questions. The answers follow the last question. If you cannot answer these questions correctly, consider reading this section again until you can.

220-802 Questions

1. You want to prevent a person from accessing your phone while you step away from your desk. What should you do?
   - ❍ **A.** Implement remote backup.
   - ❍ **B.** Set up a remote wipe program.
   - ❍ **C.** Configure a screen lock.
   - ❍ **D.** Install a locator application.

2. What does the iOS Simple Passcode allow a person to enter?

- ❍ **A.** 4-letter code
- ❍ **B.** 6-number PIN
- ❍ **C.** 4-digit passcode
- ❍ **D.** Alpha-numeric passcode

3. What do third-party apps such as Find iPhone rely on?

- ❍ **A.** Passcode
- ❍ **B.** Google Apps Device Policy
- ❍ **C.** Bluetooth
- ❍ **D.** GPS

4. Which of the following can be described as removing limitations on iOS?

- ❍ **A.** Rooting
- ❍ **B.** Jailbreaking
- ❍ **C.** Geotracking
- ❍ **D.** AV software

5. An application won't close on an Android smartphone. You've tried to Force Stop it to no avail. What should you do?

- ❍ **A.** Hard reset the device.
- ❍ **B.** Stop the service in Running Services.
- ❍ **C.** Soft reset the device.
- ❍ **D.** Bring the device to an authorized service center.

6. Your organization is concerned about a scenario where a mobile device with confidential data is stolen. What should you recommend first? (Select the best answer.)

- ❍ **A.** Remote backup application
- ❍ **B.** Remote wipe program
- ❍ **C.** Passcode locks
- ❍ **D.** Locator application

7. You are concerned with the possibility of jailbreaks on your organization's iPhones, and viruses on the Android-based devices. What should you implement?

- ❍ **A.** AV software
- ❍ **B.** Firewall
- ❍ **C.** Mobile Device Management
- ❍ **D.** Device reset

Cram Quiz Answers

220-802 Answers

1. **C.** You should configure a screen lock: either a pattern drawn on the screen, a PIN, or a password. Remote backup, remote wipe, and locator applications will not prevent a person from accessing the phone.
2. **C.** The iOS Simple Passcode allows only a 4-digit numeric passcode. To enter alpha-numeric passwords, you need to disable Simple Passcode.
3. **D.** Third-party locator apps such as Find iPhone and Where's my Droid rely on GPS to locate the device. Passcodes are used to prevent unauthorized users from accessing the mobile device. Google Apps Device Policy can initiate a remote wipe on a mobile device. Bluetooth is used so the mobile device can communicate with other devices over short range.
4. **B.** Jailbreaking is the process of removing the limitations of an iOS-based device so that the user gets superuser abilities. Rooting is a similar technique used on Android mobile devices. Geotracking is the practice of tracking a device over time. AV software is antivirus software, used to combat malware.
5. **C.** If you've already tried to stop the application within Running Services, attempt a soft reset. Pull the battery if the application is frozen. Hard resets on Android devices should be used only as a last resort as they will return the device to factory condition—wiping all the data. The question said that the application won't close, not a service, though you could try finding an underlying service that might be the culprit. But try resetting the device before doing this or bringing it to an authorized service center.
6. **B.** The remote wipe application is the most important one listed. This will prevent a thief from accessing the data on the device. Afterward, you might recommend a backup program (in case the data needs to be wiped), as well as passcode locks and a locator application.
7. **A.** You should implement antivirus (AV) software. This can protect against viruses and other malware as well as jailbreaks on Apple devices. As of the writing of this book, firewalls for mobile devices are not common, but that could change in the future. Mobile Device Management (MDM) is software that runs at a central computer enabling a user to configure and monitor multiple mobile devices. Device resets are used to restart the mobile device, or to reset it to factor condition depending on the type of reset, and the manufacturer of the device.

Index

Numbers

A

B

C

D

E

F

G

H

I

J–K

L

M

N

O

P

Q

R

S

T

U

V

W

X–Y–Z