# 9-1 Mobile Devices, Operating Systems, Connections, and Accessories

## Core 1 Objectives

- 1.1

  Given a scenario, install and configure laptop hardware components.

- 1.3

  Given a scenario, set up and configure accessories and ports of mobile devices.

- 1.4

  Given a scenario, configure basic mobile-device network connectivity and application support.

- 2.3

  Compare and contrast protocols for wireless networking.

Mobile devices vary considerably by size, functionality, available connection types, and primary purpose(s), not to mention cost. A **smartphone** is primarily a cell phone that also can send text messages with photos, videos, or other multimedia content attached; surf the web; manage email; play games; take photos and videos; and download and use small apps. Most smartphones use touch screens for input (see Figure 9-1) and allow for voice input.

### Figure 9-1

Most smartphones don’t have a physical keyboard and use a touch screen with an on-screen keyboard for input


iStock.com/Hocus-focus

A **tablet** is a computing device with a touch screen that is larger than a smartphone and has functions similar to a smartphone. As you can see in Figure 9-2, a tablet might come with a detachable keyboard or a stylus. All tablets can connect to Wi-Fi networks and use Bluetooth or NFC (near-field communication), which you learn about later in this module, to wirelessly connect to nearby devices. Some tablets have the ability to use a cellular network for data transmissions and phone calls. Installed apps can be used to make voice phone calls, send text messages, and make video calls using data transmissions. When a tablet can be used to make a phone call, the distinction between a smartphone and a tablet is almost nonexistent, except for size.

## Figure 9-2

Tablets are larger than smartphones and smaller than laptops, and can use touch or touch pen input


iStock.com/Orientfootage

# 9-1a Mobile Device Operating Systems

**Core 1 Objective**

- 1.3

Given a scenario, set up and configure accessories and ports of mobile devices.

The operating system for a mobile device is installed at the factory. **Android** OS by Google (google.com and android.com) is based on Linux and holds about 72% of the global mobile OS market. **iOS** for iPhones and **iPadOS** for iPads by Apple (apple.com) are based on macOS, and together hold about 27% of the global mobile OS market. Combined, Android, iOS, and iPadOS command about 99% of market share. Let's get familiar with each OS.

# 9-1b Get to Know an Android Device

**Core 1 Objective**

- 1.3

Given a scenario, set up and configure accessories and ports of mobile devices.

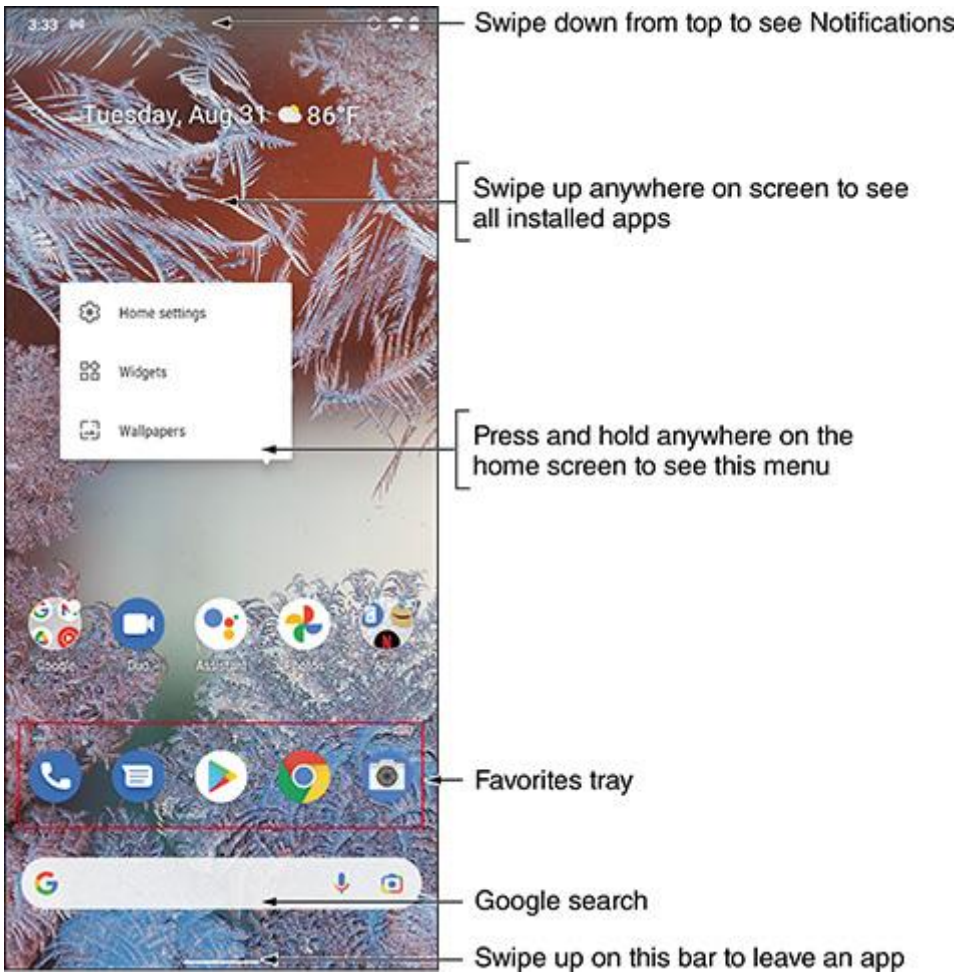
In the past, releases of Android were named after desserts. The last dessert release was Android Pie (version 9.0) in 2018. Now releases are merely numbered for the public. The current release is Android 11.0, and Android 12.0 has been released to a few devices. When a new release publishes,

device manufacturers gradually release it. Not all Android devices can support a new release; it's up to the manufacturer to decide if a particular model can handle a new release and when that model gets the release.

Most current Android mobile devices have power and volume control buttons on the right side, and some have a third Google Assistant button to enable voice input on the left side. Earlier versions of Android used three soft buttons at the bottom of the screen, but Android 11 uses swipes or gestures rather than buttons to navigate the OS. Some of these gestures are described in Figure 9-3.

## Figure 9-3

Android 11 home screen and user interface

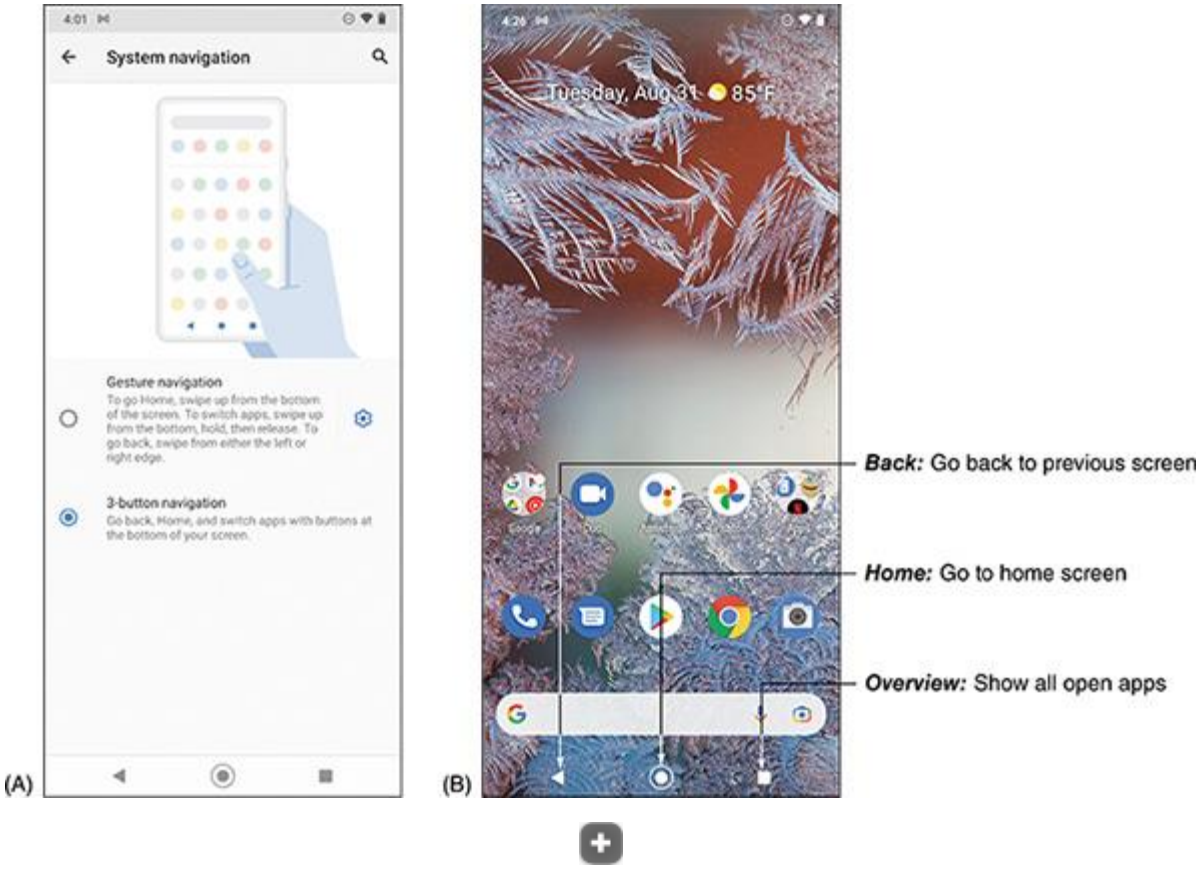



## Note 1

You can use the Settings menu to configure Android to use the three legacy soft buttons at the bottom of the screen. In the Settings menu, tap **System**, **Gestures**, and **System navigation** and select **3-button navigation** (see Figure 9-4A). Figure 9-4B shows the home screen with the three buttons enabled.

## Figure 9-4

(A) Choose gesture navigation or 3-button navigation, and (B) Android 11 home screen with 3-button navigation




## Note 2

Android is installed by various device manufacturers before the device leaves the factory, and these manufacturers can customize the OS and how it works. Therefore, specific step-by-step directions will vary from device to device, even when the devices all use the same Android release. Remember that you don't need to memorize the steps—just learn general procedures for supporting a variety of mobile devices.

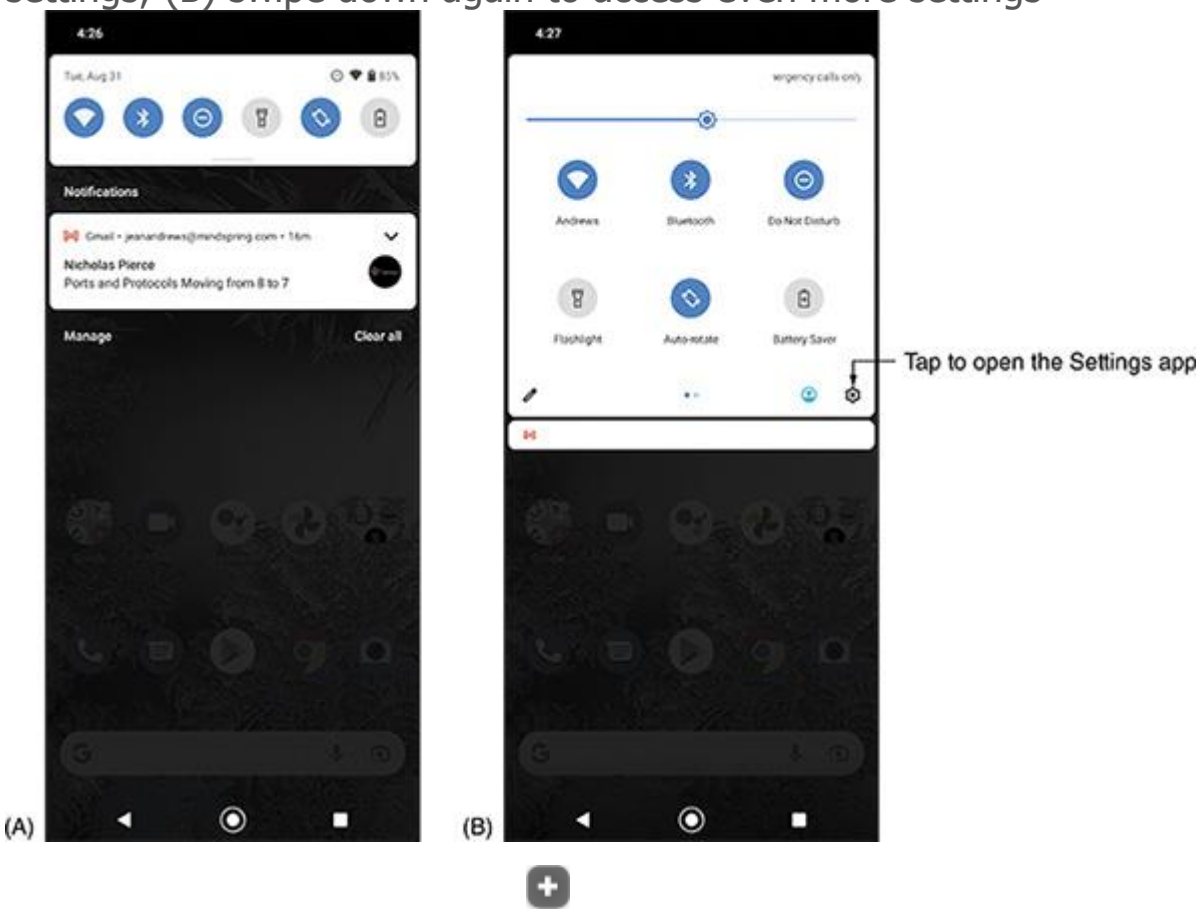
On Android phones, up to five apps or groups of apps can be pinned to the **favorites tray** just above the Google search box. Apps in the favorites tray stay put as you move from screen to screen by swiping left or right. Some other useful tools include the following:

- **App drawer.** Swipe up anywhere on the screen to access the **app drawer**, which lists and manages all apps installed on the phone. Press and hold an app in the app drawer to add it to an existing home screen or to add more home screens.
- **Notifications.** Swipe down the notifications shade from the top of the screen to see **notifications** that provide alerts and related information about apps and social media and quick settings to Wi-Fi, Bluetooth, and auto-rotate. See Figure 9-5A. Swipe down again to see more

settings, including the cog icon to access the Settings app. See Figure 9-5B.

## Figure 9-5

(A) The notifications shade includes quick access to a few settings; (B) swipe down again to access even more settings




Source: Android

- **Settings app.** To open Settings, tap the cog icon in the second notifications area, or open the app drawer and tap **Settings**. Most of the settings you need to use to support a mobile device are contained in the Settings app (see Figure 9-6). You can open the Settings app and search through its menus and submenus until you find what you need. If you get stuck, do a quick web search or check the user guide for the device.

## Figure 9-6

The Android Settings app


Source: Android, Source: Apple Inc.

**Note 3**

One step in troubleshooting an OS is to update it. To update Android, in Settings, tap **About phone, Android version**, and **Google Play system update**. Know that a device might not be able to update to the latest version of Android.

## Manage Android Apps

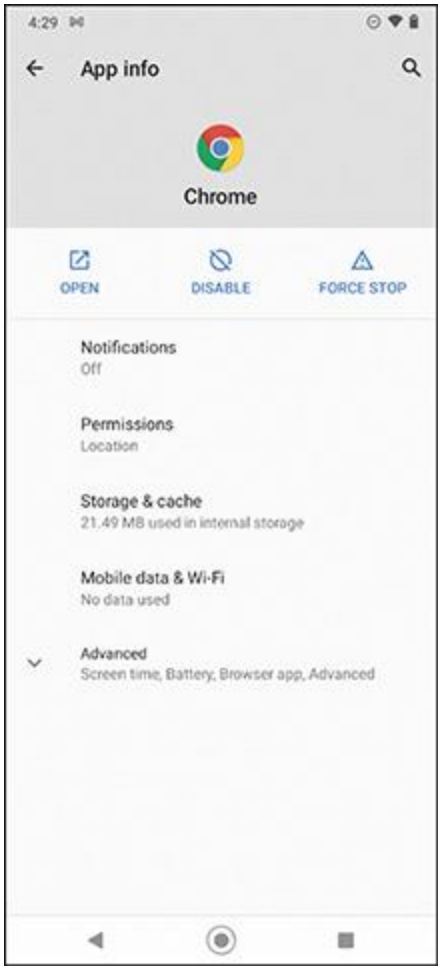
Android apps are sold or freely distributed by any source or vendor. For example, you can open the Chrome browser and download an app from a website, such as the Amazon Appstore for Android at amazon.com or directly from the website of a developer. However, the official source for apps is **Google Play** at play.google.com. A **Google account** is required to download content from Google Play and can be associated with any valid email address. Here's how to handle apps:

- **Install an app.** To get an app from Play Store, tap the **Play Store** app on the home screen. (If you don't see the app icon on the home screen, tap the **app drawer** and then tap **Play Store**.) Search for an app, and follow directions to install one.
- **Open and close an app.** To open an app, tap it on a home screen, or open the app drawer and tap the app. To leave the app, swipe up from

the bottom of the screen or, when using 3-button navigation, tap the **Home** button. To close the app, swipe up slowly from the bottom of the screen (or tap the **Overview** button). All open apps appear in small windows. To close an app, swipe it up. If an app refuses to close, you can force it: open the **Settings** app, tap **Apps & notifications**, tap the running app, and then tap **FORCE STOP** (see Figure 9-7).

**Figure 9-7**

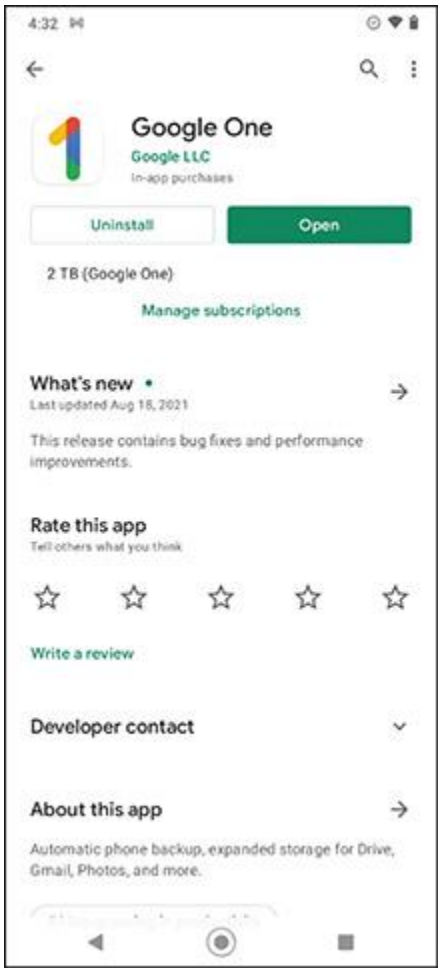
Force stop an app




- **Delete or uninstall an app.** To uninstall an app, press the app icon, tap **App info**, and tap **UNINSTALL**. Another way to delete or uninstall an app is to open the **Play Store** app, tap your Google account profile icon (your photo), tap **Manage apps & devices**, tap **Manage**, tap the app, and then tap **Uninstall** (see Figure 9-8). Sometimes an Update option is also available on this screen. Also note that some embedded apps, such as the Phone app, can't be uninstalled.

**Figure 9-8**

Use the Play Store app to uninstall an app




# 9-1c Get to Know iOS and iPadOS by Apple

## Core 1 Objective

- 1.3

Given a scenario, set up and configure accessories and ports of mobile devices.

Apple Inc. (apple.com) develops, manufactures, and sells the Apple **iPhone** (a smartphone) and **iPad** (a handheld tablet). The latest releases for both OSs are versions 15. Apple maintains strict standards on its products, which means iOS and iPadOS are exceptionally stable and bug free; they are also very easy and intuitive operating systems to use.

iPhones have volume control buttons on the left side of the device and a physical side button on the upper-right side of the device. iPads have a top button on the top right side and volume buttons on the right side. Older devices also have a home button on the front of the device. The user interface is shown in Figure 9-9 for an iPad; an iPhone interface looks and works the same. Apps can be pinned to the **dock** at the bottom of the screen.

## Figure 9-9

Access the dock on an iPad by swiping up from the bottom of the screen

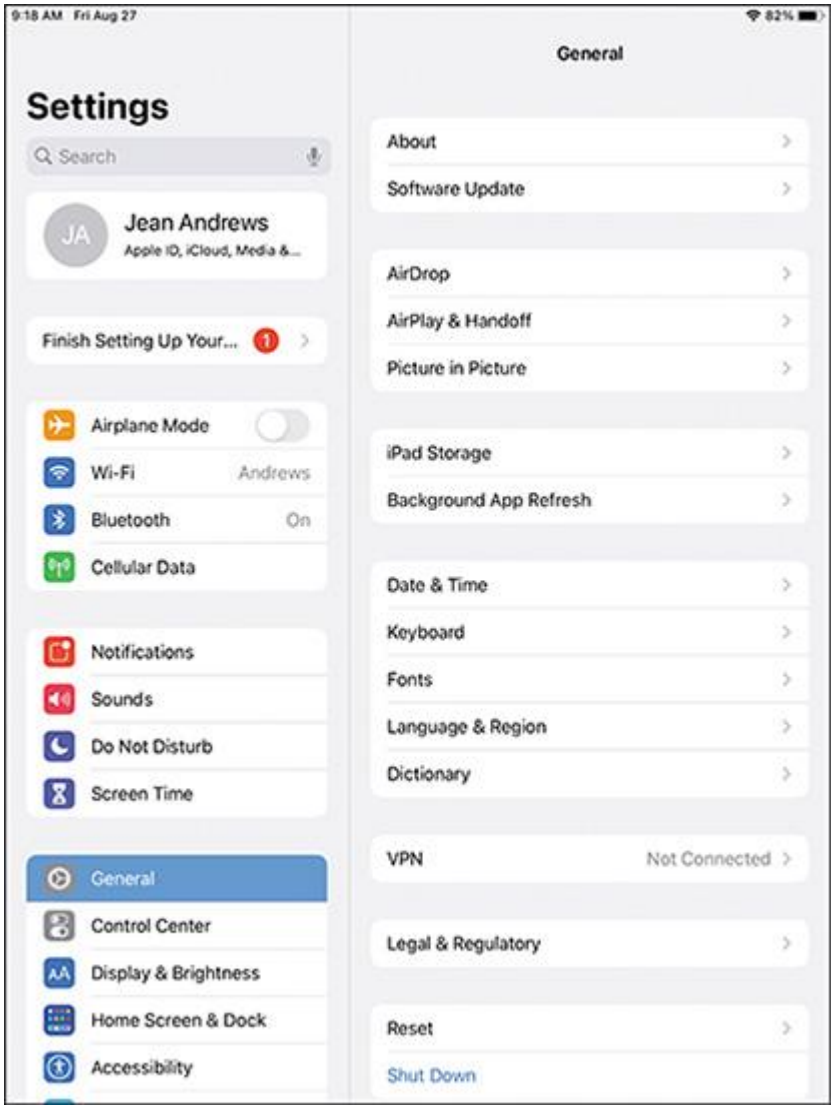

Source: Apple Inc.

Other useful tools include the following:

- **Control Center.** Swipe down from the upper-right corner to view the Control Center, where you can change basic settings such as brightness, volume, Wi-Fi, and Bluetooth. Use the Settings app to adjust which settings are available in the control center.
- **Settings app.** To open the Settings app, tap the **Settings** icon on the home screen. Just as with Android, the Settings app is the go-to place to manage the device, apps, and the OS. See Figure 9-10. For example, to manage iOS updates, in the Settings app, tap **General** and **Software Update**. You can set the device to automatically download and install updates or to download updates but not install them until you allow it.

## Figure 9-10

Manage most iOS settings in the Settings app




## Manage iOS and iPadOS Apps

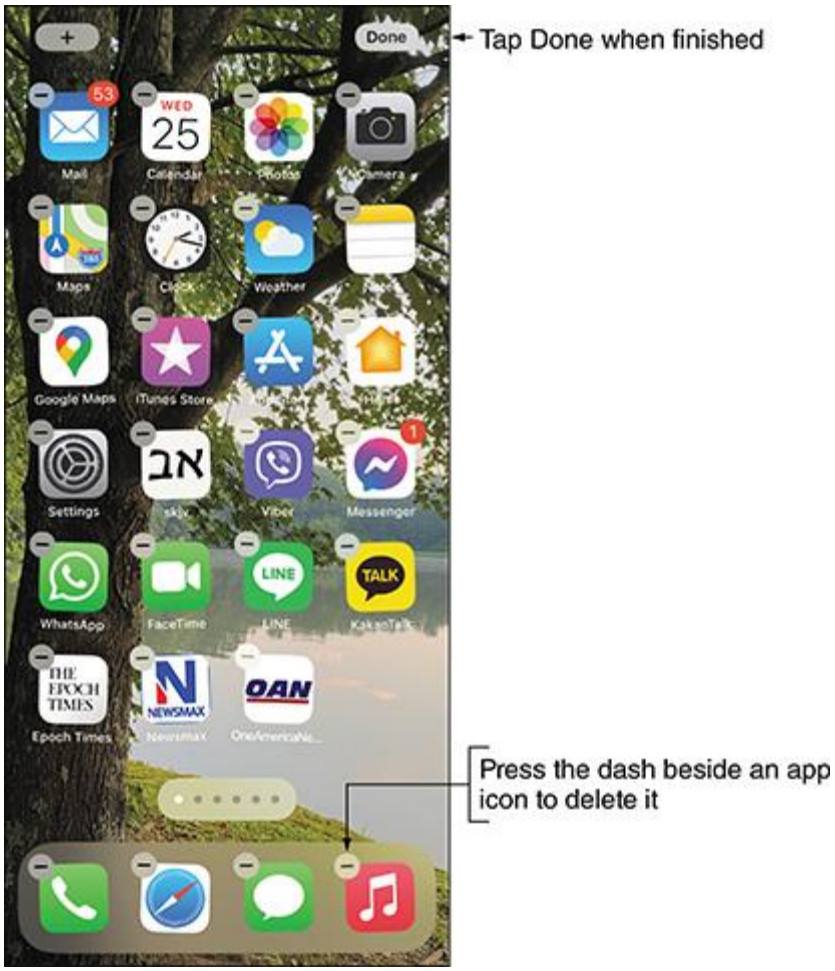
You can get Android apps from many sources, but the only place to go for an iOS/iPadOS app is Apple, which is the sole distributor of iOS apps at its App Store. (Also, entertainment, including movies and music, is available at the Apple iTunes Store.) Other developers can write apps for the iPhone or iPad, but these apps must be sent to Apple for close scrutiny. If they pass muster, they are distributed by Apple on its website. Apple offers app development tools, including the iOS SDK (software development kit), at developer.apple.com.

When you first purchase an iPad or iPhone, you activate it by signing in to the device with an **Apple ID**, or user account; using a valid email address and password; and associating the account with a credit card number. You need an Apple ID to download an app from the App Store. Here's how to manage apps:

- **Open and close apps.** Tap an app icon to open it. To leave the app, swipe up from the bottom of the screen. (For older devices with a Home button, press the Home button.) To close an app, swipe up slowly from the bottom of the screen. All open apps appear in small windows. Swipe up to close each app. (For older devices with a Home button, double-press the Home button to view all open apps. Swipe up to close each app.)
- **Install and uninstall apps.** Open the App Store app to search for and install an app. To delete or uninstall an app, press and hold the app icon, and tap **Remove App** or **Delete App**. Alternately, hold down the app until all icons start to jiggle. As the icons jiggle, press the dash beside an app icon to delete it. See Figure 9-11. To stop the jiggling, tap **Done** in the top-right corner of the screen.

## Figure 9-11

To delete multiple apps, as app icons jiggle, tap the dash beside the icon




Source: Apple Inc.

## Note 4

Most of us rarely follow step-by-step directions when learning to use a new device—until when "all else fails, read the directions." When you are called on to support a mobile device

that you don't own or normally use, it's helpful to begin by looking for how to open the Settings app and browse through settings. The information presented in this part of the module can give you an idea of what to look for, and you can likely figure out the specific steps for yourself.

## 9-1d Wireless Connections for Mobile Devices

**Core 1 Objectives**

- 1.3

  Given a scenario, set up and configure accessories and ports of mobile devices.

- 1.4

  Given a scenario, configure basic mobile-device network connectivity and application support.

A mobile device might have several antennas—primarily cellular, Wi-Fi, GPS, Bluetooth, and NFC. The device uses a Wi-Fi or cellular antenna to connect to a LAN (local area network) or WAN (wide area network) and uses Bluetooth or NFC to connect to a PAN (personal area network). Settings on the device allow you to enable or disable each antenna. Network connections are configured using the Settings app. Let's look at each type of LAN, WAN, and PAN connection.

Exam Tip

The A+ Core 1 exam might give you a scenario that expects you to decide how to configure a Wi-Fi, cellular data, or Bluetooth connection on a mobile device.

Two examples of LAN connections on a mobile device are when Wi-Fi is used to connect to a local network and when a device creates its own mobile Wi-Fi hotspot.

## 9-1e Wi-Fi Connections to a LAN

**Core 1 Objectives**

- 1.3

  Given a scenario, set up and configure accessories and ports of mobile devices.

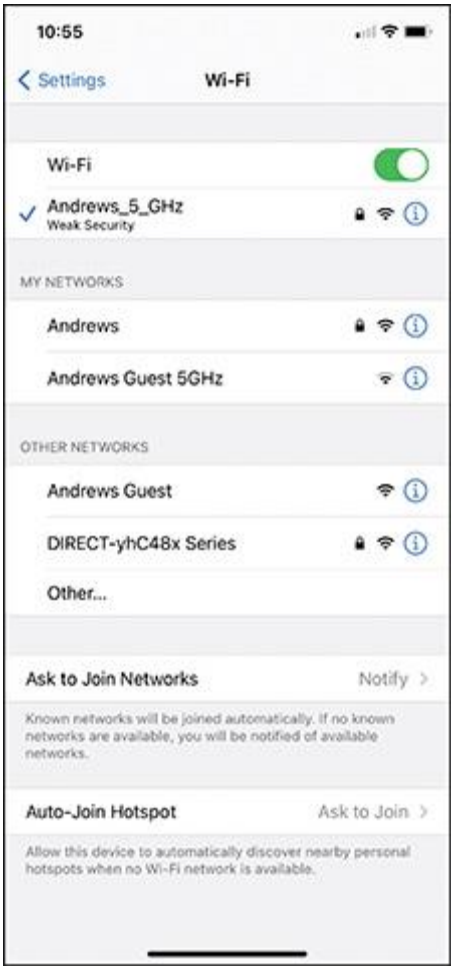
- 1.4

  Given a scenario, configure basic mobile-device network connectivity and application support.

Most mobile devices have Wi-Fi capability. On the Wi-Fi settings screen, you can add a Wi-Fi connection, manage existing networks, view available Wi-Fi hotspots, see which Wi-Fi network you are connected to, turn Wi-Fi off and on, and decide whether the device should ask the user before joining a Wi-Fi network. When the device is within range of Wi-Fi networks, it displays the list of networks. Select one to connect. If the Wi-Fi network is secured, enter the security key to complete the connection. To change to a different Wi-Fi hotspot, tap the name of the network, and select a new one from the list of available networks (see Figure 9-12). Searching for a Wi-Fi network can drain battery power. To make a battery charge last longer, disable Wi-Fi when you're not using it.

**Figure 9-12**

Select a new Wi-Fi hotspot, or see details about the current connection




Source: Apple Inc.

## 9-1f Mobile Hotspots and Tethering

**Core 1 Objective**

- 1.3

Given a scenario, set up and configure accessories and ports of mobile devices.

When a mobile device is connected to the Internet by way of its cellular WAN connection, you can allow other computers and devices to use this same connection. For example, in Figure 9-13, the smartphone is tethered by USB to a laptop so that the laptop can use the cellular network to connect to the Internet. If the smartphone has Wi-Fi capabilities, it can create its own Wi-Fi hotspot for other computers and devices to connect to wirelessly. An app on the smartphone controls these connections. To use your phone for tethering and for providing mobile hotspots, your carrier subscription must allow it. Also, know the extra burden on the phone can cause the battery to drain quicker and perhaps even overheat.

## Figure 9-13

Tether your smartphone to your laptop using a USB cable

# 9-1g Cellular WAN Connections

## Core 1 Objectives

- 1.3

Given a scenario, set up and configure accessories and ports of mobile devices.

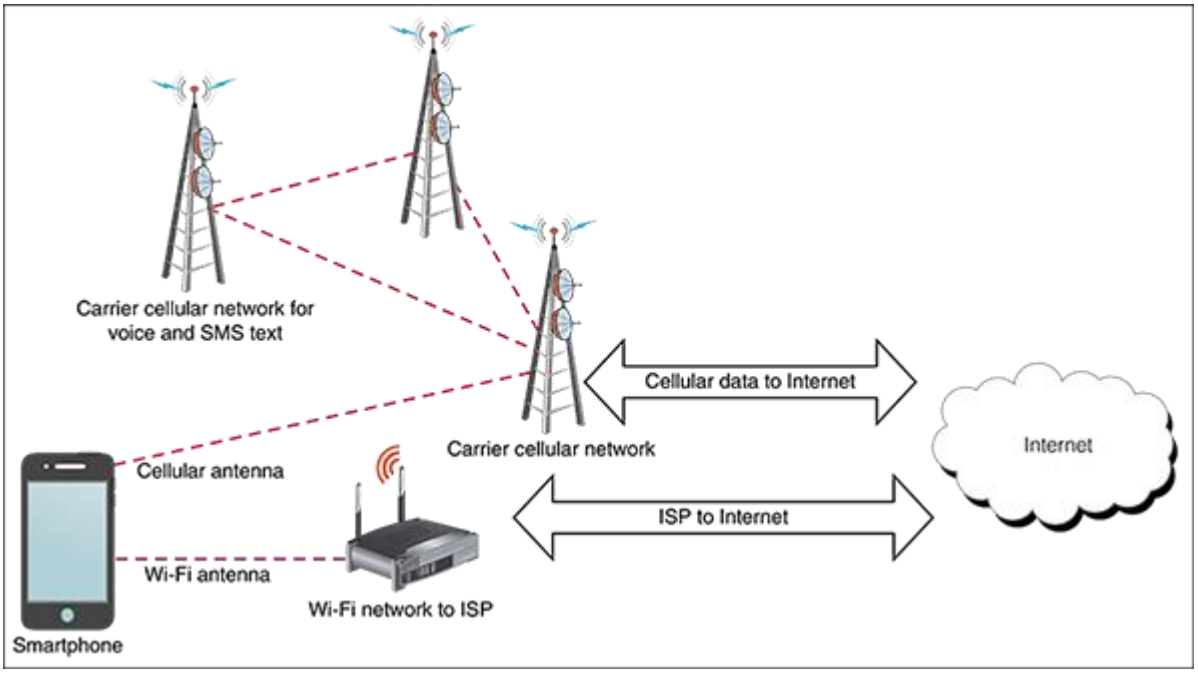
- 1.4

Given a scenario, configure basic mobile-device network connectivity and application support.

Smartphones—and some laptops, tablets, and wearable mobile devices—can connect to a cellular WAN if they have cellular capability and a subscription to the cellular network carrier. Recall from the module "Network Infrastructure and Cloud Computing" that a cellular network provided by a wireless carrier (for example, AT&T or Verizon) is used for voice, text, and data communication. As shown in Figure 9-14, cellular voice and SMS (Short Message Service) text messages transmit over the carrier's cellular network, and **cellular data** is sent from the carrier's cellular network to the Internet for distribution.

## Figure 9-14

A smartphone can communicate on the Internet via a cellular network or Wi-Fi




The following are two older radio bands a carrier might use on its cellular network for voice and SMS text communication:

- **CDMA. CDMA (Code Division Multiple Access)** communication is more popular in the USA than other nations and does not require a SIM card.
- **GSM. GSM (Global System for Mobiles)** communication is a global standard used in many nations and requires a SIM card installed in the device.

Older cell phones were built to support GSM or CDMA, but not both. Newer cell phones can support either technology. Both GSM and CDMA are being replaced by newer technologies, although they are still used as backups for voice calls in locations where more modern coverage is weak. Most carriers have announced they will stop supporting GSM and CDMA by the end of 2022.

Whereas GSM and CDMA are used only for voice and SMS texting, these standards can transmit cellular data (voice, text, video and graphics) to the Internet:

- **2G.** The **2G** standard was first used with GSM to transmit secured voice, text messages, and limited data. It was soon followed by a CDMA version of 2G that was slightly faster.
- **3G.** The **3G** standard was faster than 2G and used with CDMA and GSM. 3G can achieve download speeds up to 21 Mbps.
- **4G and 4G LTE.** The **4G** standard was faster than 3G but was soon replaced by an even faster standard: **4G LTE**. 4G and 4G LTE don't require the help of CDMA or GSM, which is why those older standards are being phased out. 4G LTE can achieve up to 1 Gbps speeds and requires a SIM card to function. 4G was the first standard that allowed a device to support a mobile hotspot.

- **5G.** The **5G** standard is the up-and-coming standard, and it currently has an average speed of 150 Mbps, with peak speeds up to 10 Gbps.

As noted, although CDMA does not require a SIM card, 4G LTE does—which is why all cell phones in the United States now use SIM cards. To make a cellular data connection, you must have a subscription with your carrier that includes a SIM card and cellular data plan. Here is information that might be used when a connection is first made to the carrier's WAN or when troubleshooting that connection:

- The **IMEI (International Mobile Equipment Identity)** is a unique number that identifies each mobile phone or tablet device worldwide. It's usually reported within the About menu in the OS (see Figure 9-15), and it might also be printed on a sticker on the device, such as behind the battery.

## Figure 9-15

The IMEI value identifies a mobile device worldwide


## Note 5

If your phone gets stolen and you notify your carrier, the carrier can block its use based on the IMEI and alert other carriers to the stolen IMEI. Also, before buying a used phone, check its IMEI against blacklists of stolen phones by doing a Google search on **imei blacklist check**.

- The **IMSI (International Mobile Subscriber Identity)** is a unique number that identifies a cellular subscription for a device or subscriber, along with its home country and mobile network. This number is stored on the SIM card. For

older phones that don't use SIM cards, the number is kept in a database maintained by the carrier and is associated with the IMEI.

## Note 6

SIM cards come in various sizes and install in a pop-out tray on the side of a phone. Alternately, an eSIM card is embedded on the motherboard and never removed. For SIM cards, when you switch carriers for your device you exchange cards. For eSIM cards, to switch carriers, you scan a QR code sent to you by the new carrier or use an app to make the switch.

### Exam Tip

The A+ Core 1 exam expects you to identify and distinguish between GSM and CDMA technologies, and might give you a scenario that requires you to know which communication technology a device is using.

## Applying Concepts

### Manage Cellular Data and Roaming

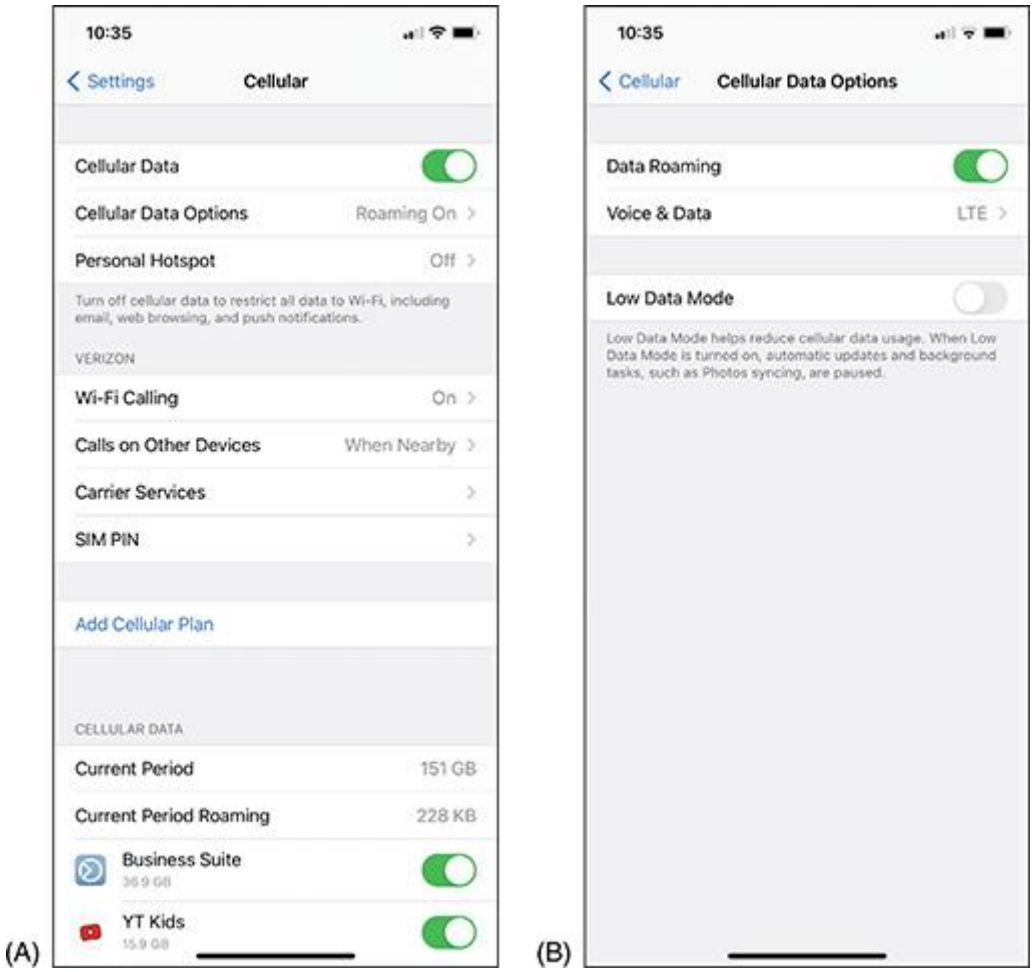
- **Est. Time:** 15 minutes
- **Core 1 Objective:** 1.4

Looking back at Figure 9-14, you can see that a smartphone can use cellular data or Wi-Fi to access the Internet. In certain situations, you might want to disable cellular data or disable cellular roaming. The advantage of disabling cellular data and using Wi-Fi for data transmissions is that Wi-Fi transmissions are not charged against your cellular data subscription plan. Also, Wi-Fi is generally faster than most cellular connections. (When you disable cellular data, you can still send SMS texts because these texts use the carrier's network and not the Internet.) Disabling roaming can prevent roaming charges on your bill incurred from using other carriers' cellular networks when you travel outside your home territory.

To disable roaming on an Android device, go to the **Network & internet** menu in the Settings app, tap **Mobile network**, and then disable **Roaming**. On an iOS device, open the Settings app, tap **Cellular** (see Figure 9-16A), and turn off **Cellular Data**. Next, tap **Cellular Data Options**, and then turn off roaming. On the Cellular Data Options screen, you can also turn on Low Data Mode to conserve cellular data usage. See Figure 9-16B.

## Figure 9-16

Control (A) data usages and (B) data roaming in iOS



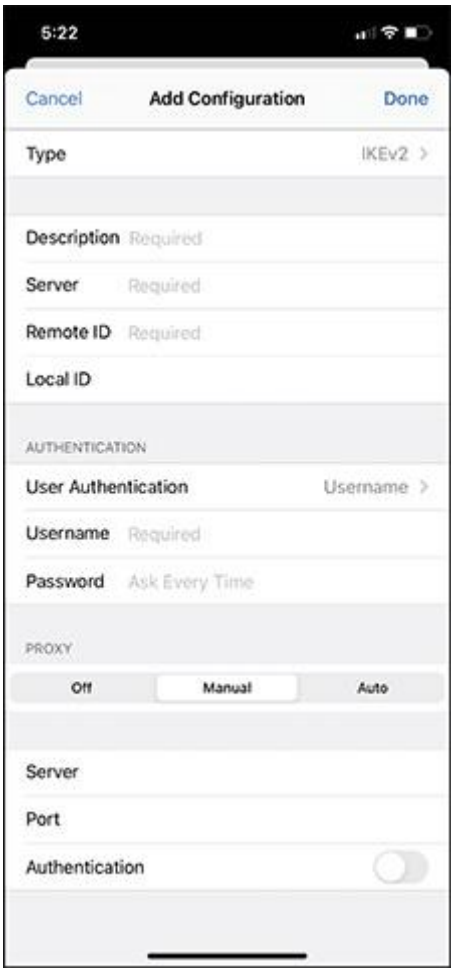

If you have roaming enabled, especially for a CDMA device, you'll want to keep the **Preferred Roaming List (PRL)** updated. The PRL is a database file that lists the preferred service providers or radio frequencies your carrier wants the device to use when outside your home network. To update the PRL, follow instructions from your carrier. For example, for Verizon, you dial *228, and select 2 to update your PRL. When the update completes, a message appears on your phone. For an Android phone, you then need to power down the device and turn it back on.

## Note 7

Like desktop computers, a mobile device can be configured to communicate information securely over a virtual private network (VPN) connection. To create a VPN connection, in the Android Settings app, tap **Connections**, **More connection settings**, and **VPN**. In iOS Settings, tap **General**, **VPN**. To set up the VPN, you'll need to know the type of encryption protocol used (IKEv2, IPsec, or L2TP), the IP address or domain name of the VPN server, and the user name and password to the corporate network. Figure 9-17 shows the configuration options on an iOS smartphone. Also, Google offers a VPN connection for Android devices using the Google One mobile app when you subscribe to Google cloud storage.

## Figure 9-17

Configure a VPN connection in iOS




# 9-1h Location Services

## Core 1 Objective

- 1.4

Given a scenario, configure basic mobile-device network connectivity and application support.

Many mobile apps, such as Google Maps, require a location service to work. The following are two services a mobile device might use:

- **GPS.** A **GPS (Global Positioning System)** feature is embedded in smartphones, smart watches, tablets, some automobiles, and even some medical devices, making it possible to identify the device's location in relation to multiple satellites in orbit around the Earth. GPS data is never sent to these satellites; the device receives the data to determine its location. However, the device might send GPS location data to Apple or Google.
- **Cellular location service.** A mobile device can also determine its location from Bluetooth, crowd-sourced Wi-Fi, and cellular databases. These databases are built from geotagged locations of Wi-Fi hotspots and cell towers using anonymous and encrypted data sent from devices.

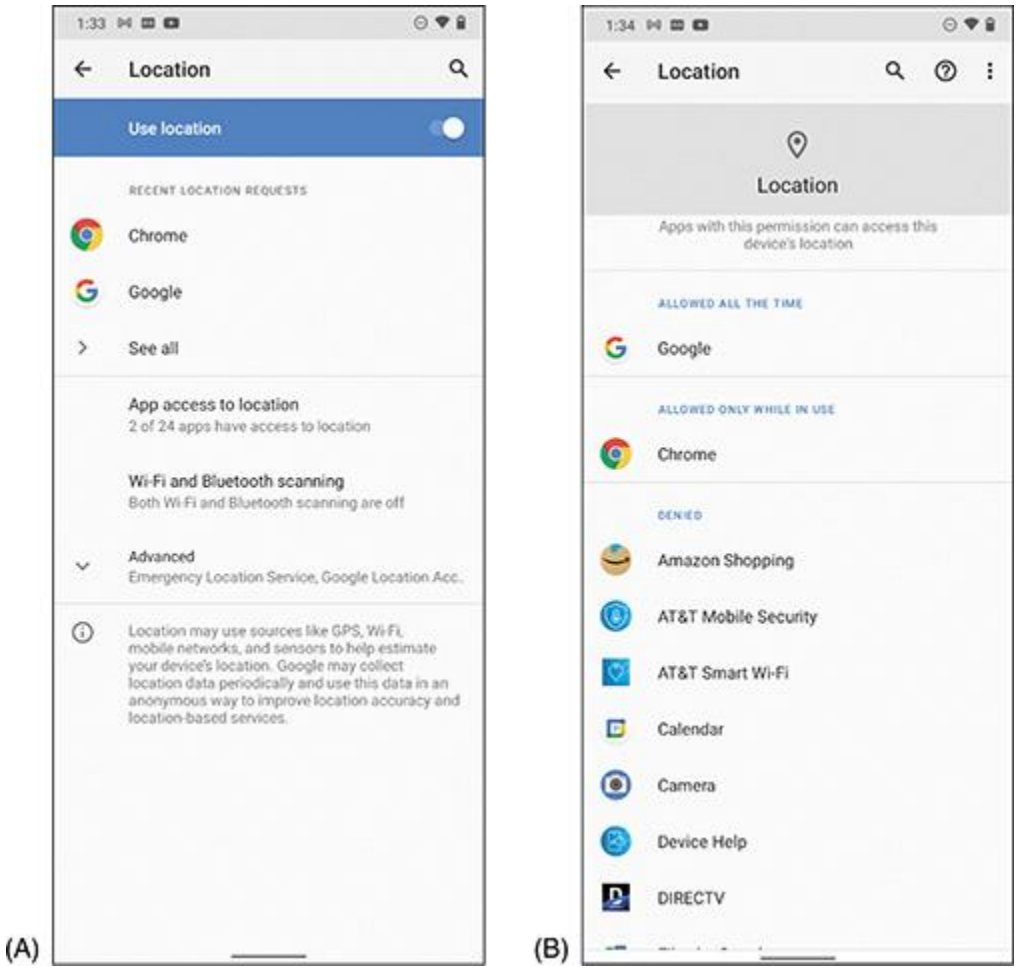
Location services are managed by Apple for iOS and iPadOS and by Google for Android. Using the Settings app, you can turn off location services and decide how apps can use the service. However, know that Apple or Google still has the right to locate your device—for example, when you place an emergency phone call or to

enhance their crowd-sourced location database—even if location services is turned off.

To manage the location services on an Android device, in the Settings app, tap **Location**. See Figure 9-18A. To change the way apps can use location services, tap **App access to location** (see Figure 9-18B). For Apple devices, in the Settings app, tap **Privacy** and **Location Services** to turn the service on or off.

## Figure 9-18

(A) Manage location services in the Settings app, and (B) fine-tune which apps can use Location services




# 9-1i PAN Connections

## Core 1 Objectives

- 1.1

  Given a scenario, install and configure laptop hardware components.
- 1.3

  Given a scenario, set up and configure accessories and ports of mobile devices.
- 1.4

Given a scenario, configure basic mobile-device network connectivity and application support.

- 2.3

Compare and contrast protocols for wireless networking.

Mobile devices typically have the capability to connect to other nearby wireless devices and accessories using a Bluetooth or NFC wireless connection:

- **Bluetooth.** Bluetooth is a short-range (about 30 feet or 10 meters) wireless technology used to connect two devices in a small PAN. To create a Bluetooth connection, the two devices must be **paired**, a process you'll learn more about later in this module. Figure 9-19 shows a smartphone connected to a Bluetooth speaker.

## Figure 9-19

Smartphone connects to speaker via Bluetooth


iStock.com/Magnetic-Mcc

- **NFC. Near-field communication (NFC)** is a wireless technology that establishes a communication link between two NFC devices that are within 10 centimeters (about 4 inches) of each other. For example, an NFC tag (see Figure 9-20) contains a small microchip that can be embedded in just about anything, including a key chain tag, printed flyer, or billboard. The NFC tag dispenses information to any NFC-enabled smartphone or other device that comes within 4 inches of the tag.

## Figure 9-20

These programmable NFC tags have sticky backs for attaching to a flat surface such as a wall, desk, or car dashboard


NFC is a form of RFID; they both operate near the 13.56 MHz radio frequency. **RFID (radio-frequency identification)** is traditionally used in small tags that attach to and identify clothing inventory, car keys, bags, luggage, pets, cattle, hospital patients, and much more. An RFID tag contains a microchip and antenna and can be a passive or active tag. Active RFID tags have built-in batteries and transmitters to respond to commands or requests for information. Passive RFID tags, which cost much less, are essentially electronic barcodes that can be read from a few feet away without requiring line-of-sight access.

NFC operates at a slightly higher frequency than RFID, and its range is shorter, which makes it more secure. For example, two iPhones must be very close to each other for NFC to work. Although NFC can read RFID tags, a mobile device does not communicate peer-to-peer with RFID devices.

## Contactless Payments

Credit card transactions processed using Apple Pay or Google Pay use NFC when the device comes close to a point-of-sale terminal. The transaction uses **two-factor authentication (2FA)**, which means two actions are needed to authenticate the payer. **Biometric authentication** can include a fingerprint or facial recognition. For example, when your iPhone comes near a point-of-sale terminal (see Figure 9-21), and you enter a passcode or PIN to access your phone, Apple Pay displays the payment amount on your phone for you to accept. You can then use FaceID or Touch ID to authenticate your face or fingerprint to complete the transaction.

**Figure 9-21**

Use NFC wireless with an iPhone to create a contactless payment


Prykhodov/ Dreamstime.com

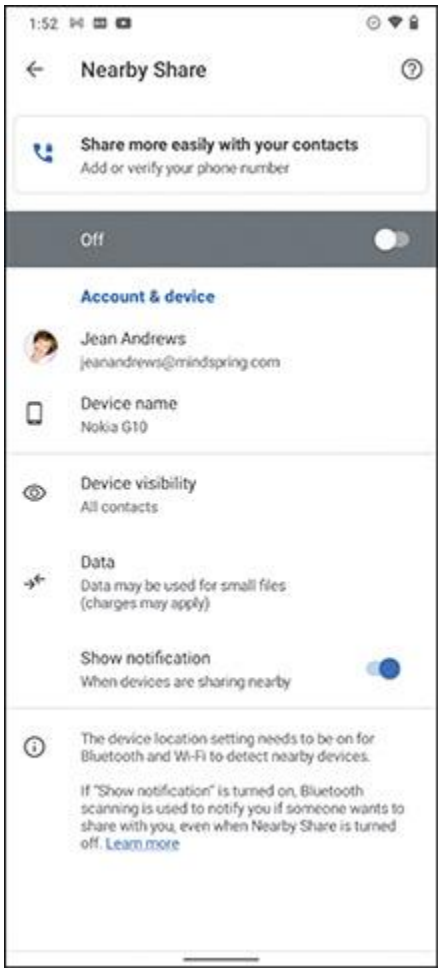
## Near-Field Privacy

Wi-Fi, Bluetooth, and NFC technologies can be used to share data between two devices when they are in close range. To protect your privacy and secure the data on your device, you can manage this near-field scanner feature as follows:

- **Android Nearby Share.** On an Android device, in the Settings app, tap **Google**, **Devices & sharing**, and **Nearby Share** (see Figure 9-22). To control which contacts can be shared, tap **Device visibility**. You can share or hide all contacts or share just a few. When notifications are turned on, you will be notified when another device is scanning for a near-field connection.

**Figure 9-22**

Manage what can be shared with near-field scanning on an Android device




- **iOS and iPadOS AirDrop. AirDrop** is an Apple wireless standard that uses both Bluetooth and Wi-Fi to provide near-field (within 30 feet) data transfers between iPhones, iPads, Macs, and other Apple devices. (AirDrop won't share with an Android device.) To manage AirDrop, swipe down from the upper-right corner of the screen to open the **Control Center** (see Figure 9-23A), press and hold the top-left group of controls, and tap the **AirDrop** icon (see Figure 9-23B). Then you can decide to turn AirDrop on or off and decide to share an item only with your contacts or with everyone. (You can also control AirDrop settings in the Settings app under General.) To share a selected item, tap the **Share** icon, and then tap **AirDrop** in the list of ways to share the item.

## Figure 9-23

Press and hold the upper-left group of icons in the iOS Control Center to see two more icons in this group, including AirDrop


## Exam Tip

The A+ Core 1 exam expects you to be able to contrast and compare Bluetooth, NFC, and RFID. You also need to know how to make a Bluetooth connection and understand what two-factor authentication is.

## Applying Concepts

### Pairing Bluetooth Devices

- **Est. Time:** 15 minutes
- **Core 1 Objective:** 1.3

To configure a Bluetooth connection, complete the following steps:

1. 1
   Turn on the Bluetooth device—such as a speaker, headset, webcam, or keyboard—to which you want to connect your mobile device.

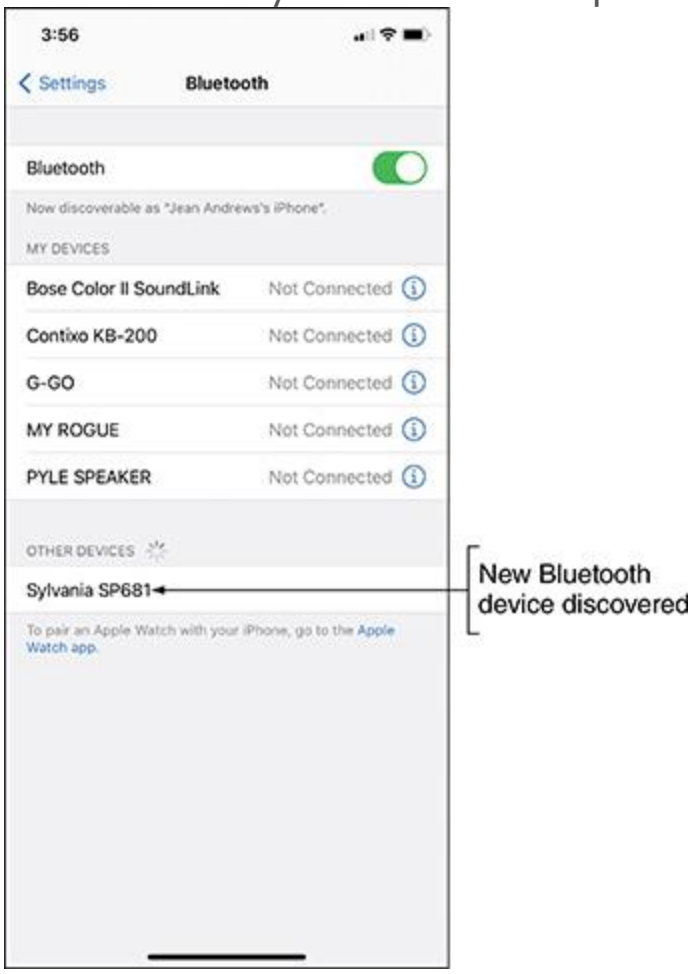
2. 2
   Enable Bluetooth on the device and enable pairing mode. Sometimes just turning on Bluetooth enables pairing automatically for a limited period of time. The device might have a pairing button or combination of buttons to enable pairing and a light that blinks to indicate the device is ready to receive a Bluetooth connection. This makes the device discoverable, which means it's transmitting a signal to identify itself to nearby Bluetooth devices.

3. 3

On your mobile device, turn on Bluetooth. The mobile device searches for Bluetooth devices. If it discovers the Bluetooth device (see Figure 9-24), tap it to connect. The two Bluetooth devices now begin the pairing process. Some Bluetooth devices might require a code to connect. For example, when an iPad and Bluetooth keyboard are pairing, the iPad displays a four-digit code that must be entered on the keyboard.

## Figure 9-24

Tap to connect the iPhone to the Sylvania Bluetooth speaker it has detected




4. 4
   Test the connection. For an audio device, play a video or audio recording on the mobile device, and for a keyboard, type into a notes application or text box.

### Exam Tip

The A+ Core 1 exam might give you a scenario that requires you to pair Bluetooth devices and then test connectivity after the connection is established.

## Note 8

You can automatically disable a mobile device antenna that transmits signals by enabling airplane mode so that the device can neither transmit nor receive the signals. Many newer devices do not disable the GPS or NFC antennas; GPS only receives and never transmits, and NFC signals don't reach very far. While airplane mode is on, you can manually enable some wireless connections, such as Bluetooth or Wi-Fi.

# 9-1j Mobile Device Ports and Accessories

## Core 1 Objective

- 1.3

Given a scenario, set up and configure accessories and ports of mobile devices.

You can buy all kinds of mobile device accessories, such as wireless keyboards, touch pens, speakers, webcams, earbuds, headsets, game pads, docking stations, printers, extra battery packs and chargers, USB adapters, memory cards (usually the microSD form factor) to expand storage space, credit card readers for accepting payments by credit card, and protective covers for waterproofing. For example, Figure 9-25 shows a Bluetooth headset.

## Figure 9-25

Bluetooth over-the-ear headset designed to connect with a smartphone

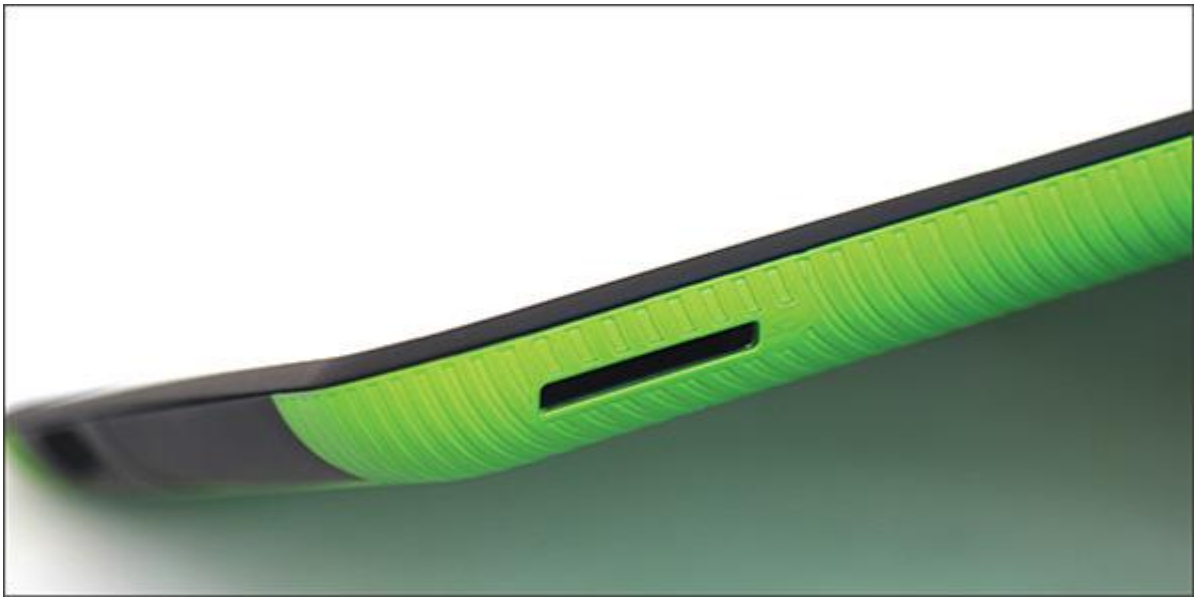

Source: Amazon.com, Inc.

When buying accessories for a mobile device, be sure to check what ports and slots are available on the device. For example, many mobile devices no longer include replaceable batteries. Current iPhones no longer have audio ports—to use a wired headset, you have to plug a dongle into the Lightning port. Some mobile devices have a slot for a memory card, which might be located on the side of the case or inside it;

however, Apple mobile devices and many others don't offer this feature. Figure 9-26 shows a memory card slot on an Android tablet, and Figure 9-27 shows a MicroSD card.

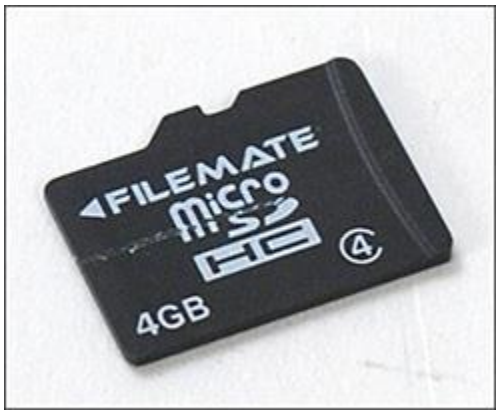
## Figure 9-26

An Android device might provide a memory card slot to allow for extra storage



## Figure 9-27

A mobile device might use a microSD card to add extra flash memory storage to the device



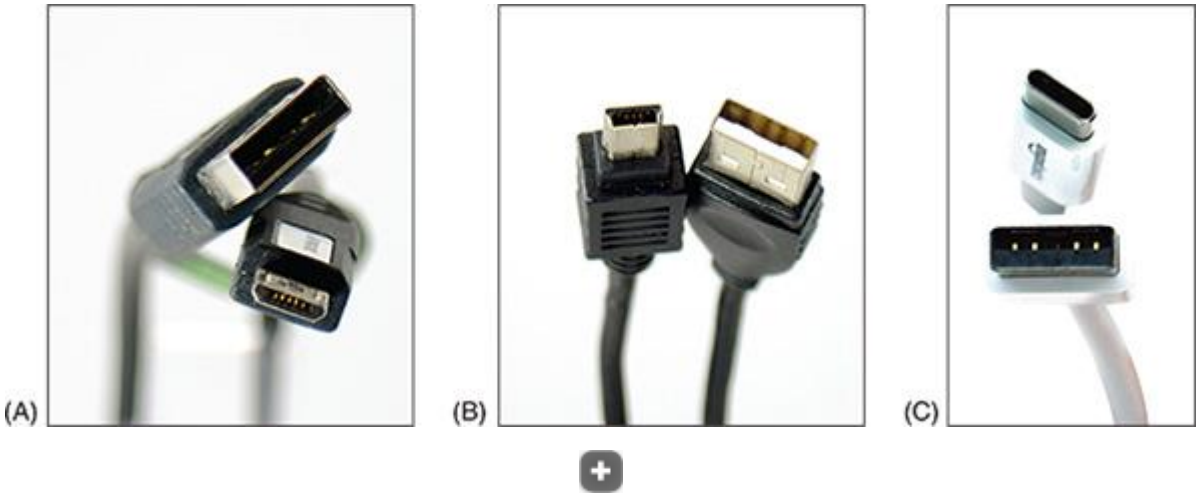

### Wired Connections for Accessories

Smartphones, tablets, and wearable devices can make a wired connection to a computer. This connection can be used to charge the device, download software updates, upload data to the computer, back up data, and restore software or data. The device's port used for power and communication may be a type of USB (Universal Serial Bus) port or a proprietary, vendor-specific port. Some USB connectors used for this purpose include microUSB (see Figure 9-28A), the smaller miniUSB (see Figure 9-

28B), and the newer USB-C (see Figure 9-28C). USB-C is the first USB connector that can plug into a port in either orientation. Apple iPhones, iPods, and iPads use the proprietary **Lightning port** and connector for power and communication (see Figure 9-29). Some newer iPads use the USB-C connector.

## Figure 9-28

Some mobile devices may connect to a computer's USB port by way of a (A) microUSB, (B) miniUSB, or (C) USB-C cable




## Figure 9-29

A Lightning cable by Apple Inc. has a USB connector for the computer end and a Lightning connector for an iPhone or iPad

Also know that you can use USB adapter cables to work with the port your device has. For example, you can purchase a Lightning-to-USB-C adapter cable or a miniUSB-to-Ethernet adapter cable. You can even buy a USB to serial port adapter cables when you need to connect your tablet to a Linux server in a server room. (A server is likely to provide a serial port for that purpose.) See Figure 9-30.

## Figure 9-30

A serial-to-USB adapter


Source: Amazon.com, Inc.

**Exam Tip**

The A+ Core 1 exam expects you to know about USB-C, microUSB, miniUSB, Lightning, and serial wired connections.

# 9-2 Mobile Apps for Business Use

## Core 1 Objectives

- 1.4

  Given a scenario, configure basic mobile-device network connectivity and application support.

- 4.1

  Summarize cloud-computing concepts.

In this section of the module, you learn how to support mobile devices that are used for corporate and business needs, including configuring corporate email and synchronizing devices for email and other corporate applications.

# 9-2aMobile Devices Managed by Corporate Policies

## Core 1 Objective

- 1.4

Given a scenario, configure basic mobile-device network connectivity and application support.

Corporations and schools might provide corporate-owned devices, which are secured and managed by corporate policies and procedures, and/or the organization might have **BYOD (bring your own device)** policies and procedures. With BYOD, an employee or student is allowed to connect their own device to the organization's network. For security purposes, an organization configures the person's device before allowing it to connect to the network.

Large corporations use **mobile device management (MDM)** software that provides tools for securing and tracking mobile devices—even when they're turned off—and managing the data on those devices. Examples of MDM software suites include Verizon MDM, Apple MDM for Apple products, Scalefusion for Android devices, and Microsoft Endpoint Manager. **MDM policies** typically include the following:

- Security policy enforcement, such as applying patches, enforcing password requirements, and requiring two-factor authentication
- Data encryption requirements, to protect data on the mobile device if it falls into the wrong hands, and synchronization of that data to cloud storage for backups
- Remote lock-and-wipe capabilities, to lock down a device and erase all data on it
- Restrictions on the use of unsecured apps

To do all this, MDM installs a small app called an **agent** on a managed mobile device, which communicates through various Wi-Fi or cellular connections back to the MDM server in the company data center. The initial installing of the agent and the agent checking the device for security compliance is called **on-boarding**. The reverse process when the mobile device is removed from the MDM fleet is called **off-boarding**.

When a corporation needs to keep financial, regulated, or other sensitive data on an employee's personal device, it might choose to enhance MDM with software that specifically targets protecting corporate apps and their data. **Mobile application management (MAM)** software serves that purpose by the following processes:

- Separating corporate data and apps from personal data and apps on a device, which is called sandboxing these corporate assets.
- Assuring that corporate data is only transmitted over a secure and encrypted connection, called a VPN (Virtual Private Network). The data is encrypted when it is at rest on the device and in transit.
- Managing and updating corporate applications remotely.

When MAM is protecting corporate data and apps, the user normally has more freedom to install their own personal apps and data on their device. MAM software is sometimes a part of MDM software, and it can also be a standalone product that works in addition to MDM software.

# 9-2bConfigure Mobile Device Email

## Core 1 Objective

- 1.4

Given a scenario, configure basic mobile-device network connectivity and application support.

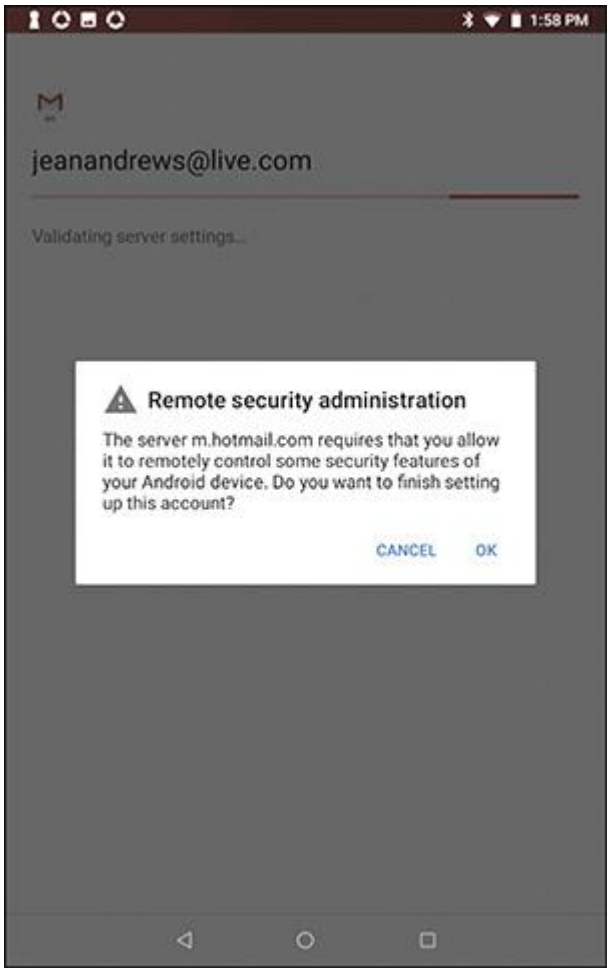
Android has its Gmail app, and iOS has its Mail app; either app can work with any email provider. Rather than using OS embedded mail apps, you can install your own. For example, Blue Mail or Spark are free open-source mail apps, and Polymail (polymail.io) and Microsoft Outlook (Microsoft.com) are paid-for **commercial mail apps**.

## Note 9

When configuring corporate email addresses, messages such as that shown in Figure 9-31 might appear asking for permission to apply extra security to the device.

## Figure 9-31

Corporate email services might require extra security on a device




To configure email in iOS, use the Settings app. In Settings, tap **Mail**, **Accounts**, and **Add Account**. A list of popular email providers appears (see Figure 9-32). If your provider is not in the list, tap **Other** and enter the requested information to set up email, contacts, and calendars. For Android, tap the **Gmail** app, and then tap **Add an email address**.

## Figure 9-32

When setting up email in iOS, select an email provider


Here is the information you'll need to configure an email app on a mobile device:

- **Your email address and password.** For iOS, iPadOS, and Android, if your email account is with Google, Microsoft Exchange, Outlook, Yahoo!, or AOL (iPhone and iPad only), your email address and password are all you need because the OS can automatically set up these accounts. If you are setting up a work account that uses Microsoft 365 for business, don't use the Outlook option, but rather check with your administrator for server settings.

**Note 10**

**Microsoft Exchange** is a private enterprise email service that is hosted on corporation or ISP servers to provide company email addresses and includes email, calendars, and contacts services. It can integrate with MDM software suites to enforce MDM policies on mobile devices.

If your email account is with any other provider, you'll also need the following information:

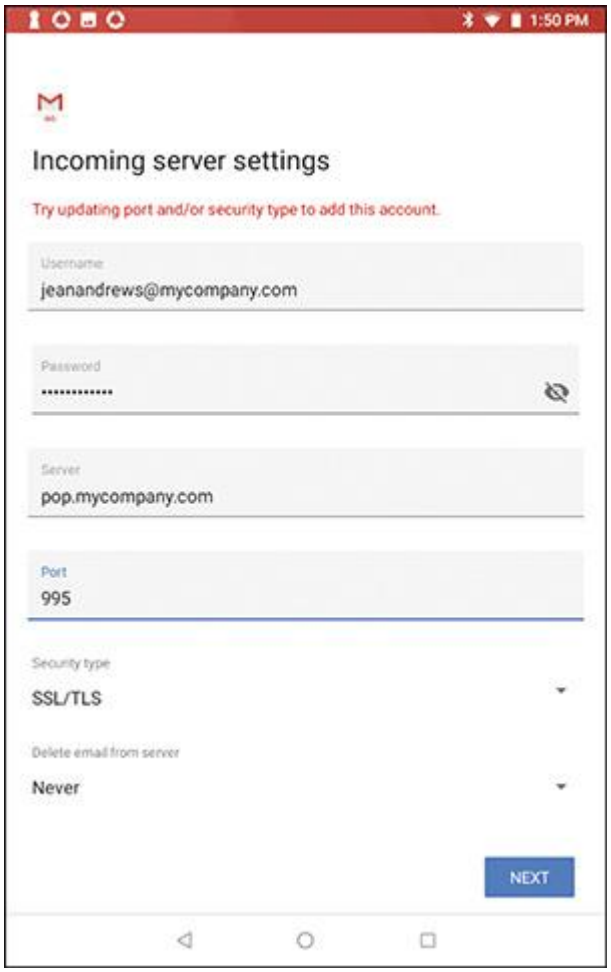
- **Names of your incoming and outgoing email servers.** To find this information, check the support page of your email provider's website. For example, the server you use for incoming mail might

be imap.mycompany.com, and the server you use for outgoing mail might be smtp.mycompany.com. The two servers might have the same name.

- **Type of protocol your incoming server uses.** The incoming server uses IMAP4 or POP3. With IMAP4, you are managing your email on the server. For example, you can move a message from one folder to another on your device, which causes that change to happen on the remote server. Using POP3, the messages are downloaded to your device, where you manage them locally. Most POP3 mail servers give you the option to leave the messages on the server or delete them after they are downloaded.
- **Security used.** Most likely, if email is encrypted during transmission, the configuration will happen automatically, without your involvement. However, if you have problems, you need to be aware of these possible settings for the incoming server:
    - An IMAP server uses port 143 unless it is secured and using SSL/TLS, which uses port 993.
    - A POP3 server uses port 110 unless it is secured and using SSL/TLS, which uses port 995 (see Figure 9-33).

**Figure 9-33**

A POP3 email server might use SSL/TLS encryption and port 995




- **Outgoing server.** Previously, outgoing email was sent using the SMTP protocol, which uses port 25. Now, most SMTP servers support secure SMTP, which uses TLS encryption for sending messages and port 587 or 2525 as an alternative port.

## Exam Tip

The A+ Core 1 exam expects you to know about POP3, IMAP, SMTP, and the ports they use, and it might require you to use this information in configuring email on a mobile device. Before you sit for the exam, memorize the protocols and ports discussed in this section, and understand how this information is used to configure email on a mobile device. A project at the end of this module will give you practice with this process.

When setting up corporate email that uses Microsoft Exchange, know that the Exchange server can control how the email service works on a mobile device based on MDM policies. These policies can include how email, calendars, contacts, and tasks are synced between the server and the device. Within Exchange, **ActiveSync** is responsible for syncing data between the server and device. If ActiveSync is disabled at the server end, no Exchange data is synced, which means no data is kept on the device, and, therefore, it is not available to the user when the mobile device is offline (not connected to the Internet). In addition, ActiveSync can perform remote wipes and enforce password policies and data encryption.

## Exam Tip

The A+ Core 1 exam expects you to describe the functions of ActiveSync in Microsoft Exchange.

# 9-2c Mobile Device Synchronization

## Core 1 Objectives

- 1.4

  Given a scenario, configure basic mobile-device network connectivity and application support.

- 4.1

  Summarize cloud-computing concepts.

In this section of the module, you learn to use a Google or Apple account to sync or mirror data among your devices and the cloud. For example, a photo taken, new contact added, or calendar event created on one device is available in the cloud and on all other devices. As another example, when you sync email, the email app on your phone shows the same email messages as the browser or email client on your desktop computer.

## Caution

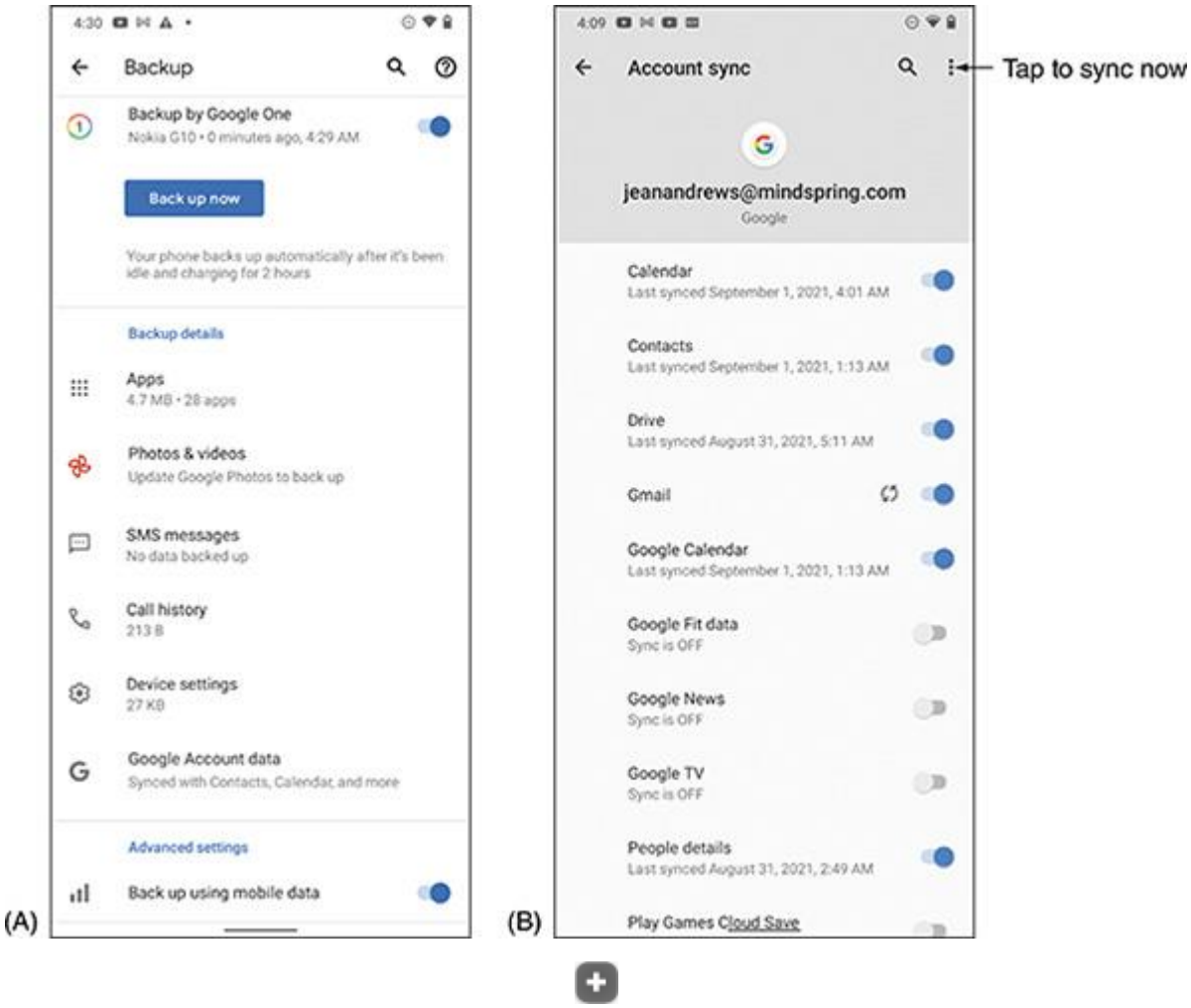
It's not safe to store passwords in your browser. It's much more secure to use a password manager app, such as KeePass (keepass.info) or LastPass (lastpass.com). KeePass stores passwords only on the local computer, which is more secure but less convenient. LastPass can store passwords in the cloud and sync passwords across devices, which is more convenient but less secure.

### Google Syncing

All data that Google keeps under your account at google.com can be synced with your Android devices. In the Google cloud, the first 15 GB of cloud storage is free. With Android devices, to manage what is synced, open the **Settings** app, tap **Google** and **Backup** (see Figure 9-34A). Then tap **Google Account data**. On the Account sync screen (see Figure 9-34B), turn on or off syncing for each type of Google account data. To sync now, tap the three-dot icon in the upper-right corner of the screen, and tap **Sync now**.

## Figure 9-34

(A) Manage Google Backup and (B) manage Google account data syncing




You can choose whether to sync only over Wi-Fi so that syncing doesn't use up your cellular data caps. On the Backup screen, shown in Figure 9-34A, turn on or off *Back up using mobile data.*

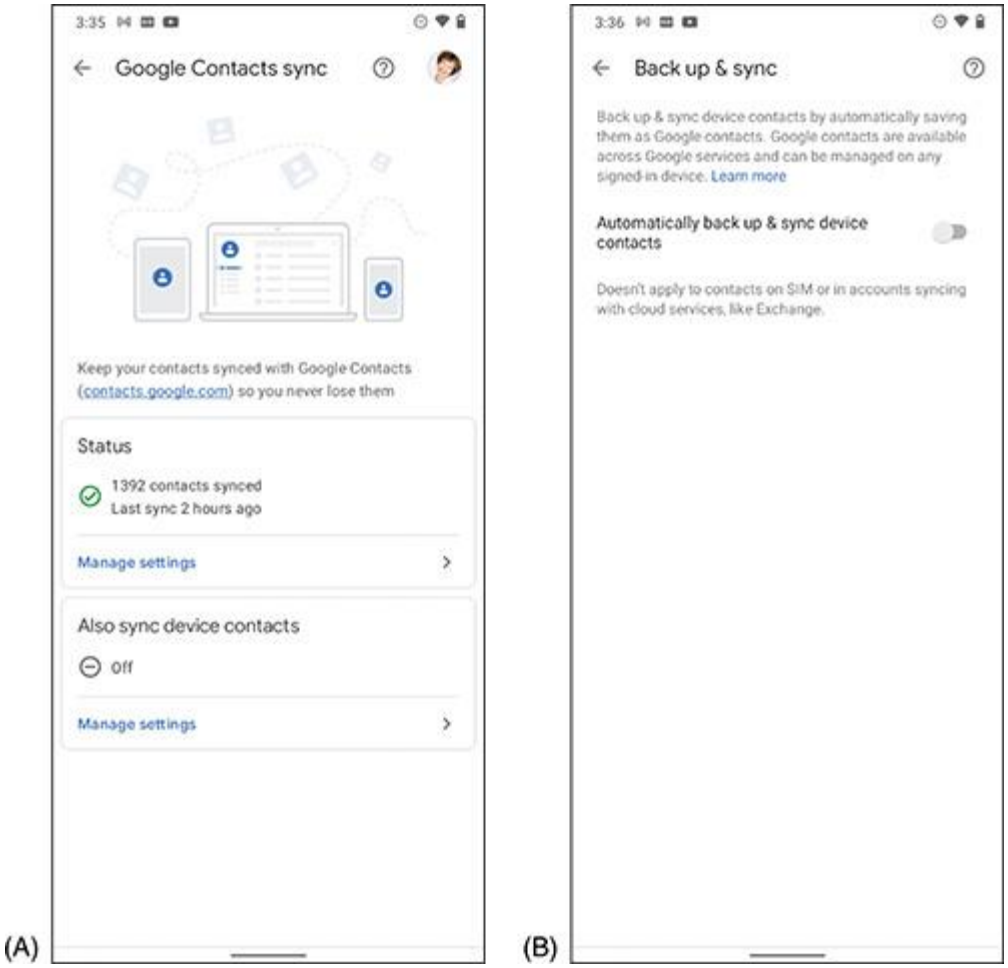
You can also control additional sync settings in the Settings app and in individual apps:

- **Contacts syncing.** Use the Settings app to sync Contacts:

    1. Open the **Settings** app, tap **Google**, **Settings for Google apps**, and **Google Contacts sync**. Notice in Figure 9-35A that Google contacts are syncing. To change this setting, tap **Manage settings** under Status. On the next screen, you can turn syncing off and on (see Figure 9-35B).

## Figure 9-35

(A) Manage Google contact syncing and (B) turn on syncing of non-Google contacts



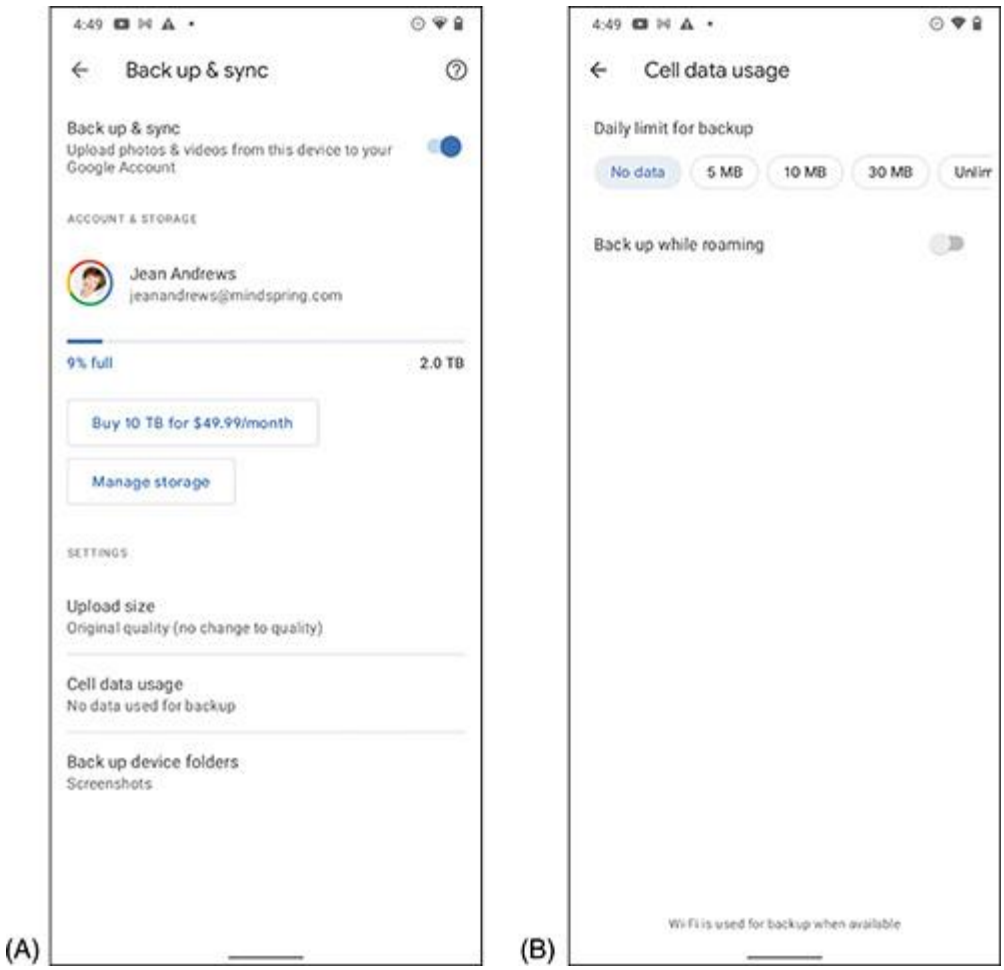

2. Notice in Figure 9-35A that *Also sync device contacts* is off. When this setting is turned on, non-Google contacts—such as contacts kept by the Covve (covve.com) app, a third-party contact app—can be imported as Google contacts and synced by Google. Tapping **Manage settings** in this area changes the way Google handles non-Google contacts, as shown in Figure 9-35B.

- **Photo syncing.** Use the Photo app to manage photo syncing:

1. Open the **Photo** app, and tap the account profile icon (your photo) in the upper-right corner. Then tap **Photos settings** and **Back up & sync** (see Figure 9-36A). Using this screen, you can turn on and off photo syncing.

## Figure 9-36

(A) Turn on and off photo syncing and (B) manage data usage for photo syncing

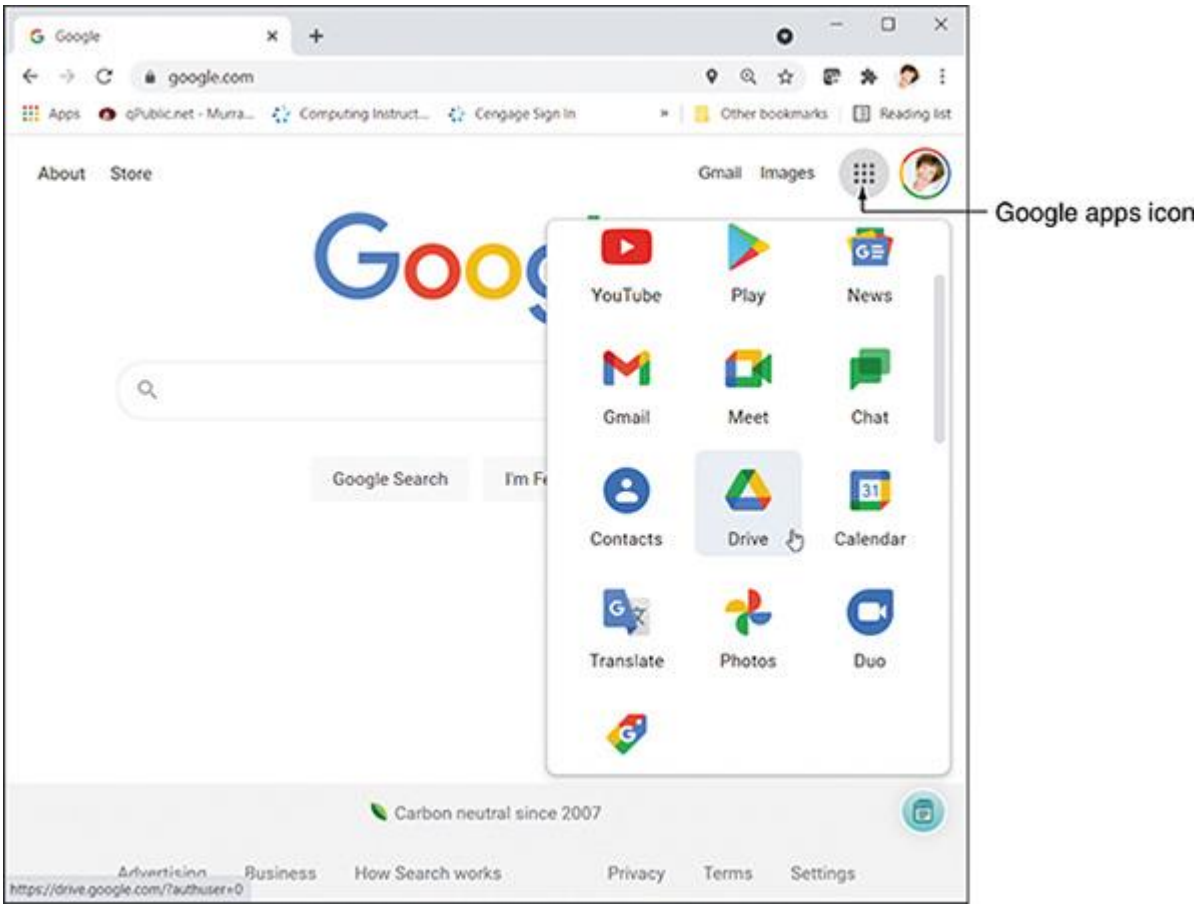



2. To manage how cellular data is used for photo syncing, tap Cell data usage (see Figure 9-36B).

To access your content in the cloud, use a browser on any computer to go to google.com and sign in to your Google account. A single sign-on (SSO) for multiple services gives access to Gmail, Google Drive, Calendar, Contacts, Photos, and other content. Click the **Google apps** icon to select different apps, as shown in Figure 9-37. When you select an app, such as Contacts or Calendar, the content in that app displays. You can also go directly to the Google content using direct links, such as contacts.google.com, photos.google.com, and calendar.google.com.

## Figure 9-37

Access Google content on the web at google.com




Source: Google.com

For a monthly fee, you can subscribe to Google Workspace Individual, which offers enhanced versions of Google Meet (a video conferencing tool), Google Calendar, and Gmail. Google Workspace for an organization is managed via an Admin console where you can add new users, migrate user content, and manage cloud storage and file sharing. To set up a user account on a mobile device for Google Workspace Individual or Google Workspace for an organization, follow the directions at support.google.com/a/answer/3035792.

## Exam Tip

The A+ Core 1 exam expects you to know how to manage contact and calendar syncing in Android and Apple devices.

### Apple Syncing

iOS and iPadOS sync content to the Apple website at icloud.com; the first 5 GB of cloud storage is free. Here is what you need to know about Apple syncing:

- **Manage what is synced.** To set up iCloud syncing, go to the **Settings** app on your iPad or iPhone, tap the user name, and tap **iCloud** to go to the screen (see Figure 9-38) where you can manage your iCloud storage and decide which apps and data get synced (including contacts and calendars).

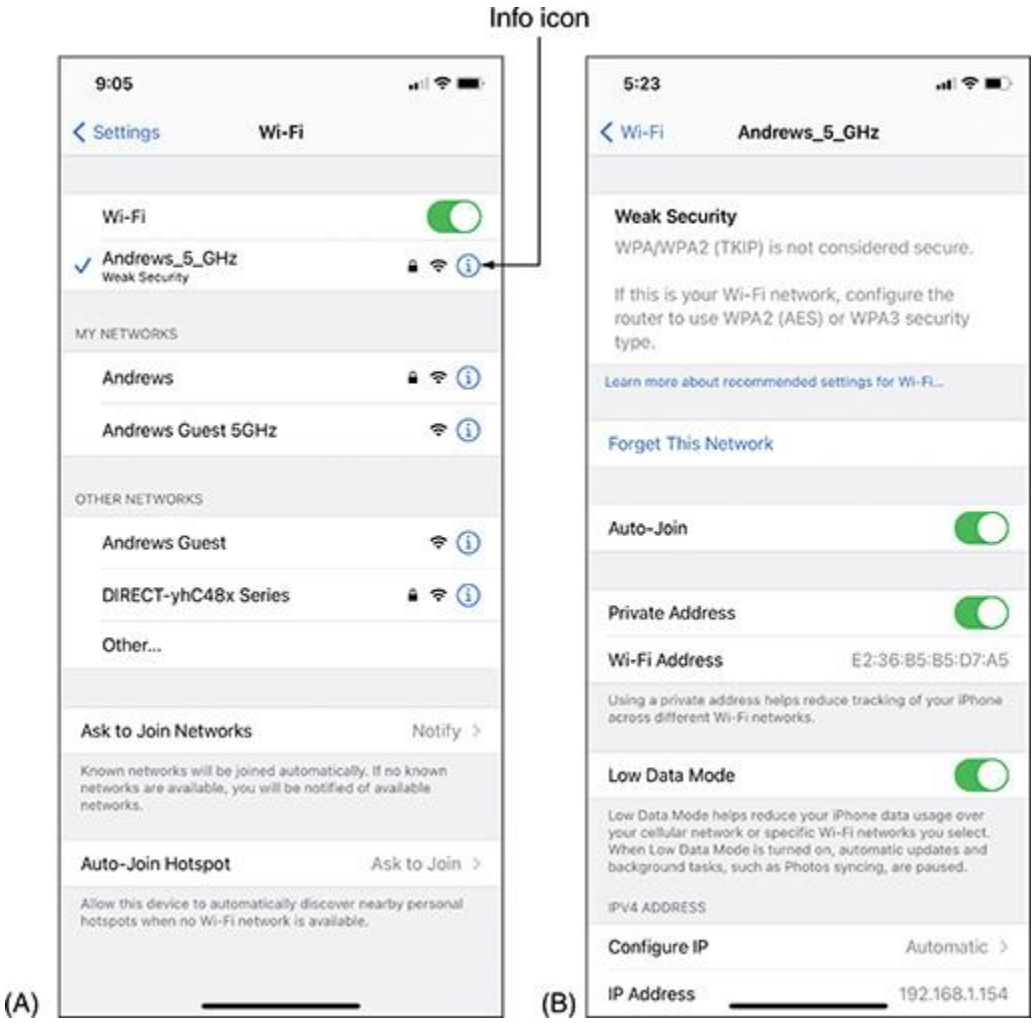
**Figure 9-38**

Manage iCloud syncing and storage on an iPhone


- **Manage cellular data used for syncing.** In the Settings app, tap **Wi-Fi** (see Figure 9-39A), and then tap the Info icon beside the current Wi-Fi connection. On the next screen (see Figure 9-39B), the Low Data Mode can be turned on or off to control how cellular data is used. When Low Data Mode is on, automatic updates and data syncing is paused unless there is a Wi-Fi connection.

## Figure 9-39

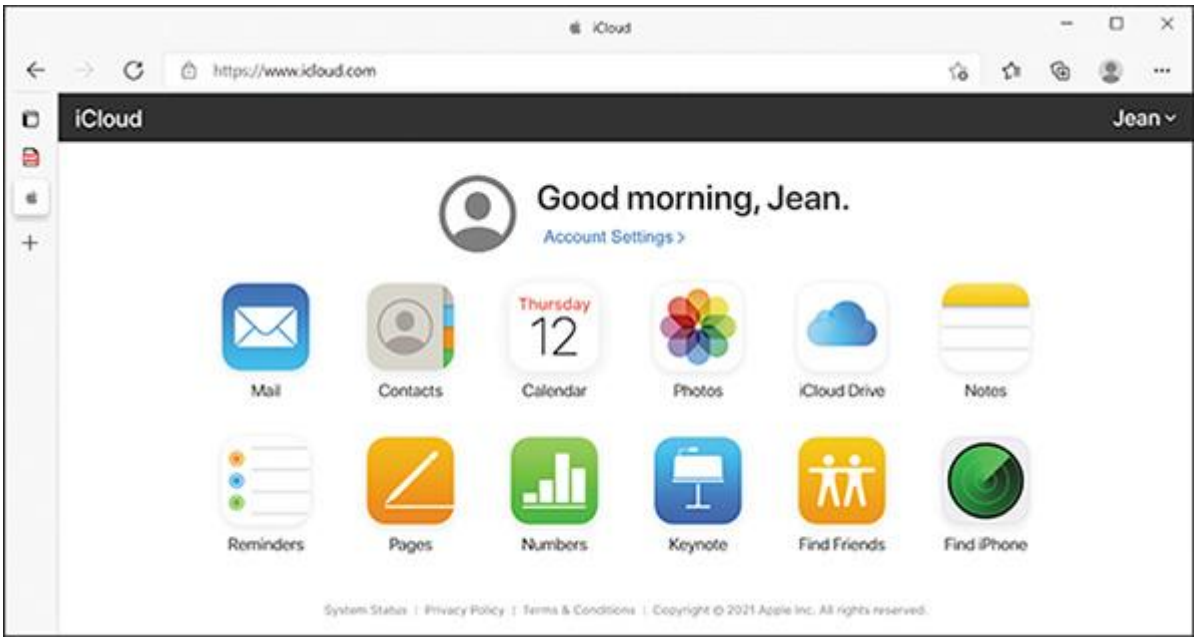
Manage Low Data Mode to limit syncing only when Wi-Fi is available




- **Manage content in iCloud.** You can access synced data in the cloud from your computer by signing in to your Apple account at icloud.com. Figure 9-40 shows the home page for your iCloud content, including Mail, Contacts, Calendar, iCloud Drive, and location data, among others. Click an item to drill down into its content.

## Figure 9-40

Access iOS content at icloud.com




## Microsoft 365, OneDrive, and SharePoint

Third-party apps and services can also be used to sync data. One example is **Microsoft 365**, previously called Office 365, which is a suite of productivity apps, including Word, Excel, PowerPoint, Outlook, and Visio. A subscription to Microsoft 365 includes 1 TB of OneDrive cloud storage (onedrive.live.com). Microsoft 365 installs on desktops, laptops, tablets, and smartphones and syncs data to OneDrive on multiple devices and in the cloud. When setting up a Microsoft 365 account for business, ask your administrator for the correct server settings for the account. Teams can collaborate with documents stored in OneDrive, or an individual user can share a document on OneDrive with anyone with a Microsoft account. OneDrive works well for syncing data for an individual or a few team members. SharePoint also provides cloud storage that integrates with Microsoft 365 but goes further than OneDrive as powerful content collaboration and management software in an enterprise.

### Exam Tip

The A+ Core 1 exam expects you to know about mobile device synchronization with Microsoft 365.

# 9-3 Troubleshooting Mobile Devices

## Core 1 Objective

- 5.5

Given a scenario, troubleshoot common issues with mobile devices.

As an IT support technician for mobile devices, know that they contain few field replaceable units (FRU), or hardware that can be replaced by field technicians. The cost of repairing the device—including parts, special tools, and labor—generally exceeds the value of replacing the device. Although it is

possible to replace the screens in some mobile devices, a support technician is generally not expected to take the time to do so.

There are, however, many problems with a device that you can troubleshoot using tools within the OS. When learning to troubleshoot any OS or device, remember the web is a great source of information. Depend on the support.google.com/android and support.apple.com websites to give you troubleshooting tips and procedures for their respective operating systems and mobile devices. For Android devices, also look for help on the device manufacturer website. Let's start with exploring the tools you need to troubleshoot mobile devices.

# 9-3a Troubleshooting Techniques

## Core 1 Objective

- 5.5

Given a scenario, troubleshoot common issues with mobile devices.

The following steps are ordered to solve a problem while making the least changes to the system (i.e., try the least invasive solution first). Try the first step; if it does not solve the problem, move on to the next step. With each step, first make sure the device is plugged in or already has sufficient charge to complete the step. After you try one step, check to see if the problem is solved before you move on to the next step. Here are the general steps we're following, although some might not be possible, depending on the situation:

1. 1
   Close, uninstall, and reinstall an app. Too many open apps can shorten battery life and slow down device performance. If you suspect an app is causing a problem, uninstall it and use the app store to reinstall it.
2. 2
   Use the Settings app to update the OS.
3. 3
   Restart the device (also called a soft boot) and reboot the device (also called a hard boot). This step is covered in more depth in the following section.

### Restart or Reboot the Device

A restart powers down the device and restarts it, which is similar to a Windows restart. A reboot, also called a hard boot, is similar to a Windows shutdown and performs a full clean boot. First try a restart, and if that doesn't fix the problem, try a hard boot:

- 1.

**Restart the device, also called a soft boot.** To restart an Android device, press and hold the power button, and select **Restart** (see Figure 9-41). To restart an iPhone or iPad, press and hold the side or top button, and slide the power-off message to the right. To turn the device back on, press and hold the Android power button or the iPhone or iPad side or top button. Power cycling a smartphone every few days is a good idea to keep the phone functioning at peak efficiency.

**Figure 9-41**

Restart an Android device


- 2.

  **Reboot the device using a hard boot.** When the menus in a device don't work or the device freezes entirely, a full clean boot might help. For most Android devices, hold down the power button to see the menu shown in Figure 9-41, and tap **Power off** twice. If that doesn't work, try holding down the power button and the volume-down button at the same time. (Check Android device manufacturers for details.) To reboot an iPhone or iPad, hold down the side or top button and the volume-down button at the same time until the Apple logo

appears. (For older iPhones and iPads, press and hold the side or top button and the Home button.)

If the device has a removable battery and it refuses to hard boot, you can open the back of the device and then remove and reinstall the battery as a last resort (unless the device is under warranty).

In the module "Mobile Device Security," you learn more troubleshooting techniques to solve mobile device problems, including how to repair and reinstall the OS, perform a factory reset, and recover the system.

# 9-3b Common Mobile Device Malware Symptoms

**Core 1 Objective**

- 5.5

Given a scenario, troubleshoot common issues with mobile devices.

Android mobile devices are more susceptible to malware than iPhones and iPads because apps can be downloaded from sites other than Google. With iOS and iPadOS, apps can be obtained only from the Apple App Store and are therefore more strictly vetted. However, for any mobile device, malware can be introduced by a Trojan that a user accepts (for example, as an email attachment) or by macros embedded in shared documents.

Here are some symptoms that indicate malware might be at work on an Android, iOS, or iPadOS device:

- **Power drain, sluggish response time, slow data speeds, high network traffic, high number of ads, data-usage limit notification, limited or no Internet connectivity.** All these symptoms can indicate that apps are running in the background—draining resources and leaking your data to online servers. For example, when the XAgent malware app installs on an Apple device with iOS version 7 or older, the app icon is hidden, and the app runs in the background. When you close the app, it restarts. The malware not only uses resources; it also steals personal data and makes screenshots, which it sends to a remote command-and-control (C&C) server.
- **Fake security warnings, unexpected app behavior, and strange text messages.** A C&C server might send coded text messages back to the phone. If you receive strange text messages, suspect malware. Fake security warnings can bait you into installing an app, which is actually more malware, to clean the system

- **Dropped phone calls or weak signal.** Dropped phone calls can be caused by a weak signal, which can be resolved by moving to a place where cellular coverage is stronger. However, dropped phone calls can also happen when malware is interfering and trying to eavesdrop on your conversations or is performing other background activities.
- **Unintended Wi-Fi and Bluetooth connections.** Malicious Wi-Fi hotspots and Bluetooth devices can hijack a device or inject it with malware. When a mobile device connects to a malicious Wi-Fi hotspot, the device can receive a malicious script that repeatedly reboots the device, which makes it unusable. To prevent this type of attack, avoid free Wi-Fi hotspots or use a VPN connection. To prevent a device from pairing with a malicious Bluetooth device, turn off Bluetooth when it's not in use.
- **Unauthorized account access or leaked personal files or data.** A malicious app can steal passwords and data from other apps and can pretend to be a different app to get access to online accounts. If you suspect an online account has been hacked, consider malware might be on the mobile device that uses this account.
- **Unauthorized use of camera or microphone.** Unauthorized surveillance is a sure sign of malware. Stalker spyware apps have been known to take photos and send them to a C&C server; send a text alert to a hacker and then add the hacker to a live call; use the microphone to record live conversations and then send the recording to a C&C server; report Facebook, and iMessage activity, including passwords and location data; and upload all photos, videos, and text messages to a C&C server.

**Note 11**

When is spyware legal? Parents can legally install spyware (politely called monitoring software) on a minor child's phone, tablet, or computer, and employers can monitor employee devices when they are company owned. One example of a spyware app is FlexiSPY (flexispy.com), an app that runs in the background to monitor text, email, Facebook and other visited websites, apps, photos, videos, contacts, bookmarks, location tracking, and phone calls. It can also record calls and surrounding sounds. It comes with a mobile viewer app installed on the parent's or employer's smartphone.

# 9-3c Mobile Device Malware Removal

**Core 1 Objective**

- 5.5

  Given a scenario, troubleshoot common issues with mobile devices.

Here are general steps for removing malware from a mobile device, listed from least to most invasive:

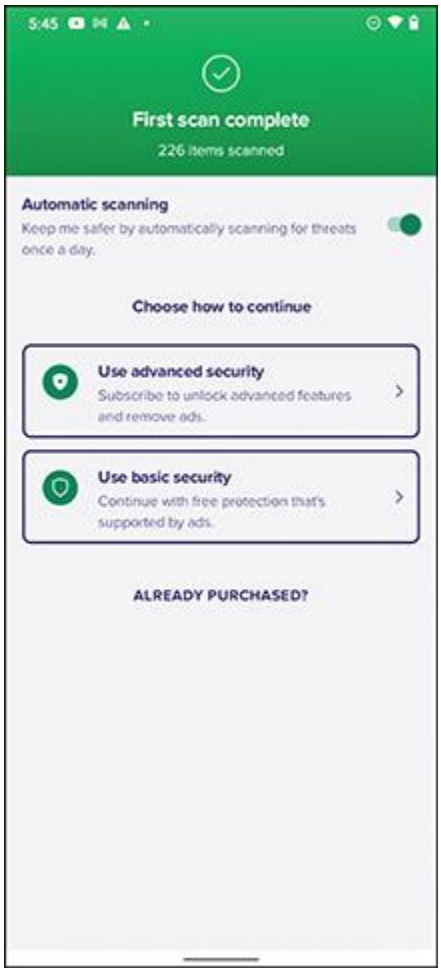
- **Uninstall the offending app.** If you can identify the malware app, close the app and uninstall it. If the app won't uninstall, force stop the app or any background processes that belong to the app. Then try again to uninstall the app.
- **Update the OS.** Check to see if any updates are available for the device.
- **Perform a factory reset.** The most surefire way to remove malware is to back up data and other content, reset the device to its factory default state, and then restore the content from backup. How to perform a factory reset is covered in the module "Mobile Device Security."

After you have removed malware on a mobile device, you will want to keep it clean. Here are a few tips:

- Keep OS updates current.
- Educate users about the importance of privacy settings (for example, disable cookies, and turn off Bluetooth when it's not in use). Also, users should not open email attachments or download shared files from untrusted sources.
- Consider installing an anti-malware app. Search online reviews, and consider the features offered before deciding on an anti-malware app. An anti-malware app, such as Avast shown in Figure 9-42, can scan apps and files for malware, scan for unauthorized surveillance, monitor security and privacy settings, find the device when it's lost, lock and remote wipe it, and maintain automatic updates. It might even include a firewall or a VPN feature.

**Figure 9-42**

Avast performs regular scans once a day on an Android device




Source: Avast

# 9-3dOther Common Problems and Solutions

## Core 1 Objective

- 5.5

Given a scenario, troubleshoot common issues with mobile devices.

Several common problems with mobile devices can be addressed with a little understanding of what may have gone wrong behind the scenes. Here's a description of how to handle some common problems:

### Display and Touchscreen Issues

Problems with the display and touchscreen might include the following:

- **Malfunctioning touch response.** Most smartphones today never need touch screen calibration, which is realigning the screen to touch. However, for Android, you can download and install the free Touchscreen Calibration app. There is no such app for an iPhone or

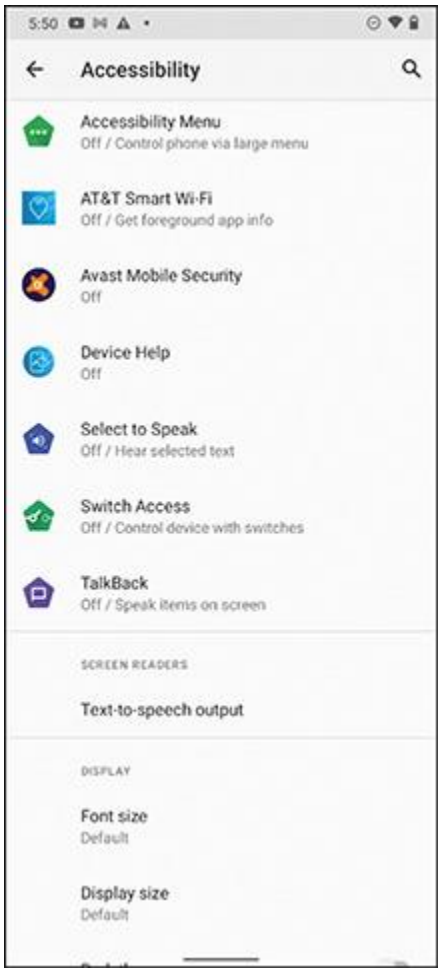
iPad. If you think calibration is needed on these devices, Apple recommends you first try rebooting the device. If that doesn't work, go to Settings, and reset all settings. The next step is to take the phone to an Apple service center for repair.

Here are some general tips to try when a touch screen is giving you problems:

- Clean the screen with a soft, lint-free cloth.
- Don't use the touch screen when your hands are wet or you are wearing gloves.
- Restart the device.
- Remove any plastic sheet or film protecting the touch screen. Some screen protectors are too thick and interfere with the touch screen interface. Bubbles and debris under the screen protector can also cause problems. Use a screen protector that is approved for your device, and carefully follow instructions for installing it. Turn on the screen protector's touch sensitivity setting if available.
- If you recently installed a third-party app when the touch screen became unresponsive, try uninstalling the app.
- Sometimes touch response and displays are affected by settings on the accessibility menu in the Settings app (for Android, see Figure 9-43).

**Figure 9-43**

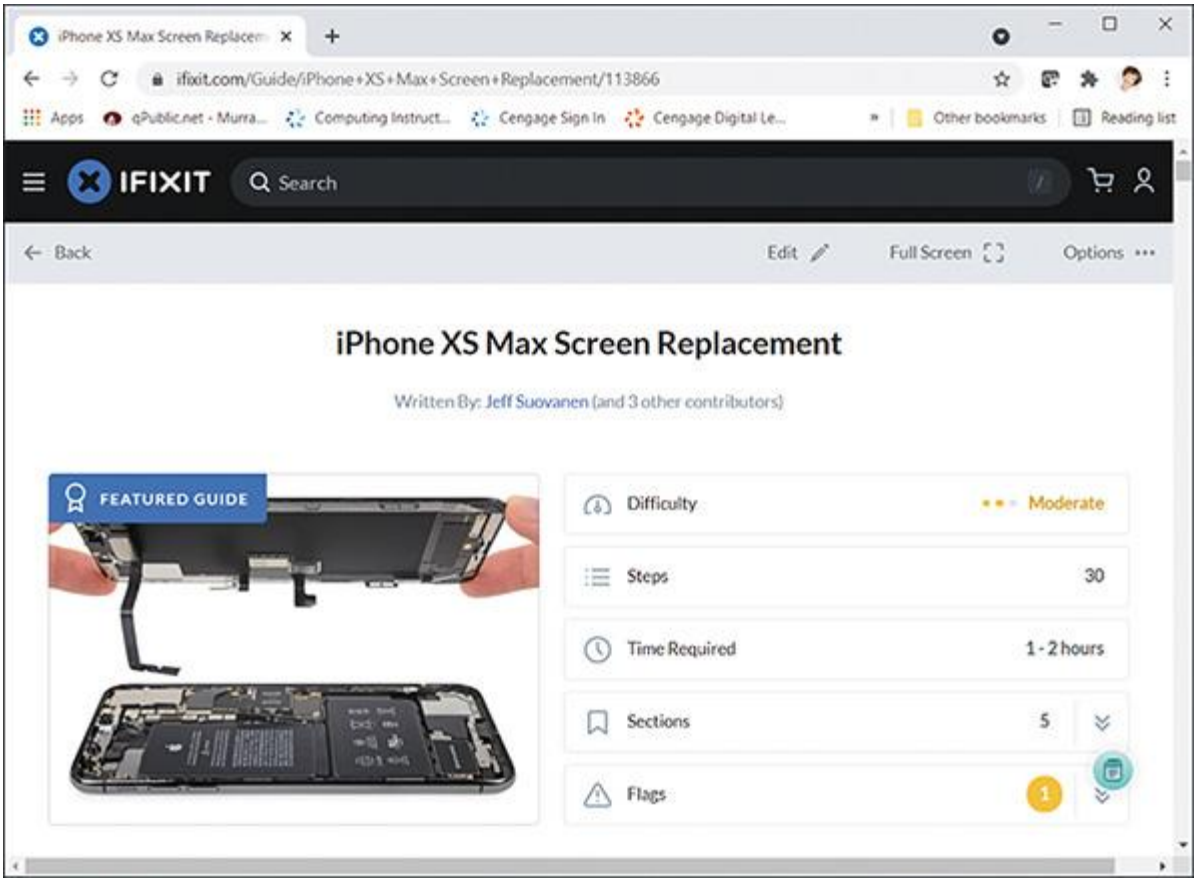
Accessibility settings can make a mobile device act in unexpected ways




- **Digitizer issues.** A mobile device screen contains three layers: a thin layer of glass, a digitizer, and the LCD screen that displays the graphical interface. The digitizer, also called a touch screen, is an electrical sheet just under the glass that turns a tap or swipe into digital data transmitted to the OS. The digitizer is often fused to the LCD component. When the digitizer stops working, touch does not work, and it's time to replace the digitizer. When you repair a device's screen, in most situations, you replace the entire screen—including the glass, digitizer, and LCD—as one component.
- **Broken screen.** If you can still use the device, first transfer all the data and settings to your computer or the cloud. How to do that is covered in the module "Mobile Device Security." If the device is under warranty, follow the warranty holder's directions for repairs or replacement. Alternately, you can take the device to a repair center or replace the screen yourself. For most mobile devices, you can find teardown instructions, videos, tools, and replacement parts for purchase online at various websites, such as ifixit.com (see Figure 9-44).

**Figure 9-44**

At ifixit.com, you can find instructions and purchase tools or parts to replace an iPhone screen




Source: ifixit.com

## Caution

Be sure to check out a cell phone repair (CPR) shop before you trust it with your device. Although there are many trustworthy businesses, some have been known to trade expensive parts inside a phone for cheap plastic ones while they perform a repair. In addition, the quality of the replacement components contributes to the success of the repair.

### Connectivity Issues

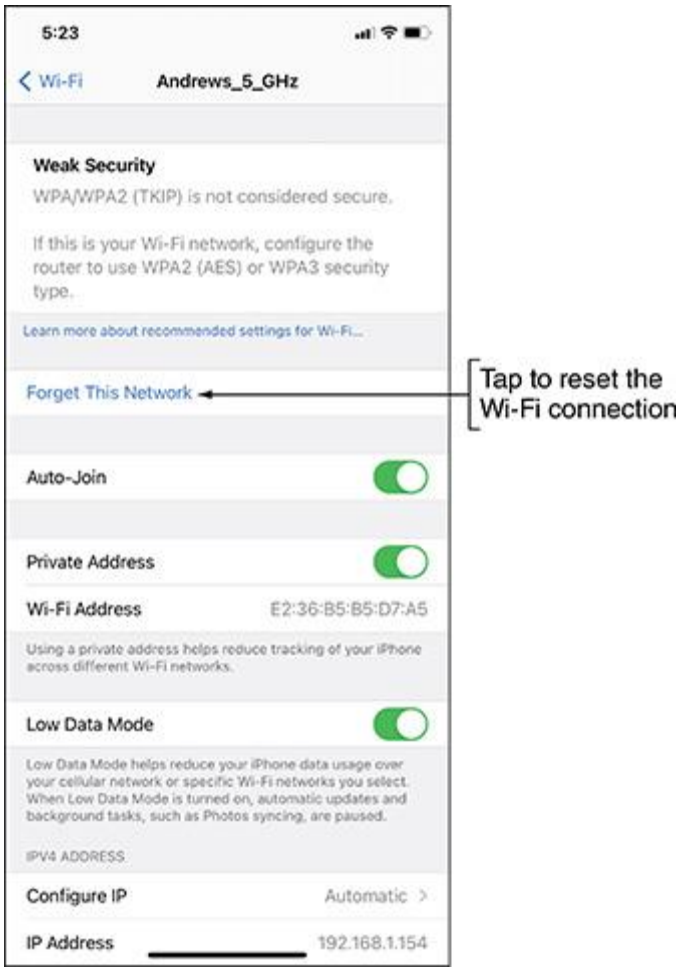
Bluetooth, Wi-Fi, NFC, and Apple AirDrop connections may experience connectivity issues, such as those described here:

- **Bluetooth connectivity issues.** Turn the Bluetooth radio off and then back on again. Devices typically limit the time they're available for pairing, so reactivating Bluetooth restarts the pairing process. In Bluetooth settings, you might be able to adjust the visibility timeout so devices have more time to discover each other. You can also delete all known Bluetooth devices in the Settings app to try the pairing process from the beginning. Sometimes an OS update will cause issues with Wi-Fi network connectivity or Bluetooth pairings. In this case, reset network settings in the Settings app. This restores network settings to factory defaults, and then you can attempt pairing again.

- **Wi-Fi connectivity problems.** Intermittent connectivity problems or no wireless connectivity might be caused by problems with the signal that is being broadcast from the router or access point. First make sure the access point and router are working correctly, that they're positioned closely enough to each other and the device, that the Wi-Fi network you want to connect to is visible to the device (not hidden), and that you're using the correct security key. For Wi-Fi issues on the device side, first start with Wi-Fi settings in the Settings app for the network to which you're trying to connect. Try renewing the IP address, and if that doesn't work, tell the device to forget the network (see Figure 9-45), and then retry connecting to the network. Finally, try resetting the network settings. By default, many mobile devices stop attempting to reconnect to a weak Wi-Fi signal to conserve battery power, but you can sometimes change this setting so the device will attempt to maintain a connection even with a weak signal.

## Figure 9-45

Forget the Wi-Fi network and try to connect again




- **Near-field communication (NFC) issues.** NFC range between devices should be less than eight inches. Verify the battery has at least a 75% charge and the OS is up to date. Try removing the device cover, which

might be hindering a good wireless connection. With Android, to resolve NFC issues, try updating the Google Pay app. If you are trying to pay using a manufacturer's pay app, such as Samsung Pay, try updating the app, erasing data in the app, forcing the app to close, and then reopening the app. If NFC issues began immediately after an OS update, try a hard boot, which usually fixes an NFC issue after an OS update. If problems persist, consider a factory reset and restore from backup.

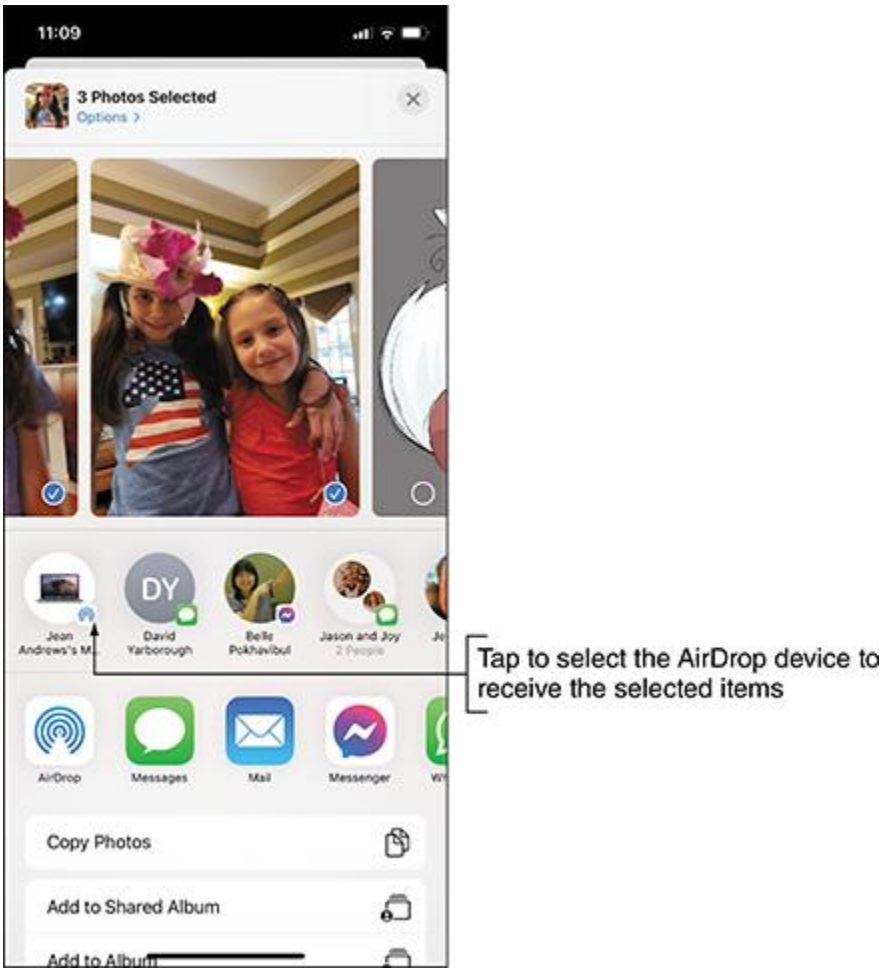
- **AirDrop connectivity issues.** AirDrop uses Bluetooth to find other Apple devices to connect with and then uses a peer-to-peer Wi-Fi connection to transmit files. Because of Bluetooth limits, the devices must be within a 30-foot range. For AirDrop to work, both Bluetooth and Wi-Fi radios must be turned on. To make the initial contact, both devices must be awake and AirDrop turned on and discoverable. To allow a Mac computer to be discovered by AirDrop, in the Finder window, select **AirDrop** in the left pane, and select an option in the right pane (see Figure 9-46). If you still have difficulty connecting, try turning AirDrop off and back on. To use the connection, select items to share, and then tap the share icon (see Figure 9-47).

## Figure 9-46

Allow the Mac computer to be discovered by other AirDrop devices


## Figure 9-47

Share selected items over AirDrop




## Damaged Ports and Liquid Damage

Physical damage to ports can include the following:

- **Physically damaged port.** Android devices might use a microUSB or USB-C port, and Apple devices use a Lightning port. Their connectors are shown earlier, in Figures 9-28 and 9-29. If a port is not working, try blowing out the port with compressed air. Dust or lint may be stuck in the port. Using a toothpick or needle to clean out a port is not recommended.
- **Water or other liquid damage.** When you connect a cable to an iPhone or iPad Lightning port and the device detects liquid in the port, it displays a Liquid Detected alert. Charging is not available, and accessories using the port won't connect. For any mobile device, don't use the port until it's completely dry. Tap your phone gently to shake out excess liquid. Put it in a dry place, in front of a cool fan. Wait at least 30 minutes before trying the port again. Don't use heat or compressed air to dry your device. For Android devices that are not under warranty, remove the battery to speed up drying.

**Note 12**

In an emergency, you might need to use or charge your phone even if it's wet. In this situation, Apple recommends you dismiss the Liquid Detected alert and try charging your phone

anyway or use a wireless charger. Although recommended on many websites, Apple says not to put your device in a bag of rice to dry it out.

## Battery, Overheating, and Charging Issues

Problems with the battery can include the following:

- **Improper charging.** A device charging slowly or not charging at all might be caused by a loose connection between the device and charging cable or electrical outlet, a damaged port the charger is used, or the electrical outlet. Do the simple things first: check the cable connections, and verify the electrical outlet is working. Try cleaning the port and exchanging the charging cable. Make sure the device is not overheating; when a device gets too hot, charging will stop. Try restarting and rebooting your device. Can you replace the battery?
- **Poor battery health.** Too many apps or malware running in the background will drain the battery quickly, as will Wi-Fi, Bluetooth, or other wireless technologies. Disable wireless connections and close apps when you're not using them to save battery juice. Consider that malware might be at work. If the battery charge still lasts an extremely short time, try exchanging the charging cable. If that doesn't work, exchange the battery unless the device is under warranty. Many Android devices have replaceable batteries, so if a battery is performing poorly, consider replacing it. Try searching the ifixit.com website on the device brand and model to see how complicated it is to replace the battery and the cost of a new battery.
- **Overheating or swollen battery.** For a true overheating problem where the device is too hot to touch safely, power off and replace the device. However, all devices can get fairly warm if the display is left on for too long, if the surrounding environment is particularly hot, if the device is sitting on a blanket or other soft surface, if the case is not properly vented, if the battery is going bad, or if the device remains plugged in to a power source for a long period of time. Don't use a mobile device for too long in direct sunlight, turn off the display when you're not using it, and close apps that you're not using. This will also help conserve battery power. Also, using the device as a mobile hotspot can stress the battery and cause it to overheat.

If you know where the battery is located inside a mobile device, check for heat originating from that area of the device. If the area is hot, replacing the battery might be your solution. First check if the phone is under warranty. If the phone is not under warranty, open the case, and examine the battery for damage. Is it swollen or warped? If so, replace the battery. If the phone is under warranty, do not open it. Instead, see if you can tell if the battery is swollen or warped by laying the phone on a flat surface. If the phone itself appears warped, take it in for repair.

**Note 13**

Some Android smartphones provide information about the device when you enter *#*#4636#*#* in the phone's dialer keypad. In the screen that appears, select Battery Information. If the Battery Health screen reports "unknown," suspect a bad battery. The screen also reports the temperature of the battery, which should be less than .

# 9-4a Module Summary

## Mobile Devices, Operating Systems, Connections, and Accessories

- An IT support technician might be called on to service mobile devices such as smartphones and tablets, and, therefore, needs to know the basics of using and supporting Android, iOS, and iPadOS mobile operating systems.
- A mobile device might have several antennas for wireless connections—primarily Wi-Fi, GPS, Bluetooth, NFC, and cellular. The device uses a Wi-Fi or cellular antenna to connect to a LAN (local area network), a WAN (wide area network), or to create its own hotspot, and it uses Bluetooth or NFC to connect to a PAN (personal area network). A wired connection might use a microUSB, miniUSB, USB-C, or proprietary port, such as the Lightning port by Apple, for syncing with a computer or tethering to provide the computer with cellular WAN access.

## Mobile Apps for Business Use

- Large corporations use mobile device management (MDM) software on mobile devices to secure and back up their content on the device. Mobile application management (MAM) software enhances MDM by providing additional protection for corporate apps and data.
- Email can be accessed on a mobile device through an email client embedded in the mobile OS or through third-party commercial mail apps. Microsoft Exchange is a private enterprise email service that is hosted on corporation or ISP servers.
- Syncing mirrors app data and other content among your devices and the cloud. Apple and Google both offer syncing that is linked to your Apple or Google account. In addition, Microsoft offers Microsoft 365 and OneDrive or SharePoint syncing as do other software and cloud providers.

## Troubleshooting Mobile Devices

- To troubleshoot a mobile device using tools in the OS, you can close running apps, uninstall and reinstall an app, update the OS, and restart and reboot the device.
- Common problems a technician might face when supporting mobile devices include malware, malfunctioning touch response, digitizer

issues, a broken screen, connectivity issues, damaged ports, liquid damage, improper charging, poor battery health, overheating, and a swollen battery.

## 9-4c Thinking Critically

These questions are designed to prepare you for the critical thinking required for the A+ exams and may use information from other modules and the web.

1. Which of these network connections would allow your smartphone to sync your photos to your online account? (Choose all that apply.)

    1. Wi-Fi
    2. Bluetooth
    3. GPS
    4. Cellular

2. While visiting a coffee shop, you see a poster advertising a concert for a music group you'd love to see. You notice there's an NFC tag at the bottom with additional information about the concert. Which of the following devices would likely be able to read the NFC tag?

    1. GPS
    2. Smartphone
    3. eReader
    4. Laptop

3. You work for a company that provides the same smartphone model for dozens of its employees. While troubleshooting one smartphone that won't connect to the cellular network, you call the provider's tech support number for some assistance. The technician asks for the device's IMEI. What is she trying to determine?

    1. The OS version on the phone
    2. The specific device you're calling about
    3. The SIM card installed in the device
    4. The IP address of the phone on the cellular provider's data network

4. You're at the store to buy a car charger for your dad's iPhone. There are several options, with many different types of connectors. Which of these connectors should you choose?

    1. USB-C
    2. microUSB
    3. Lightning
    4. VGA

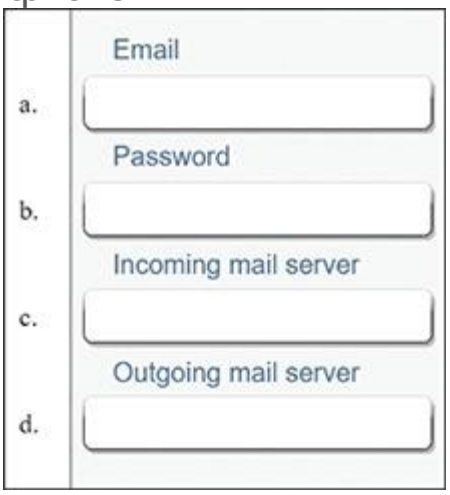
5. Place the following information in the correct fields in Figure 9-48 to add an email account to a smartphone using port 143 for the incoming mail server and port 25 for the outgoing mail server (not all information will be used):

    - imap-mail.sample.com

- p@ssw0rd
- pop-mail.sample.com
- mjones@sample.com
- smtp-mail.sample.com
- Mary Jones

**Figure 9-48**

Configure email for a smartphone




6. Congratulations! You just bought a new-to-you car, and it comes with a media system that can sync with your iPhone. You're concerned about data usage on your cell phone, so before you go pick up your car, you decide to download the necessary app at home while you're connected to Wi-Fi. What app do you need to download?
7. You're traveling across the country for a much-anticipated vacation. When you get there, your smartphone seems to be having trouble connecting to the local cellular network. You call the provider, and the technician suggests you update the PRL. Why might this help? Where would you find this option on your Android smartphone to perform the update?
8. You're trying to cast a video presentation from your tablet to a projector for a training session with some new hires. Although you tested it successfully yesterday, today the connection is not cooperating. You've closed apps you're not using, and you've checked that the projector and the tablet are working otherwise. Of the following troubleshooting steps, which should you try first? Second?

    1. Restart the projector.
    2. Restart the tablet.
    3. Reinstall the presentation app.
    4. Verify that you have Internet access on the tablet.

9. Suppose you and your friend want to exchange lecture notes taken during class. She has an iPhone, and you have an iPad. What is the easiest way to do the exchange?

    1. Copy the files to an SD card and move the SD card to each device.
    2. Drop the files in OneDrive and share notebooks with each other.
    3. Send a text to each other with the files attached.
    4. Transfer the files through an AirDrop connection.

10. Jorge has asked you to explain to him how a touch pen can work with his Android tablet. Which of the following are true statements about touch pens? (Choose all that apply.)

1. A touch pen might use a Bluetooth connection to write on a tablet.
2. A touch pen is made of material that can touch the screen without damaging it.
3. A touch pen might need charging.
4. A touch pen does not use a Wi-Fi connection.

11. Android and iOS both offer a quick swipe to get to some basic settings such as those that allow you to turn on Bluetooth and adjust brightness. What are these tools called?

1. Android Notifications and iOS Control Center
2. Android Settings app and iOS Notifications
3. Android Control Center and iOS Notifications
4. Android Notifications and iOS Notifications

12. You are asked to help change some settings on an older smartphone. When you examine the phone, you find it doesn't have a slot for a SIM card. What type of technology can you confidently say this phone is not using? (Choose all that apply.)

1. 4G
2. 5G
3. CDMA with 3G
4. GSM with 3G

13. In an enterprise, when an employee is allowed to use their smartphone for business, which software is used to verify the smartphone satisfies the security requirements needs to protect enterprise data on the device?

1. Microsoft Exchange
2. VPN
3. MDM
4. ActiveSync

14. Dyane asks for your help to understand why her corporate email is not working as she expects on her tablet. The tablet has no cellular capability, but she connects to Wi-Fi when at work and at home. When she's at a customer site and needs to find a particular email about the customer, she finds that email is not available. What can you tell Dyane about the situation?

1. Most likely, the email app is corrupted, and she needs to uninstall and install it again.
2. Corporate policies don't allow email to be stored on her device.
3. ActiveSync is enabled.
4. She needs to download all her email while she's connected to Wi-Fi.

15. A friend calls to tell you they have just dropped their iPhone in water. They ask you what to do. What advice can you give your friend? (Choose all that apply.)

1. Take the phone out of the case and dry off the surface.
2. Place the phone in a bag of rice so the rice can absorb the moisture.
3. Use a hair dryer set to medium heat to dry the phone.

4. Set the phone in front of a cool fan.

# 9-4d Hands-On Projects

## Hands-On Project 9-1

### Selecting a Mobile Device

- **Est. Time:** 15 minutes
- **Core 1 Objective:** 1.3

Shop for a new smartphone or tablet. Be sure to read some reviews about a device you are considering. Select two devices that you might consider buying, and answer the following questions:

1. What is the device brand, model, and price?
2. What is the OS and version? Amount of storage space? Screen size? Types of network connections? Battery life? Camera pixels?
3. What do you like about each device? Which would you choose and why?

## Hands-On Project 9-2

### Exploring ifixit.com for Cost of Repair

- **Est. Time:** 15 minutes
- **Core 1 Objective:** 5.5

A friend just dropped their iPhone 11 Pro and broke the screen. They have asked you to help them decide how much they should pay for the repair and if you are willing to do it. Do the following:

1. 1
   Search the ifixit.com website, which is a wiki-based site with tons of guides for tearing down, repairing, and reassembling all kinds of products, including smartphones, tablets, and laptops. Locate the directions for an iPhone 11 Pro screen replacement. and browse through the instructions.

2. 2
   How much would the parts for the repair cost if they are purchased at ifixit.com?

3. 3
   How much would the tools to do the repair cost if they are purchased at ifixit.com?

4. 4
   What is the cost of a refurbished iPhone 11 Pro sold on other sites?

5. 5
   What advice should you give your friend? Is it better to buy a replacement phone or have the broken phone repaired? If you were willing to do the repair, how much would you charge for the labor?

## Hands-On Project 9-3

## Syncing to the Cloud

- **Est. Time:** 15 minutes
- **Core 1 Objective:** 1.4

Using an Android smartphone or tablet, do the following to manage data syncing on an Android device:

1. 1
   On your computer, go to google.com and sign in using your Google account. Browse through photos, contacts, and your calendar. Which of this content is currently syncing with your Android device?
2. 2
   To manage what is synced, on your Android device, open the **Settings** app, tap **Google**, and tap **Settings for Google apps**. Set Google contacts for syncing.
3. 3
   Open your **Calendar** app, and verify calendars are syncing.
4. 4
   Make an entry in your calendar for a meeting tomorrow.
5. 5
   On your computer, go to Google Calendar. Did the meeting sync to your Google calendar?
6. 6
   Make an entry in the calendar.
7. 7
   On your Android device, verify the event showed up on your Android Calendar.

For an Apple device, do the following:

1. 1
   On your computer, go to icloud.com, and sign in using your Apple account. Browse through your mail, contacts, photos, notes, and iCloud Drive. What content is currently syncing with your Apple device?
2. 2
   To manage what syncs to iCloud, on your iPhone or iPad, open the **Settings** app, tap your account name, and tap **iCloud**. Turn on the items you want to sync. Make sure Notes is syncing.
3. 3
   On your device, type an entry into Notes.
4. 4
   On your computer, go to icloud.com. Did your entry in Notes sync to the cloud?

5. 5
   Make an entry in Notes.

6. 6
   Return to your Apple device. Did the entry show up in your Notes app?

## Hands-On Project 9-4

### Syncing Android Files to Google Drive

- **Est. Time:** 15 minutes
- **Core 1 Objective:** 1.4

Sometimes an Android user might want to sync data files between an Android device and Google Drive. To set up a two-way sync, you can use the Autosync for Google Drive third-party app. You'll need an Android device to do this project:

1. 1
   If you don't already have a Google account, go to google.com and create one. It's free and comes with 15 GB free storage. Create a folder in Google Drive to sync with your Android device. What did you name the folder?

2. 2
   If the Autosync for Google Drive app is not already installed on your Android device, download and install it.

3. 3
   Open the **Autosync** app where you set up the folder pair to sync. Set the app to sync your Pictures folder with the folder you created on Google Drive. Enable two-way syncing. Take a photo on your device.

4. 4
   Sign in to Google Drive. Did the photo appear on your Google Drive? Copy a photo from your computer to the Google Drive folder.

5. 5
   Check your Android device. Is the file on your device? The sync might take a few moments. If you don't want to wait, open the **Autosync** app, go to **SYNCED FOLDERS**, tap the three-dots menu beside the synced folder, and tap **Sync now**.

# 9-4e Real Problems, Real Solutions

## Real Problem 9-1

### Configuring Email on a Mobile Device

- **Est. Time:** 15 minutes
- **Core 1 Objective:** 1.4

For this project, use an Android device and an email account that you have not already set up on the device. If you don't already have an email account you can use, you can create a free one using mail.google.com, outlook.live.com, or mail.yahoo.com.

Follow these steps to manually configure the email client on an Android device:

1. 1
   Open the **Gmail** app. If an email address is already set up, tap the account profile photo, and tap **Add another account**. If this is the first email setup, tap **Add an email address**. Gmail can automatically configure email from many providers. Because it's essential that you know how to manually configure email on a mobile device, tap **Other**.

2. 2
   Add your email address and tap **MANUAL SETUP**. Check with your email provider to determine whether to use POP3 or IMAP. What is the main difference between these two protocols? What are the ports for these two protocols? What are the secure ports for these protocols?

3. 3
   Enter the password and click **NEXT**. On the Incoming server settings screen, verify the incoming server name, and, for POP3, decide when you want to delete mail on the server, and click **NEXT**. If the OS needs more direction for security settings, you might need to tell it which security protocol the email provider uses. Options are STARTTLS, SSL/TLS, and None.

4. 4
   Verify the outgoing server name and security settings, and tap **NEXT**.

5. 5
   Set your account options as desired, then tap **NEXT**.

6. 6
   If you were successful, you'll get a notice confirming your account is set up. Set the account name and your name as desired; then tap **NEXT**. If you weren't successful, backtrack and troubleshoot to solve the problem.

7. 7
   When you're finished, send an email to a classmate, and check an email sent from someone else to confirm your email account is working on your smartphone.

8. 8
   You need to know how to change the settings on an account. What steps are required to change the server settings for the account you just added?

9. 9
   You should also know how to remove an email account from a mobile device. What steps are required to remove the email account you just added?

## Real Problem 9-2

### Exporting and Importing Contacts

- **Est. Time:** 30 minutes
- **Core 1 Objective:** 1.4
- **Note:** This problem works well as a group problem where at least one person in the group has an Apple device and another person in the group has an Android device. If you or a group member doesn't have access to an iPhone or iPad, Apple account, Android device, and Google account, list the basic steps to take rather than actually doing the work.

Jamal has just purchased a new Android phone and has asked for your help to import his contacts from his old iPhone to his new Android. If necessary, research how to help Jamal, and then do the following:

1. Export three contacts on your iPhone or iPad, using a single export operation.
2. Import these contacts to an Android device.

Answer the following questions:

1. What is the file extension of your exported file? What does the three-character file extension stand for?
2. Use Notepad to examine the contents of the export file. In the file, what marks the beginning and end of the data for one contact?
3. List the steps you took to export and import the contacts.

Conversely, suppose someone asks how to export contacts from an Android to an Apple device. Answer the following questions:

1. Which file types can Google use to export contacts?
2. Which file type would you use if you were exporting to an Apple device?