CHAPTER 9

Understanding Mobile Devices

In this chapter, you'll learn about the different types of mobile devices, with an emphasis on tablets such as Apple's iPad. These devices have enjoyed great popularity in recent years, and it's clear that they are here to stay. This chapter compares tablets to laptops, compares different operating systems on the devices, and covers methods used to connect them. You'll also learn some basics about using these mobile devices and important information about how you can secure them.

Exam 220-801 objectives in this chapter:

- 1.7 Compare and contrast various connection interfaces and explain their purpose.
  - Speeds, distances and frequencies of wireless device connections
    - Bluetooth
    - IR
    - RF
- 2.7 Compare and contrast Internet connection types and features.
  - Cellular (mobile hot spot)

Exam 220-802 objectives in this chapter:

- 3.1 Explain the basic features of mobile operating systems.
  - Android vs. iOS
    - Open source vs. closed source/vendor specific
    - App source (app store and market)
    - Screen orientation (accelerometer/gyroscope)
    - Screen calibration
    - GPS and geotracking
- 3.2 Establish basic network connectivity and configure email.
  - Wireless / cellular data network (enable/disable)

- Bluetooth
  - Enable Bluetooth
  - Enable pairing
  - Find device for pairing
  - Enter appropriate pin code
  - Test connectivity
- Email configuration
  - Server address
    - POP3
    - IMAP
    - Port and SSL settings
  - Exchange
  - Gmail

- 3.3 Compare and contrast methods for securing mobile devices.
  - Passcode locks
  - Remote wipes
  - Locator applications
  - Remote backup applications
  - Failed login attempts restrictions
  - Antivirus
  - Patching/OS updates
- 3.4 Compare and contrast hardware differences in regards to tablets and laptops.
  - No field serviceable parts
  - Typically not upgradeable
  - Touch interface
    - Touch flow
    - Multitouch
  - Solid state drives
- 3.5 Execute and configure mobile device synchronization.
  - Types of data to synchronize
    - Contacts
    - Programs
    - Email
    - Pictures

- Music
- Videos

- Software requirements to install the application on the PC
- Connection types to enable synchronization

REAL WORLD **LOCATING YOUR LOST iPAD**

Not too long ago, a friend of mine lost his iPad. He used it all the time and was sure that someone had stolen it. When he mentioned it to me a few days later, I asked if he had enabled Location Services. His puzzled look indicated that he didn't know what I was talking about, but he did say that when he bought it, his brother-in-law helped him set it up. It was possible that Location Services was enabled and that we could find it.

We ended up downloading a location app, and he signed in using his information. Within a couple of minutes, we pinpointed the exact location of his iPad. Interestingly, it was at my house. I assured him I didn't have it but suggested it might be in his car, which was in my driveway. After a few minutes of searching, he found it beneath some papers under a car seat.

This location feature is common on most mobile devices, not just iPads. Not only can the device be located but you can also send signals to erase all the data or lock the device. Knowing what features are available will help you be a better technician, even if you don't have a mobile device of your own.

Tablets vs. Laptops

Tablets are handheld devices such as the Apple iPad, the Samsung Galaxy Tab, or the HP Touchpad. They have a touchscreens allowing you to operate them without a keyboard or mouse. Instead you use gestures (described later in this chapter) to operate them.

These devices use solid state storage drives and flash memory, providing excellent speed when being rebooted and while running applications. Solid state drives (covered in Chapter 4, "Comparing Storage Devices") are lighter and consume less power. This allows the rechargeable battery to be smaller, and the overall weight of a tablet is less than that of a typical laptop.

Tablets commonly include Wi-Fi capability, allowing them to connect to a wireless network. Some tablets also include the ability to access a cellular network for Internet access. When using the cellular network, the user needs to sign up with a wireless provider such as Verizon or AT&T. The cellular network used by tablets is the same cellular network used by smartphones.

Hardware for tablets is rarely upgradable or serviceable. If you buy a 16-GB iPad and later decide you want a 64-GB iPad, you need to buy a new one. If it breaks, you might be able to

send it back to the company to get it serviced, but this can be quite expensive if it isn't under warranty.

In contrast, laptops are bigger, include more hardware, and are upgradable and serviceable. Laptops include keyboards along with the display screens, but tablets use a display keyboard that allows you to touch the keys on the touchscreen. You can purchase laptops with display screens as big as 17.3 inches, which are much bigger than the 9.7-inch diagonal display of an iPad or the 10.1-inch diagonal display of the Galaxy Tab.

NOTE **TABLET SIZES**

Tablet display sizes are commonly quoted as the diagonal display size. This is the length of the screen from an upper corner to the opposite lower corner and includes only the viewable area.

Table 9-1 summarizes some of the important differences between tablets and laptops related to the A+ exams.

TABLE 9-1 Comparing Tablets and Laptops

	Tablet	Laptop
Upgrades	Rarely upgradable	Memory and hard drives easily upgradable.
Repairs	No field-serviceable parts	Technicians can open and replace components.
Hard drives	Solid state drives	Most use traditional hard drives. Some can use solid state drives but these are not as common.
Interface	Touch interface	Keyboard and mouse.

EXAM TIP

Tablets do not have field-serviceable parts and are rarely upgradable. They include solid state drives, contributing to their high performance and lighter weight.

Tablets have many common features that aren't always in laptops. The following sections cover these features.

Accelerometers and Gyroscopes

Many devices include an *accelerometer* and a Micro-Electro-Mechanical System (MEMS) *gyroscope* to measure the orientation of the device. In many devices, a single chip includes both. The output of the accelerometer and gyroscope indicates the orientation of the device, and the device can use this information to change the display.

The most basic use of accelerometers and gyroscopes is to determine whether the device is positioned horizontally or vertically in front of a user. If the user changes the orientation

of the device, the software can automatically switch the screen orientation to landscape or portrait mode.

> ***NOTE*** **LANDSCAPE AND PORTRAIT MODES**
>
> **Landscape mode is used when the device is held horizontally, and portrait mode is used when the device is held vertically. The automatic change in orientation can be disabled in many devices by using a Lock Rotation setting.**

A more sophisticated use is to sense the exact orientation of the device and change the display to match. For example, Star Walk (shown in Figure 9-1) is an application that shows information about satellites, planets, stars, constellations, and more.

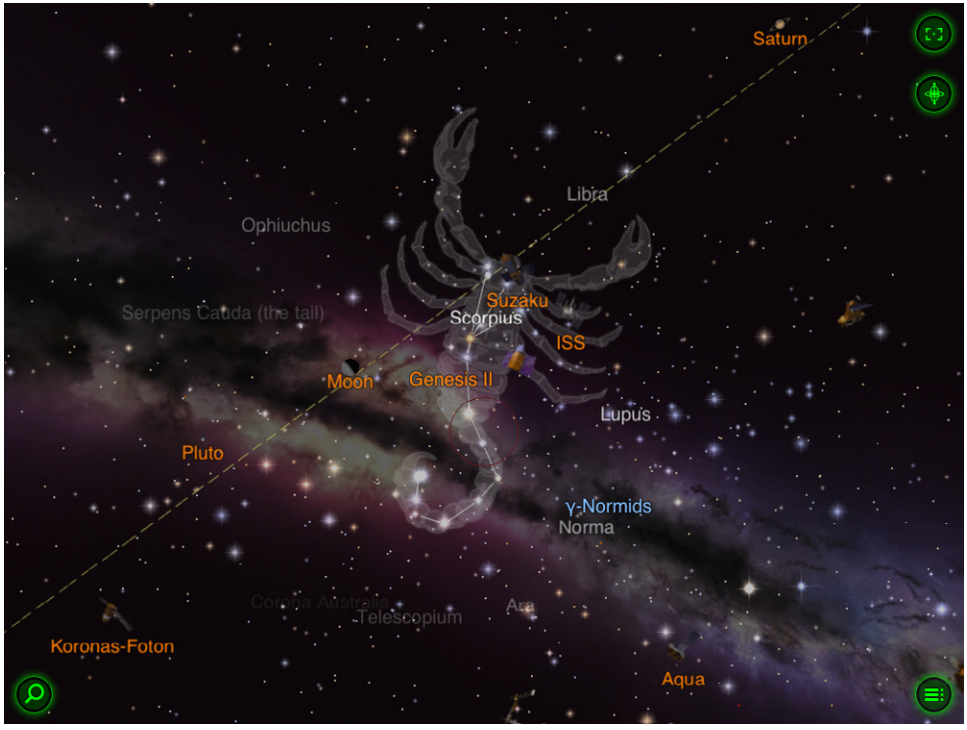

FIGURE 9-1 Star Walk application screen.

If you hold the tablet up with the back pointing toward the sky, the display shows the names of everything in that direction. Move the device in any direction, and the display automatically changes to show you what's in the new direction. If you were looking for Saturn, you could scan the sky with the back of the tablet until Saturn was displayed. You could then look at the sky in that direction. Similarly, many games use this feature. For example, in some racing games, you can hold the tablet like a steering wheel to make turns within the game.

EXAM TIP

Tablets include accelerometers and/or gyroscopes to sense the position of the device. Applications and the operating system use the output of these components to automatically adjust the display. This includes switching from landscape to portrait mode or making incremental changes in the display when the device is moved.

GPS

Most tablets and smartphones include access to a *Global Positioning System (GPS)*, which can be used to determine the exact location of the device. The location is used by many apps on tablets to provide location-specific data. For example, if you use Google Earth, this feature allows GPS to zoom in on your location. Similarly, weather service apps use the GPS to provide local weather reports.

Geotracking

Geotracking is the practice of recording the location of a mobile device and using it to track the movements of the device. The location is identified based on cell towers accessed by the device and can provide specific information including latitude, longitude, the azimuth or compass heading from the tower, and the time and date. It can also record information if users connect to geographically tagged Wi-Fi hot spots.

NOTE **APPLE'S USE OF GEOTRACKING**

Apple has stated this data is used for apps that need location-based information. They mention that calculating a phone's location by using only GPS satellite data can take several minutes, but the time can be reduced to a few seconds by using the logged location data.

Mobile devices store this data in a file on the device, and if someone knows how to retrieve it, they can track the location of the device over a period of time. Some forensics classes teach specifically how to retrieve this information from a device. Similarly, some applications can retrieve the data from a device.

There are also apps that you can install on devices to track their movement and location. Parents sometimes use them to keep track of their children, and employers have used them to keep track of employer-supplied devices.

Screen Calibration

In some cases, the touchscreen can become uncalibrated. You might find that instead of touching directly on an item, you have to touch somewhere else close to the item. For example, if you touch a button on the screen, it doesn't respond, but if you touch to the right

of the button, it works. This isn't common with many current tablets but has been an issue with tablets and devices using touchscreens in the past.

If the device needs to be calibrated, you need to follow the directions for the device to start the calibration program. For example, on one version of an Android Samsung tablet, you start the screen calibration program by holding the menu button down for 10 seconds.

After the calibration program starts, you see a circle or prompt displayed somewhere on the screen that you need to touch. Touch it, and another circle appears with a prompt to touch it. It's common for the calibration program to display this circle in each of the four corners and at the center of the screen. Each time you touch the circle, the device records this as the correct calibrated location. After touching the last circle, the screen is calibrated.

Quick Check

1. **What's the difference in upgradability between a laptop and a tablet?**
2. **What is used to identify the location of a device?**

Quick Check Answers

1. **Tablets are not upgradable.**
2. **GPS. Geotracking can track the movement of a device.**

Comparing Operating Systems

The primary operating systems used on mobile devices are from Apple, Google, and Microsoft. Apple uses iOS, Google uses Android, and Microsoft uses Windows-based operating systems.

These operating systems are used on tablets and smartphones. A smartphone is a mobile device that includes additional features beyond making phone calls. Some of the common features of smartphones today include surfing the Internet, sending and receiving email, taking pictures with built-in digital cameras, and playing music as an MP3 player does. Smartphones often include other *personal digital assistant (PDA)* features, such as contact lists and/or an address book, calendar and appointment lists, and note-taking capabilities.

The following sections describe the basics of the operating systems and some key differences between them.

Open Source vs. Closed Source

When talking about mobile operating systems, it's important to understand the basic differences between *open source* and *closed source* software. Closed source software is sometimes referred to as *vendor-specific*, although this term isn't as common.

The primary differences are the availability of the code to the public and the cost to use the code.

- **Open source.** Open source software is code that is freely available to anyone. Developers have access to the code and can modify, improve, and at times, freely redistribute it. The Android operating system is open source software, and it was derived from the open source Linux operating system.
- **Closed source/vendor-specific.** Closed source software is code that is not freely available to the public but is instead protected by the company that developed it. It is often viewed and protected as a trade secret or intellectual property, and any usage of the software is subject to restrictions. Both the Apple iOS and Microsoft Windows operating systems are closed source operating systems, although the licenses are different.

EXAM TIP

While you can also find open source and closed source applications, the A+ 220-801 exam is focused only on understanding the differences between open source and closed source operating systems. More specifically, you should know that Android is open source and the Apple iOS is closed source.

iOS

The *iOS* is the operating system used on Apple products including iPhones, iPads, iPod Touch, and Apple TV. A unique characteristic of the iOS is that Apple does not let anyone but Apple use it. This is the same philosophy they've employed since their early Apple and Macintosh computers. If you want to use the Mac OS X operating system, buy a Mac from Apple. If you want to use iOS, buy an Apple product.

Additionally, Apple controls all software sales through the Apple App Store. Therefore, if you want to buy an app, you purchase it through their store.

The benefit to users is that they are less likely to download malicious software from the App Store. The benefit to Apple is that they receive about 30 percent from every sale. With enough 99-cent apps, this starts to add up. Based on a recent query, Apple's stock market value of over 500 billion dollars (yes, that's a *B* as in *billion*), this strategy seems to be working for them, at least for now.

NOTE **iPHONE OS TO iOS**

Apple's iOS was previously called iPhone OS. Apple began using the lowercase *i* on its products in 1998 with the iMac. Cisco uses the Cisco IOS (shortened from *Internetwork Operating System* with an uppercase *I*) for networking devices. However, iOS and IOS are two completely different operating systems.

Android

The *Android* operating system is a Linux-based operating system, but it's not owned by a single company. Google purchased Android, Inc., in 2005 and ultimately came out with the Android operating system in 2007. Google leads the Open Handset Alliance (OHA), a consortium of 84 companies that work together to develop open standards for mobile devices, and the Android operating system is a major product developed by OHA. Currently, the Android Open Source Project (AOSP) maintains and develops improvements for Android.

As mentioned previously, Android is an open source operating system, and any hardware developer can use it to create a device with Android as the base operating system. There is no obligation to pay Google, the OHA, or AOSP for Android. This has resulted in an explosion of devices running the Android operating system, including smartphones (such as Droids), tablet computers (such as the Kindle Fire or the Samsung Galaxy Tab), and many more.

As of February 2012, the Android operating system was reportedly running on over 300 million smartphones and tablets worldwide. Some experts expect Android-based tablets to exceed sales of the iPad by 2015.

Windows

The Windows Phone operating system is used on smartphones such as Windows Phone 7. Additionally, most Windows desktop operating systems can run on tablets. For example, all versions of Vista and Windows 7 can run on tablets, except for the Starter editions. Similarly, Windows 8 can run both on tablets and on PCs. Windows XP had a dedicated version called Windows XP Tablet PC Edition that ran on tablets.

Microsoft licenses the operating system to hardware developers. These hardware developers can then design the hardware around the operating system, and they include the operating system license as part of the price.

Windows 8 is in a different category. It can run on desktops, and Microsoft has developed its own tablets known as the Surface and the Surface Pro. However, CompTIA had already released the objectives for the A+ exam before Windows 8 was released, and it stated that Windows 8 will not be on these exams. CompTIA can change its mind later and decide to add Windows 8. If it does, I'll blog about it at *blogs.getcertifiedgetahead.com*.

EXAM TIP

As a comparison between the three mobile operating systems, Apple does not license iOS to anyone, the Android operating system is free for everyone, and Microsoft licenses the operating system to hardware vendors.

Application Sources

Applications are what make these devices useful, and some apps really help people be more productive. Some, like Angry Birds, are just fun. There have been over 500 million downloads of Angry Birds (including the Angry Bird spinoffs), indicating that many people are using mobile devices for some fun. A logical question is, "Where can you get these apps?"

Apps for mobile devices are available almost exclusively online. The user connects to the store with the device and makes a purchase, and the app is immediately downloaded and installed. For the iOS, Android, and Windows operating systems, the primary application sources are:

- **Apple App Store**. Links directly to Apple's App Store are included in Apple mobile devices. Users can click the link, connect, shop, and buy. Apple-based apps are not easily available through other sources. Figure 9-2 shows the App Store on an iPad.

FIGURE 9-2 App Store as seen on an iPad.

- **Google Play.** Android-based apps are available through Google Play: *https://play.google.com/store*, and other sources. Google Play was previously called Android Marketplace. Other sources for Android apps include Amazon.com in the Appstore for Android section, Mobihand.com, and Handango.com.

- **Windows Store and Windows Phone Marketplace**. Windows apps are available through the Windows Store and the Windows Phone marketplace: *http://www.windowsstore.com/* and *http://www.windowsphone.com/marketplace*. As with other mobile stores, users can connect to them from within a mobile device. Users can also use a regular browser to connect to the marketplace and purchase applications. These applications are then synchronized to their devices.

NOTE **ANDROID AND GOOGLE PLAY STORE**

It is possible to configure Android-based devices so that they can download only apps from the Google Play store. This adds an element of security because only developers with an account can upload apps to Google Play.

Application developers who create an app for one device must rewrite the code for other devices. For example, an app that runs on an iOS-based device will not run an on Android-based device until the developers modify the code to match the Android operating system. However, when developers recode the app, you often can't tell the difference between the functionality on the different devices.

Quick Check

1. **What operating system is used on Apple devices?**
2. **What is the major difference between the Android operating system and the operating system used on Apple devices?**

Quick Check Answers

1. **iOS.**
2. **Android is open source, while the iOS is closed source and vendor-specific.**

Connectivity

Mobile devices have the ability to connect wirelessly to an outside network by using one or more different technologies. As mentioned previously, many mobile devices include either Wi-Fi capability or cellular access. Two other connectivity methods are Bluetooth and infrared.

RF (Wireless)

Radio frequency (RF) connections on mobile devices enable the devices to connect to a wireless network. If your mobile device supports wireless connections and a wireless network is in range, you can configure the device to connect to the wireless network. Almost all mobile devices include this ability.

When connected, it will have access to the same resources as other devices on the wireless network. For example, you can connect smartphones and tablets to wireless networks and then use the network to surf the Internet or answer email. Wireless networks are covered in more depth in Chapter 23, "Exploring Wireless Networking." That chapter includes the information you need to connect any device to a wireless network.

Cellular

Many mobile devices can tap into the same cellular network used by smartphones. The cellular network has been steadily improving and currently provides speeds up to 1 Gbps in some areas. Cellular has gone through the following generations, with each generation providing an improvement over the previous one:

- **1G (first generation).** These were analog phones that had no digital capabilities.
- **2G (second generation).** These were the first generation of digital phones, and 2G is still used in some rural areas.
- **3G (third generation).** A large portion of cellular devices connect with 3G today, and the 3G networks are widely available in both urban and rural areas. Telecommunications companies are regularly updating the capabilities of the cellular towers and steadily improving the service.
- **LTE (Long Term Evolution).** LTE is a standard that is an improvement over 3G but doesn't necessarily meet the requirements of 4G. Some LTE networks are marketed as 4G LTE but don't fully meet the specifications of a 4G network.
- **4G (fourth generation).** 4G networks are available in many major cities and major metropolitan areas but not in rural areas. 4G is sometimes called WiMax.

A subscription is required to use these cellular data services. If you have a smartphone or a tablet that includes cellular access, you can pay additional money for these data services. They give you Internet access anywhere that you have cellular access. Plans often limit how much data you can download in a month, with limits such as 3 GB or 5 GB. If you exceed the limit, you're charged more.

EXAM TIP

It takes power to periodically communicate with cellular towers and wireless networks. You can conserve the battery by disabling these connections when you're not using them. This is very effective with tablets, and it increases the amount of time you can use the tablet before recharging it. You can also limit bandwidth usage by disabling the connection.

In contrast, if you have a wireless capability, you don't have to pay a monthly subscription fee. Anywhere there's a wireless network and you have the means to connect you can do so without paying a subscription fee.

Mobile Hotspot

Many wireless providers also sell portable wireless devices that act as hot spots. They're commonly called MiFi (pronounced My Fye, similar to Wi-Fi). They can connect to the Internet by using the cellular network, and they provide access to up to five other wireless users.

Bluetooth

Bluetooth is a type of wireless protocol used with many mobile devices. Devices that support Bluetooth are called *Bluetooth-capable* or *Bluetooth-enabled* devices, and it is common to use Bluetooth to create personal area networks (PANs).

> ***MORE INFO*** **CHAPTER 18**
>
> **Chapter 18, "Introducing Networking Components," covers other types of networks, including local area networks (LANs), wireless local area networks (WLANs), wide area networks (WANs), and metropolitan area networks (MANs). A WAN connects two or more LANs that are in separate geographic locations. A MAN covers a large metropolitan area, such as a city.**

For example, you can have a Bluetooth-enabled phone and a Bluetooth-enabled headset like the one shown in Figure 9-3. These types of headsets have an earpiece and microphone and are worn on the ear.

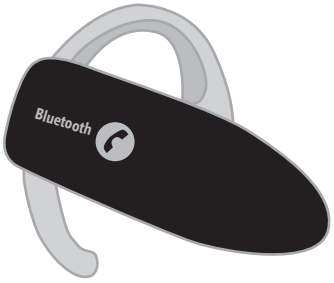

FIGURE 9-3 Bluetooth headset.

However, the headset won't work with the phone until you pair the two devices together. Pairing is the process of configuring the devices so that they can communicate with each other. After pairing the devices, you can keep the phone in your pocket or purse and use the headset to carry on conversations.

You need to follow the directions for the devices you're pairing, but the basic steps for pairing are:

- Enable Bluetooth if required
- Enable pairing if required

- Enter a personal identification number (PIN) if required
- Test connectivity

EXAM TIP

The same PIN needs to be entered on both devices, but sometimes one of the devices won't have a way to enter a PIN. For example, it's not possible to enter a PIN on most Bluetooth headsets. In this situation, you can enter the PIN only on the other device. What PIN should you use? Normally, you'd use either 0000 or the last four digits of the headset's serial number.

Depending on the version of Bluetooth that the devices are using, you might not need to take these steps. For example, Bluetooth version 2.1 uses Secure Simple Pairing (SSP), and one type of SSP is called Just Works. As the name implies, it just works without requiring the user to go through these steps. As a security precaution, the devices might require the user to approve the pairing process.

While Bluetooth is normally used for PANs, it can support distances farther away than someone's personal space. Table 9-2 shows the three classes of Bluetooth and their ranges.

TABLE 9-2 Bluetooth Classes and Ranges

Bluetooth Class	Approximate Range
Class 1	100 meters (about 328 feet)
Class 2	10 meters (about 33 feet)
Class 3	5 meters (about 16 feet)

Many wireless mouse and keyboard combos use Bluetooth. They include a USB transceiver (commonly called a *USB dongle*) that you plug into any USB port. Most are Class 2 devices so that you can use the mouse and keyboard from up to 33 feet away. Additionally, most use the Just Works version of SSP, so they don't require any user interaction.

Infrared

Infrared (IR) is a line-of-sight wireless technology used with many computing devices. The IR standards are developed by the *Infrared Data Association (IrDA)*. IR devices use light-emitting diodes (LEDs) to send IR signals that can be picked up by IR sensors.

You can use IR to connect and transfer information between two mobile devices or between a mobile device and a PC. For example, if someone has a ringtone you want, you can often transfer it between the devices with IR. Of course, both devices must have IR capabilities.

This is the same technology used with television remotes. You point the remote at the TV, select a button, and it does your bidding. However, it has a primary weakness that you probably know: if there is anything between the remote and the TV, the signal doesn't make it to the TV. A single piece of paper can block the signal. Similarly, if there is anything between the two devices, the IR signal is blocked.

NOTE **INFRARED NEEDS TO BE ENABLED**

Infrared is usually not enabled by default on devices. You need to go into the device settings to enable it.

There was a time when infrared was common on desktop PCs and laptops and used with some printers. However, the line-of-sight restriction has caused a lot of problems. All you have to do is put a book in the wrong location on your desk, and you lose the connection. Because of this, IR connections aren't very common except on some smartphones.

Quick Check

1. **What PIN is used when a PIN can't be entered with a Bluetooth device?**
2. **What is the range of Class 2 Bluetooth?**

Quick Check Answers

1. **0000, or the last four digits of the serial number.**
2. **10 meters, or about 33 feet.**

Email Configuration

One of the great benefits of mobile devices is the ability to access email while you're on the go. As long as you have connectivity to the Internet via either a wireless network or a cellular subscription service, you can usually access your email.

You'll learn more about protocols in Chapter 20, "Understanding Protocols," but as a short introduction, the following protocols are used for email:

- **Simple Mail Transport Protocol (SMTP).** This is the primary protocol used to send email.
- **Post Office Protocol version 3 (POP3).** This is the primary protocol used to receive email.
- **Internet Message Access Protocol (IMAP).** This protocol allows users to access and manage email stored on a mail server.

Configuring Settings

Internet Service Providers (ISPs) manage mail servers for their customers. Similarly, many organizations manage mail servers for their employees. To use these servers, you need to have an account on the server and know the full server name. After entering the correct information on the mobile device, you can use it to send and receive email.

As an example, Figure 9-4 shows the settings page to add a new email account on an iPad. The incoming mail server (using POP3) is named mail.GetCertifiedGetAhead.com, and the outgoing mail server using SMTP is named smtp.GetCertifiedGetAhead.com. This account (as with most accounts) requires a user name and password, so they are both added. After saving this information, I can send and receive email with this account on the iPad.

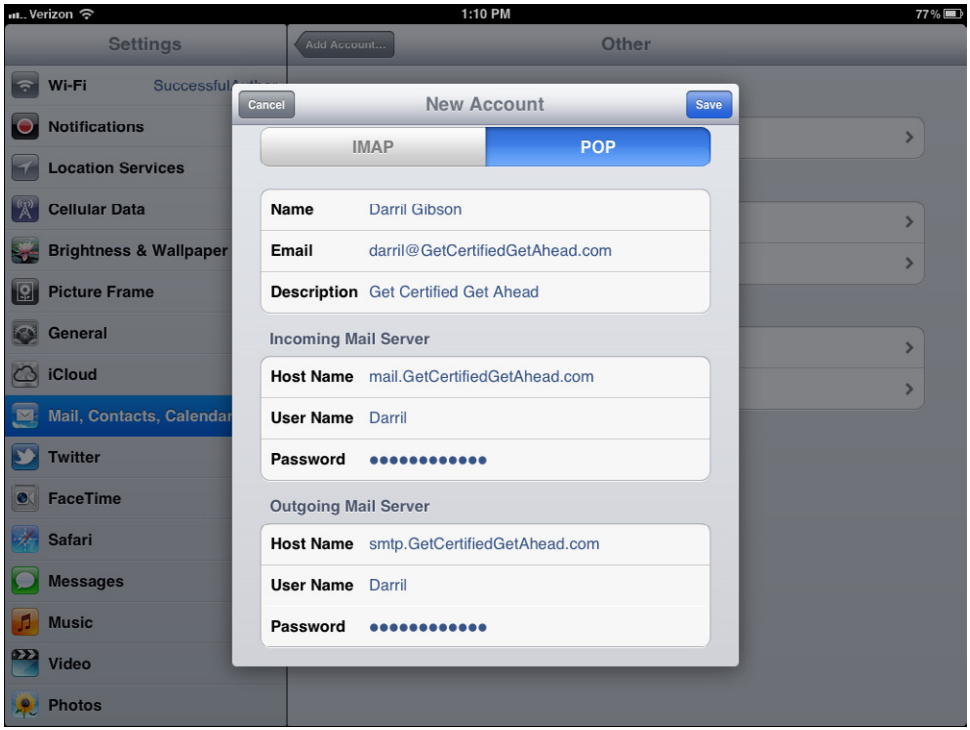

FIGURE 9-4 Configuring email on an iPad.

You need to enter the *fully-qualified domain name (FQDN)* of the mail server. The first part is known as the host or computer name, and everything following the first period is known as the domain name. For example, a computer named mail in the domain getcertifiedgetahead.com has an FQDN of mail.GetCertifiedGetAhead.com.

While the example in Figure 9-4 shows the settings, you probably don't have an account with GetCertifiedGetAhead.com. However, you might have a Microsoft Exchange email account with your company or a Gmail account through Google.

Microsoft Exchange is a server application that many organizations use for email. If your company is using Microsoft Exchange and it has been configured so that it is accessible via the Internet, you'll need the following information to connect:

- Email address of your account
- User name and password of the account
- Name of the Microsoft Exchange server

If you want to connect to a Gmail account, you can usually simply enter the email address and password to connect. Most email apps have the name of the Gmail server, but if you're prompted to add it, use smtp.gmail.com.

Email Port Settings

Occasionally, you're required to enter port data when configuring email settings. Chapter 20 provides more information about ports, but as an introduction, protocols are mapped to numbers called ports. These numbers indicate the type of data contained in traffic being sent over a network.

For example, when SMTP data is sent over the network, instead of including the words "Simple Mail Transport Protocol" within the data packet, it uses the port number of 25. Port numbers 0 through 1023 are known as well-known ports and are used for specific protocols. The well-known ports for the basic mail protocols are as follows:

- SMTP—port 25
- POP3—port 110
- IMAP—port 143

Many email servers require secure connections, and they use Secure Sockets Layer (SSL) or Transport Layer Security (TLS) to create secure connections. For example, SSL is used with Hypertext Transfer Protocol (HTTP) as HTTPS to create secure connections in web browsers. It's also used to create secure connections for many other protocols, including SMTP, POP3, and IMAP. If you're prompted to enter the SSL port number or the secure port number, use the following:

- SMTPS (SMTP over SSL)—port 465
- POP3S (POP3 over SSL)—port 995
- IMAPS (IMAP over SSL)—port 993

NOTE **PORTS**

Ports 993 and 995 are formally assigned to POPs and IMAPs, respectively. Port 465 is not formally assigned for SMTPS but is commonly used.

Quick Check

1. What is the primary protocol used to send email?
2. What is the well-known port number for a secure SMTP connection?

Quick Check Answers

1. SMTP.
2. Port 465 is used for SMTP over SSL, or SMTPS.

Using Mobile Devices

Mobile devices have touchscreens that allow you to control the actions by touch using specific gestures. If you've never used the devices, the gestures might take a moment to get used to. However, when you understand the basic motions, most mobile devices are remarkably easy to use. The common gestures are:

- **Tap.** You can select items with a single tap with any finger. You simply touch the screen by using a quick up-and-down motion with a finger. It is similar to clicking an item with a mouse.
- **Double-Tap.** Double-tapping is done with two quick taps and is similar to double-clicking an item with a mouse. It will often allow you to zoom in or zoom out on an item.
- **Flick.** You can flick the screen to scroll up or down or to pan from side to side. This is done by placing your finger on the screen and quickly swiping it in the desired direction. This is sometimes called *fling*.
- **Touch and Hold.** In this action, you touch a selection but don't remove your finger. Different items react differently to this action. For example, if you do this on the iPad's main screen, the items will shake and you can move them or press the X to delete them. This is sometimes called *press* or *long press*.
- **Drag.** Some items can be moved with a drag action. You select an item with your finger and then drag your finger across the screen to move the selected item. This is sometimes called *pan* or *scroll*.
- **Pinch.** This is commonly done by touching the screen with your finger and thumb at the same time and dragging them closer together, as if you were pinching the screen. It will often zoom in closer. For example, if you do this with a picture or a map, you can zoom in. You can also do this with two fingers instead of a finger and a thumb. Pinch is sometimes called *pinch close*.
- **Spread.** This is similar to the finger pinch but is done in the opposite direction. You touch the screen with your finger and thumb (or with two fingers) at the same place and spread them apart. It will often zoom out. Spread is sometimes called *pinch open*.

These capabilities are available on touch-based devices using two important technologies: multitouch and touch flow.

Multitouch refers to a device's ability to sense a user touching the surface at two or more places at a time. This is important when a user is doing pinch and spread gestures.

Touch flow refers to the ability of the screen to recognize users moving their finger across the screen. This is important when a user is doing flick gestures and when doing pinch and spread gestures.

EXAM TIP

Touch flow and multitouch are two primary capabilities supported by the touch interface on mobile phones and tablets.

Synchronizing Data

Synchronization is the process of storing the same data in two separate locations and ensuring it's the same in both places. For example, if you add music, pictures, or contacts to an iPad, you can synchronize it with a PC so that the same music, pictures, and contacts are on the PC.

Synchronizing also provides you with a backup. If you lose the data on the device (or lose the device), you still have a copy of the data. You can restore the data onto the original device or another device from the synchronized data.

Most mobile devices give you the ability to synchronize just about any type of data. This includes music, videos, pictures, contacts, programs, and email.

NOTE **AUTHORIZING A COMPUTER**

As a security precaution, you are often required to authorize a computer with a mobile device. This usually requires you to enter a user name and password associated only with you. This helps prevent someone from accessing your data through a synchronization program on their computer.

Installing Synchronization Applications

Mobile devices commonly have specific applications you use for synchronization. For example, you can use the iTunes application to synchronize most iOS-based devices. iTunes is available as a free download from the Apple website.

EXAM TIP

You need administrative rights to install an application on most systems. This is granted to users differently, but if the user does not have administrative rights, the installation will fail.

Connection Types for Synchronization

The connection type you use when synchronizing mobile devices is dependent on the device. However, the most common method is by using a USB cable from the device to a PC. After you connect the device, you can initiate the synchronization process with the application.

Many devices use USB cables such as the ones discussed in Chapter 5, "Exploring Peripherals and Expansion Cards." The cables have a Standard-A connector on one end to connect to a computer and a Mini-B, Micro-A, or Micro-B connector that connects to the device. Some devices have special one-of-a-kind connections. They require a cable with a unique connection on the device and a Standard-A USB connector on the other end.

Instead of connecting using a cable, you might be able to connect using one of the following methods:

- **Wireless or cellular to the Internet.** Using the cloud for synchronization is becoming more common. You'll need to first connect to the Internet via either a wireless network or a cellular connection. When connected, you can synchronize. You can also set up many devices to automatically synchronize at different times without any interaction.
- **Bluetooth.** You need to ensure that the devices are paired before the synchronization will work.
- **IR.** Some devices can use IR to connect to a PC and synchronize. Of course this requires the PC to have an IR interface and also requires a clear line of sight between the two.

Quick Check

1. **What technology allows a tablet to sense a user touching the screen in two places at the same time?**
2. **What types of connections are commonly used to synchronize mobile devices?**

Quick Check Answers

1. **Multitouch.**
2. **USB, wireless, cellular, Bluetooth, and IR.**

Securing Mobile Devices

If lost or stolen, mobile devices have tools that you can use to help protect them or the data stored on them. These tools are available on many smartphones and tablets.

> ***NOTE*** **DEFENSE IN DEPTH**
>
> **Thieves have many tools at their disposal to circumvent or override many security settings. None of the security methods described here are completely reliable, but by using a variety of tools, you can increase the security. Using multiple layers of security is referred to as *defense in depth*.**

Passcode Locks

A passcode is a simple password or set of digits that you must enter to start using the device. On some devices, it's called a *screen lock,* and it works like a password-protected screensaver. On other devices, it is a four-digit PIN. When the device is idle for a period of time, it locks. The user must then enter the passcode to use the device.

If you lose the device or it's stolen, another person won't be able to easily access the device because the person won't know the passcode. Of course, when a user writes the passcode on the device or attaches a sticky note with the passcode to the device, it defeats the purpose. You may laugh, but more than a few users have done this.

Failed Logon Attempts Restrictions

In addition to using a passcode lock, many devices include failed logon restrictions. For example, Figure 9-5 shows the screen for an iPad Passcode Lock. The Erase Data section can be turned on so that all data on the iPad is erased when the user enters the wrong passcode too many times. This prevents a thief from accessing data on a device by entering all the possible combinations.

FIGURE 9-5 Enabling the Passcode Lock and Erase Data as a failed logon restriction.

Remote Wipe

A remote wipe is a signal that, when sent to a lost device, removes all data on the system. If you lose the device or it's stolen, you can send the remote wipe signal to the device and it will wipe it clean. While it won't get the device back to you, it will ensure that any sensitive data on the device cannot be used by someone else.

EXAM TIP

The remote wipe capability must be enabled before the device is lost. If it is lost, you can then send the remote wipe signal to the device. Many mobile devices send a confirmation email when the remote wipe signal has been received and has erased the data on the device.

Locator Applications

Many applications are available to identify the location of a lost device. They use the GPS capability of the device and can pinpoint its location. These are useful if you've recently lost the device, and especially useful if it has been stolen.

Figure 9-6 shows an example of a locator application on an iPad. The application allows you to zoom in on the exact street address or zoom out. In the figure, I've zoomed it out to show a general location on the East Coast of the United States.

FIGURE 9-6 Locating an iPad.

This application also includes the following capabilities:

- **Play Sound.** This sends a signal to play a sound on the device. It's useful if you've lost it between the cushions of a couch or somewhere else within earshot. The sound continues to play until it's dismissed on the device.
- **Send Message.** It's possible that a Good Samaritan has found your device and would love to return it if only she knew who you were. You can send a message to the device with your contact information to let the person know that you lost it, you miss it, and you'd love to have it back.
- **Remote Lock.** Remote Lock works similarly to a passcode lock except that you can send the signal remotely. After it's set, users can't access the device unless they know the passcode.
- **Remote Wipe.** This sends the remote wipe signal to remove all data from the device.
- **Email When Found.** If you send any signal to the device, you can have an email sent to you when the signal has been received by the device. This provides verification that it has been completed.

Remote Backup Applications

Many devices support storing backup data in the cloud. For example, Android-based systems support Android backup, which allows you to back up all data to the cloud (the Internet). Windows 8 has a backup ability using Windows Azure–based technologies. Windows Azure is a group of cloud-based technologies used in several different Microsoft applications.

Apple's iOS-based systems allow users to back up their data and settings with iTunes, an application running on a PC. Recently, Apple launched iCloud Backup, which can automatically back up photos, accounts, documents, and settings. It senses when the unit is plugged in and receiving a charge, locked (indicating it isn't in use), or connected to a wireless network. Apple provides 5 GB of free storage, and you can purchase additional storage if you need it.

If the device is lost or destroyed, or you've sent a remote wipe signal to it, you can use the cloud-based backup to restore the data.

Antivirus Software

Sadly, malicious software (malware) is making its way onto mobile devices. Chapter 26, "Recognizing Malware and Other Threats," covers malware in much more depth, but as an introduction, malware includes viruses, worms, Trojans, rootkits, spyware, and more.

In January 2011 there were a reported 80 infected Android apps. This grew to more than 400 infected apps by June 2011. Compared with the millions of viruses that can infect PC-based systems, this number is small. However, they have started and they're on the rise.

The Apple iOS has had relatively few problems with malware. One of the things that Apple does is vigorously screen apps before they are offered for sale in the Apple App Store. It is difficult for an attacker to create an infected app and get it into the store.

Google Play requires developers to create an account before they can upload apps. The app is made available almost immediately, and Google doesn't follow the same vigorous screening process used for apps in the Apple App Store. However, if an infected app is discovered, it is quickly removed from the store, and Google has information about the developer who uploaded it. If users download apps from other sources, there is a higher level of risk.

EXAM TIP

One of the safest steps you can take to protect mobile devices against malware infection is to purchase apps only from the official stores. This includes Apple's App Store, Google Play, and Microsoft's Marketplace. Other sources aren't policed as vigorously, making it easier for attackers to upload malware.

At this writing, very few antivirus programs are available for mobile devices. However, as the malware for these devices increases, you can expect antivirus programs to become available.

Patching/Operating System Updates

Bugs and security issues are detected with any operating system after it is released. As issues are detected, the vendor updates and releases patches and operating system updates. As a best practice, you should always ensure that your system is up to date. This includes the operating systems on mobile devices and the operating systems on any desktop PC.

The method of patching the system varies by device. Windows-based systems can be configured to automatically download and install patches and updates without any user intervention. Apple iOS-based systems require you to connect your device to a PC with a USB cable and use iTunes to update it. Android-based systems often prompt you when an update is available.

EXAM TIP

Before applying a patch or doing an update, it's always a good idea to synchronize the device. This will save all your applications, data, and settings, and if something goes wrong during the update, you can fully restore the device.

Quick Check

1. **What can be enabled to prevent a thief from easily using a stolen mobile device?**
2. **What is used to remotely erase data on a lost device?**

Quick Check Answers

1. **Passcode lock.**
2. **Remote wipe.**

Chapter Summary

- Tablets are not upgradable or serviceable by technicians in the field. In contrast, technicians can upgrade and service laptops.
- The orientation of a tablet's screen is automatically sensed by an accelerometer and/or gyroscope. Applications use this data to change the display for the user, such as switching between landscape mode and portrait mode.
- GPS identifies the exact location of the device. It can be used to locate a lost device and is also used by geotracking. Geotracking records the location of a device and stores the data in a log on the device.
- Apple devices use iOS, a closed source operating system that is not licensed to any other company. Applications can be purchased only via Apple's App Store.

- Android is an open source operating system developed by a consortium of companies led by Google. It is used on mobile devices created by many different companies. Users primarily buy applications from the Google Play website, but applications can be purchased through other sources.
- Mobile devices commonly connect to the Internet through wireless or cellular connections. Disabling these connections reduces battery consumption. Other connections are Bluetooth and infrared.
- Bluetooth devices need to be paired before they can be used. In some cases, a PIN is needed. If you are unable to enter a PIN on a device (such as on a headset), the common PIN code is either 0000 or the last four digits of the device's serial number.
- Class 2 Bluetooth connections have a range of 10 meters (about 33 feet). Class 1 and Class 3 Bluetooth connections have a range of 100 meters (about 328 feet) and 5 meters (about 16 feet), respectively. IR connections are limited by line of sight.
- When configuring email, you'll need to know the full name of the SMTP, POP3, and/or IMAP servers, depending on what the email server is using. You might also need to know the basic and secure ports used for the connections.
- The basic and secure port numbers are SMTP port 25, SMTPS port 465, POP3 port 110, POP3S port 995, IMAP port 143, and IMAPS port 993.
- Tablets have a touch interface using touch flow and multitouch capabilities to sense different gestures.
- Synchronization allows you to keep a backup of all the data and settings for a device. Many devices allow you to synchronize with a PC through a USB cable, and some devices allow you to synchronize through a cloud-based service on the Internet.
- Security for mobile devices is enhanced through several features, including passcode locks, remote wipe, and GPS locator applications.
- When updates and patches are available, they often include security enhancements and should be installed as soon as possible. Data and settings should be backed up before doing an update.

Chapter Review

Use the following questions to test your knowledge of the information in this chapter. The answers to these questions, and the explanations of why each answer choice is correct or incorrect, are located in the "Answers" section at the end of this chapter.

1. Of the following choices, what would cause a device to change from portrait mode to landscape mode when the device is moved?

   A. Touch flow

   B. Accelerometer

C. Gyro

D. Geotracking

2. Of the following choices, what represents a benefit to users of purchasing apps only through Apple's App Store?

A. Cheaper than purchasing at a store

B. Automatically includes source code

C. Upgrades are automatic

D. Less chance of downloading malicious software

3. What is required before using two Bluetooth devices together?

A. Subscribe to a cellular plan

B. Connect to a Wi-Fi network

C. Enable POP3

D. Pair them

4. You are helping a user configure email on a tablet. It is prompting you for the port used for secure POP3. What is the most likely port number you should enter?

A. 25

B. 110

C. 993

D. 995

5. A business owner wants to ensure that her tablet is as secure as possible. Of the following choices, what should she enable? (Choose all that apply.)

A. Remote wipe

B. GPS location services

C. Passcode lock

D. Bluetooth pairing

6. What should you do before updating the operating system of a mobile device?

A. Flash the BIOS

B. Back up the device

C. Enable remote wipe

D. Disable Wi-Fi and cellular connections

Answers

This section contains the answers to the questions for the Lesson Review in this chapter.

1. **Correct Answer:** B
   - **A. Incorrect:** Touch flow is used to sense when a user moves a finger across a touch screen.
   - **B. Correct:** Devices commonly include accelerometers (and electronic gyroscopes) to sense the orientation of the device and change the display.
   - **C. Incorrect:** A gyro is type of sandwich sold in many Greek restaurants, wrapped in a flatbread or pita.
   - **D. Incorrect:** Geotracking uses recorded GPS information to track the past locations of a device.
2. **Correct Answer:** D
   - **A. Incorrect:** You can't purchase Apple Apps at a store, so there is no cost benefit.
   - **B. Incorrect:** Purchased software is typically closed source, so it does not include the source code.
   - **C. Incorrect:** While software can often be upgraded, upgrades are not automatic with Apple App Store apps.
   - **D. Correct:** Apple screens all software in their App Store, so software purchased through their site is less likely to be infected with a virus or other malicious software.
3. **Correct Answer:** D
   - **A. Incorrect:** Cellular plans are used with smartphones and some mobile devices, but they are unrelated to Bluetooth.
   - **B. Incorrect:** Connecting to a wireless network is not required to pair two Bluetooth devices.
   - **C. Incorrect:** Post Office Protocol v3 (POP3) is configured for email but not for Bluetooth.
   - **D. Correct:** Bluetooth devices must be paired before they can be used together. This can be automatic or can require entering a PIN on one or both devices.

4. **Correct Answer:** D

   A. **Incorrect:** Port 25 is the well-known port for Simple Mail Transport Protocol (SMTP).

   B. **Incorrect:** Port 110 is the well-known port for Post Office Protocol3 (POP3).

   C. **Incorrect:** Port 993 is the well-known port for IMAP over Secure Sockets Layer (IMAPS).

   D. **Correct:** Port 995 is the well-known port for POP3 over Secure Sockets Layer (POP3S).

5. **Correct Answers:** A, B, C

   A. **Correct:** Remote wipe allows her to send a remote signal to a lost device to delete all information on the device.

   B. **Correct:** Global Positioning System (GPS) location services allow a lost device to be located.

   C. **Correct:** Passcode locks require a user to enter a passcode before using a device.

   D. **Incorrect:** Bluetooth pairing is done to match two Bluetooth devices. However, you don't enable Bluetooth pairing. Instead, you pair devices after enabling Bluetooth.

6. **Correct Answer:** B

   A. **Incorrect:** Flashing the BIOS is commonly done for a motherboard BIOS to update it. It can be done on a mobile device, but it is not necessary before an update.

   B. **Correct:** It's possible to lose data, applications, and settings during an update, so all data should be backed up before an update whenever possible.

   C. **Incorrect:** Remote wipe is a security feature that allows you to remove data on a lost device.

   D. **Incorrect:** It is not necessary to disable connectivity during an update, and sometimes the connectivity is required.