Chapter 1

Mobile Devices

COMPTIA A+ CERTIFICATION EXAM CORE 1 (220-1101) OBJECTIVES COVERED IN THIS CHAPTER:

✓ **1.1 Given a scenario, install and configure laptop hardware and components.**

- Hardware/device replacement
- Physical privacy and security components

✓ **1.2 Compare and contrast the display components of mobile devices.**

- Organic light-emitting diode (OLED)
- Mobile display components
- WIFI antenna connector/placement
- Camera/webcam
- Microphone
- Touch screen/digitizer
- Inverter

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

- Connection methods
- Accessories
- Docking station
- Port replicator
- Trackpad/drawing pad

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

- Wireless/cellular data network (enable/disable)
- Bluetooth

- Location services
- Mobile device management (MDM)/mobile application management (MAM)
- Mobile device synchronization

This chapter will focus on the exam topics related to mobile devices. It will follow the structure of the CompTIA A+ 220-1101 exam blueprint, objective 1, and cover the four subobjectives that you will need to master before taking the exam. The Mobile Devices domain represents 15 percent of the total exam.

1.1 Given a scenario, install and configure laptop hardware and components

Whether you choose to call them laptops, notebooks, tablets, or something different is mostly a matter of semantics. In this section, I'll discuss some of the basic components of laptops and their installation (when possible and called for). In many cases, the components are the same as in a desktop computer.

The following topics are addressed in exam objective 1.1:

- Hardware/device replacement
- Physical privacy and security components

Hardware/device replacement

Replacing hardware and devices in a laptop can be a challenge because of the size limitations. The best way to determine the proper disassembly method is to consult the documentation from the manufacturer.

Many laptop manufacturers will consider a warranty void if an unauthorized person opens a laptop case and attempts to repair it.

Some models of notebook PCs require a special T-8 Torx screwdriver. Most PC toolkits come with a T-8 bit for a screwdriver with interchangeable bits, but you may find that the T-8 screws are countersunk in deep holes so that you can't fit the screwdriver into them. In such cases, you need to buy a separate T-8 screwdriver, available at most hardware stores or auto parts stores.

Prepare a clean, well-lit, flat work surface; assemble your tools and manuals; and ensure that you have the correct parts. Shut down the PC, unplug it, and detach any external devices such as an external keyboard, mouse, or monitor. In this section, with these general guidelines for opening the laptop in mind, you'll look at replacing various components of a laptop. Always ensure that you have grounded yourself before working with computer components of any kind. Use an antistatic wristband and attach it to the case.

Battery

Replacing the battery in a laptop is simply a matter of removing the battery storage bay, removing the old battery from the bay, inserting the new battery into the bay, and replacing the bay. Determining the battery type for the replacement will probably take longer than the replacement procedure. In fact, many users carry extra batteries for situations where they know they will need to use the laptop for longer than the battery life (such as a long plane trip) and change the battery as needed.

If BitLocker encryption is enabled, the laptop will not boot after a battery replacement unless the BitLocker encryption key is provided.

Keyboard/keys

When replacing the keyboard, one of the main things you want to keep in mind is *not* to damage the data cable connector to the system board.

1. With the laptop fully powered off and unplugged from the wall, remove the battery. Examine the screws on the back of the laptop. Ideally, icons indicating which screws are attached to the keyboard will be available. If not, look up the model online and determine which of the screws are attached to the keyboard.
2. Remove the screws with a T-8 or Phillips-head screwdriver. With the laptop turned back over, open it. If the keyboard is tucked under any plastic pieces, determine whether those pieces need to have screws removed to get them out of the way; if so, remove the screws and the plastic pieces. In some cases, there may just be clamps that are easily removed.
3. With any plastic covers out of the way, remove any screws at the top and remove the keyboard itself from top to bottom. There should be a thin, but wide, data cable to the system board at the bottom. This is the piece to be careful with!
4. Take a pick and lift the plastic connectors that hold this data cable in place. Remove the data cable. Take the new keyboard and slip the data cable back in between the plastic connectors on the system board. Ensure it's all the way in.
5. Put the plastic connector back into place and make sure it's holding the data cable in. Position the keyboard into place and refasten the keyboard in place at the top, replacing any screws that were there before.
6. Replace any plastic pieces that were covering the keyboard, turn the laptop over, and replace all of the keyboard screws. When you replace the battery and turn it on, check the functionality. If the keyboard doesn't work, the main component to check is the data connector.

Random-access memory (RAM)

There should be a panel used for access to the memory modules. If the panels are not marked (many are not), refer to your laptop instruction manuals to locate the panel on the bottom.

1. Remove any screws holding the panel in place, remove the panel from the laptop, and set it aside. If removing an existing memory module, remove it by undoing the module clamps, gently lifting the edge of the module to a 45-degree angle, and then pulling the module out of the slot.
2. Align the notch of the new module with that of the memory slot and gently insert the module into the slot at a 45-degree angle. With all pins in the slot, gently rotate the module down flat until the clamps lock the module into place.
3. Replace the memory access panel, replace any screws, and power up the system. When the computer is powered back up, it may be necessary to go into the computer BIOS to let the system properly detect the new RAM that has been installed in the computer. Please refer to the user manual for the computer system for any additional information.

HDD/SSD replacement

Before changing a hard drive, you should back up the old hard drive if the data is needed. Then, to change the hard drive, follow these steps:

1. Turn the laptop upside down and look for a removable panel or a hard drive release mechanism. Laptop drives are usually accessible from the bottom or side of the chassis. Release the drive by flicking a lock/unlock button and/or removing a screw that holds the drive in place.
2. You may be required to remove the drive from a caddy or detach mounting rails from its sides. Attach the rails or caddy to the new drive using the same screws and washers. If required, remove the connector attached to the old drive's signal pins and attach it to the new drive. Make sure it's right side up and do not force it. Damaging the signal pins may render the drive useless.
3. Reverse your steps to place the drive (and caddy if present) into the case. Replace the screws and start the laptop. The system should recognize the drive. If you or the user created a bootable backup disc or a complete image disc (before the drive failed, by the way), place it in the optical drive and follow the instructions for restoring the data.

SSD drives

Although many devices still use a magnetic disk hard drive, most laptop vendors are moving to using either solid-state drives or hybrid drives, which are a combination of magnetic disk and solid-state technology.

The advantage of solid-state drives is that they are not as susceptible to damage if the device is dropped, and they are generally faster because no moving parts are involved. They are, however, more expensive, and when they fail, they don't typically display any advanced warning symptoms like a magnetic drive will do.

Hybrid storage products have a magnetic disk and some solid-state memory. These drives monitor the data being read from the hard drive, and they cache the most frequently accessed bits to the high-speed flash memory. These drives tend to cost slightly more than traditional hard drives (but far less than solid-state drives), but the addition of the SSD memory for cached bits creates a surprising improvement in performance. This improvement will not appear initially because the drive must "learn" the most frequently accessed data on the drive.

1.8 in vs. 2.5 in

The 2.5-inch hard drives are small (which makes them attractive for a laptop, where space is at a minimum), but in comparison to 3.5-inch hard drives, they have less capacity and cache, and they operate at a lower speed.

Moreover, whereas 2.5-inch drives operate from 5,400 to 7,200 rpm, 3.5-inch drives can operate from 7,200 to 10,000 rpm. However, 2.5-inch drives use about half the power (again, good for a laptop) of a 3.5-inch drive (2.5 W rather than 5 W).

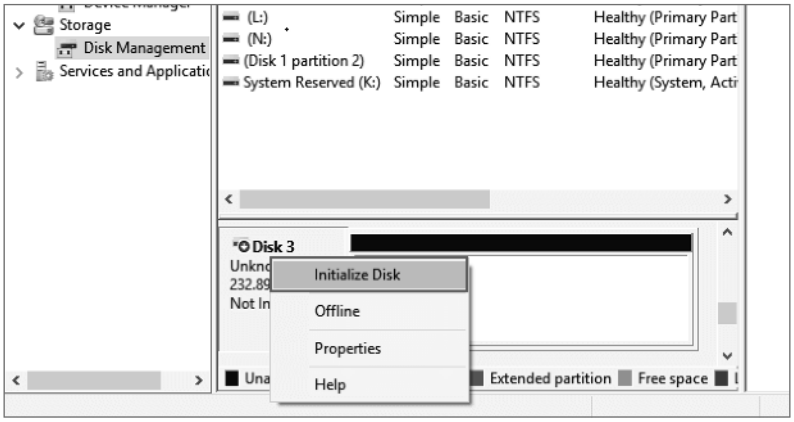
The 1.8-inch drive is the smallest of the three I'm discussing here. It was originally used in subnotebooks and audio players. It has the least capacity of the three, with the largest up to 320 GB. It has only two platters, each of which can hold 220 GB maximum.

Hard disk drive (HDD)/solid-state drive (SSD) migration

When you have made the decision migrate data from hard disk drives (HDD) to solid-state drives (SDD), the process may be easier than you think.

1. First, ensure both drives are connected to the motherboard. Make sure both the power cable and the data cable are in place.
2. In Windows, open Disk Management, select the SSD drive, and then select Initialize Disk, as shown in Figure 1.1 (this assumes the HDD has already been initialized to the local system).

FIGURE 1.1 Initialize Disk



3. Select Control Panel ➢ System And Security ➢ Backup And Restore (Windows 7).
4. Click **Create A System Image** in the left pane. On the **Do You Want To Save Backup** page, from the **On A Hard Disk** drop-down list, choose the SSD drive. After selecting the destination disk or volume, click Next.
5. Make sure both System Reserved (System) and (C:) (System) drives (assuming C: is where the operating system is) are selected. Select any other drives that may hold data as well. Click Next. Confirm the backup settings and click Start Backup.

Wireless cards

Both 802.11 and Bluetooth wireless cards that are built in can be replaced if they go bad. Sometimes they reside near the memory, so you would open the same panel that holds the memory. In other cases (such as a Dell Inspiron), you have to remove the memory, keyboard, optical drive, and hand rest to get to it. The Bluetooth card may be located in the same place, or it may be located at the edge of the laptop with its own small panel to remove. Consult your documentation.

Once you've found either type of wireless card, disconnect the two antenna contacts from the card. Do not pull by the wire; pull by the connector itself. Remove any screws from the wireless card and gently pull out the card from the slot. Insert the replacement card into the slot at a 45-degree angle, replace the screws, and reconnect the antenna to the adapter. Replace the parts you were required to remove to get to the card, reversing your steps carefully.

Cellular card

Changing an external mobile broadband card is as simple as pulling the old USB stick out and plugging in the new one. Because USB is plug and play, you shouldn't have to do anything, but even in the case of an issue the manufacturer usually provides a CD with the drivers or you can obtain them from the vendor website. Changing an internal card is much like the process of changing an internal 802.11 card; follow the instructions indicated in the previous section.

Mini PCIe

Since many of the wireless cards are mini-PCIe, replacing any other card in this format will follow the same procedure, with the exception of removing and reconnecting the antenna cables (present only on the wireless cards). You can find the location of the card in the documentation. Make sure that the new card is firmly inserted into the slot after removing the old card.

Physical privacy and security components

Some features are designed to enhance the privacy of the data on a device and of the transmission of said data by enhancing physical security. In the following section, you'll learn about two concepts that help to provide additional security in this regard.

Biometrics

Most mobile devices now offer the option to incorporate biometrics as an authentication mechanism. The two most common implementations of this use fingerprint scans or facial scans or facial recognition technology. While there can be issues with both false negatives (the denial of a legitimate user) and false positives (the admission of an illegitimate user), they offer much better security than other authentication mechanisms.

A good example is a fingerprint lock that uses the fingerprint of the user as credentials to authenticate the user and, when successful authentication completes, unlocks the screen. Because it relies on biometrics, it is for the most part more secure than using a passcode or a swipe.

To set up fingerprint authentication in Windows 10, follow these steps:

1. Select Start ➢ Settings to open the Settings app.
2. Select Accounts ➢ Sign-in Options page. In the right pane, find the Fingerprint section under Windows Hello and click the Set Up button.
3. On the Welcome screen, click the Get Started button to continue.
4. Authenticate yourself with a PIN or a password to continue.
5. Scan your finger on the fingerprint sensor multiple times. As you scan your finger, you will see a fingerprint animation filling. When you see the All Set screen, you are done.

Near-field scanner features

A near-field scanner allows you to measure and map the EMI that may be leaking from a system or its cables, creating a physical security issue. While these devices are used for much more than detecting EMI, they can be used for that purpose. They can be used to analyze potential circuit designs for flaws as well. These devices are typically handheld.

Exam essentials

List the steps to install or replace laptop components. This includes but is not limited to keyboards, hard drives, optical drives, wireless cards, mini-PCIe cards, and batteries,

List the steps to configure biometrics. This includes features that depend on biometrics such as the fingerprint authentication in Windows 10.

1.2 Compare and contrast the display components of mobile devices

The display of a laptop contains more components than you may expect. In this section, I'll discuss these components and, in some cases, cover competing technologies. The following topics are addressed in exam objective 1.2:

- Types
- Mobile display components
- WIFI antenna connector/placement
- Camera/webcam
- Microphone
- Touch screen/digitizer
- Inverter

Types

Laptop displays can use any of several technologies: LCD, LED, or OLED. This section provides a quick survey of these display types and their characteristics as they apply to laptops.

Liquid crystal display (LCD)

LCDs have completely replaced CRTs as the default display type for both laptops and desktops. Two major types of LCDs are used today: active matrix screens and passive matrix screens. Their main differences lie in the quality of the image. Both types use some kind of lighting behind the LCD panel to make the screen easier to view. One or more small fluorescent tubes are used to backlight the screen.

Passive Matrix A passive matrix screen uses a row of transistors across the top of the screen and a column of them down the side. It sends pulses to each pixel at the intersection of each row and column combination, telling it what to display. Passive matrix displays are becoming obsolete because they're less bright and have poorer refresh rates and image quality than active matrix displays. However, they use less power than active matrix displays.

Active Matrix An active-matrix screen uses a separate transistor for each individual pixel in the display, resulting in higher refresh rates and brighter display quality. These screens use more power, however, because of the increased number of transistors that must be powered. Almost all notebook PCs today use active matrix. A variant called thin-film transistor (TFT) uses multiple transistors per pixel, resulting in even better display quality.

In-plane switching (IPS)

There are two major LCD technologies used in LCDs. In-plane switching (IPS) is a newer technology that solves the issue of poor quality at angles other than straight on. It also provides better color quality. However, it has much slower response time and is more expensive. Newer versions like Super-IPS (SIPS) make improvements on the response time.

Twisted nematic (TN)

Twisted nematic (TN) is the older of the two major technologies for flat-panel displays. While it provides the shortest response time, has high brightness, and draws less power than

competing technologies, it suffers from poor quality when viewed from wide angles. It suffers color distortions when viewed from above or from the sides.

Fluorescent vs. LED backlighting

LCDs can use two kinds of backlighting: LED-based and fluorescent. Fluorescent is an older technology and consists of a fluorescent tube connected to a voltage inverter board that provides power to the backlight. LED-based is a newer technology and uses a matrix of LEDs for the backlighting. Table 1.1 compares the two technologies.

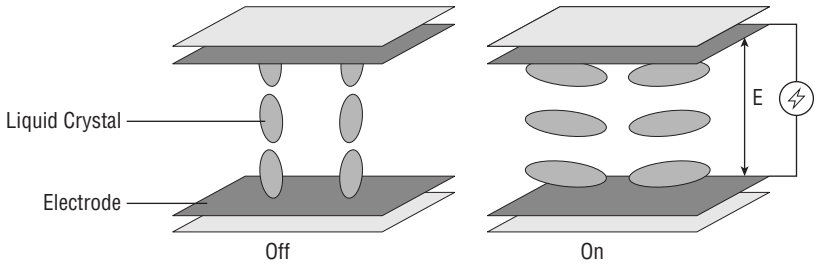
TABLE 1.1 Fluorescent and LED

Characteristic	Fluorescent	LED
Size	Thicker and heavier	Thinner and lighter
Cost	Cheaper	More expensive
Power	High power consumption and heat generation	Lower power consumption and heat generation
Brightness	Lower	Higher
Lifespan	Shorter	Longer

Vertical alignment (VA)

A third type is an LED that uses vertical alignment (VA). In VA, when no electric current is running through the liquid crystal cells, the cells naturally align vertically between two substrate panes of glass, which block the transmission of light from the backlight. This renders the crystals opaque and results in a black display screen. When an electric current is applied, the liquid crystal cells shift to a horizontal position between the substrates, allowing light to pass through and resulting in a white display screen. Monitors with VA LCD panels provide the advantages of wide viewing angles and high-contrast ratios and reproduce colors well. The operation of VA is shown in Figure 1.2

FIGURE 1.2 Vertical alignment



Organic light-emitting diode (OLED)

An organic light-emitting diode (OLED) is another type of LED technology. It uses an emissive electroluminescent layer of organic compounds that emit light in response to an electric current. An interesting characteristic of these displays is their flexibility and transparency. This means they can roll up for storage (like a mat), and you can see through the display to objects behind the display. These displays are now available but quite expensive.

Mobile display components

The display of a laptop contains more components than you may expect. In this section, I'll discuss these components.

WIFI antenna connector/placement

The wireless antenna is located in the display. You may recall that when replacing a laptop screen, you encountered a number of wires coming from the screen to the laptop body. One of these is the cable that connects the wireless antenna (located in the display) with the wireless card located in the body of the laptop.

The antennas built into the display usually work quite well. In any specific situation, you may improve your signal by moving the laptop around. This changes the polarization of the antenna and may cause it to line up better to the incoming signal.

Camera/webcam

Many displays today, especially laptop displays, have a webcam built in. They come ready to go with all drivers preinstalled and nothing to configure or set up. If you need to replace the webcam, you will have to disconnect the laptop lid (which holds the display) from the base, remove the screw covers and screws holding the display bezel in place, and remove the bezel. After removing the screws holding the mounting rails to the hinges, remove the LED screen from the lid assembly. Now you can get at the camera, but first carefully remove the tape that holds the camera cable in place and remove it and the camera. Attach the replacement cable to the new camera, install the new camera, and reverse these steps.

Microphone

While many desktop systems lack a built-in microphone, almost all laptops have one. In some cases, this microphone will be located on the laptop bottom, but in many cases, it will be in the display next to the webcam or off to the side. If you need to replace it, you will need to take the same steps to get inside the display that you took for the webcam.

When you unhook the lid from the bottom, you will need to unplug several things from the board, and one of those will be the microphone cable. If the microphone is not working (which it probably isn't or you wouldn't be replacing it), take a moment to inspect the cable. Sometimes the cable can be cut by the constant opening and closing of the case (it shouldn't, but sometimes it does happen). You may be able to repair the cable without replacing the microphone.

If that is not the case, remove the microphone and cable and replace both with the new mic and cable. Reverse the steps to get into the display, reconnect the cables to the board, and put the back on the bottom.

Touch screen/digitizer

Digitizers read pressure applied to the surface of the display and are what make touchscreens work. In some cases, they work with a stylus or small pen-like device; in others, you simply touch the screen with your finger. The digitizer is a thin piece of clear material that fits on top of the display. It has its own cable just as the display itself does. If it gets cracked, which often happens, it can be replaced without replacing the display itself. Typically, when you perform this replacement, you will have to open the display lid, as I covered earlier, and separate the digitizer from the display. It is usually glued to the display, and you can use a hair dryer to heat the glue to make removing it easier. When you put the new digitizer in, you may need to reheat the glue on the display to stick them back together.

Inverter

An inverter is a component that takes DC power and converts it to an AC form that can be used by the LCD screen. It is implemented as a circuit board that is located behind the LCD. If problems with flickering display or dimness occur, the inverter is a prime suspect. If the inverter needs to be replaced, you should be aware that it may contain stored energy, so it may need to be discharged to be safe.

Exam essentials

Differentiate the types of displays available in laptops. Two major types of LCDs are used today: active matrix screens and passive matrix screens.

Describe the location and operational characteristics of the wireless antenna in a laptop. The wireless antenna is located in the display. Moving the laptop changes the polarity of the antenna and may result in a better signal.

Identify the location and function of the inverter. An inverter is a component that takes DC power and converts it to a form that can be used by the LCD screen. It is implemented as a circuit board behind the LCD.

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

Mobile devices can come with a variety of interfaces or ports to which various types of peripherals can be connected. The following topics are addressed in exam objective 1.3:

- Connection methods
- Accessories
- Docking station
- Port replicator
- Trackpad/drawing pad

Connection methods

Many connection methods have come and gone with respect to external ports on devices. In this section you'll learn about the most common ones found in today's mobile devices.

Universal Serial Bus (USB)/USB-C/microUSB/miniUSB

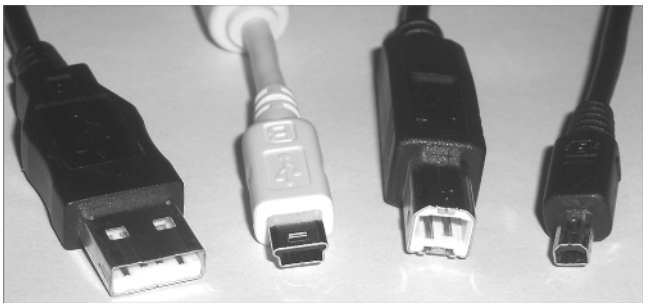
USB is an expansion bus type that is used almost exclusively for external devices. All motherboards today have at least two USB ports. Some of the advantages of USB include hot-plugging and the capability for up to 127 USB devices to share a single set of system resources. A USB port requires only one IRQ (short for interrupt request, an IRQ is a signal sent to the computer processor to stop [interrupt] it momentarily) for all USB devices that are connected to it, regardless of the type or number of devices.

Connector types: A, B, mini, micro

USB connectors come in two types and two form factors or sizes. The type A connector is what is found on USB hubs, on host controllers (cards that are plugged into slots to provide USB connections), and on the front and back panels of computers. Type B is the type of USB connector found on the end of the cable that plugs into the devices.

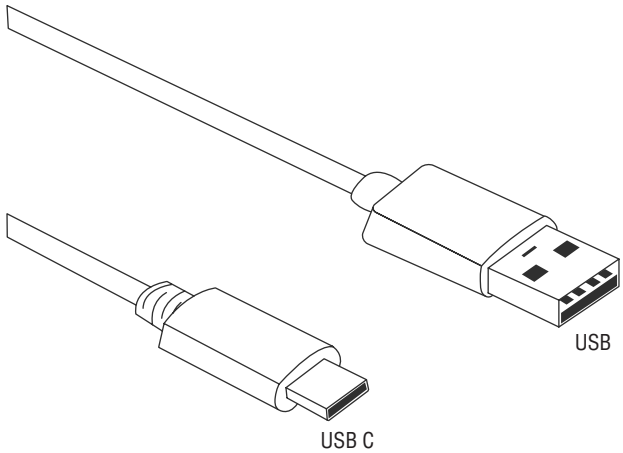
The connectors also come in a mini version and a micro version. The micro version is used on mobile devices, such as mobile phones, GPS units, and digital cameras, whereas the mini is found in applications described in the previous paragraph. The choice between a standard A and B and a mini A and B will be dictated by what is present on the device. The cables used cannot exceed 5 meters in length. Figure 1.3 shows, from left to right, a standard Type A, a mini Type A, a standard Type B, and a mini Type B. Some manufacturers have chosen to implement a mini connector that is proprietary, choosing not to follow the standard.

FIGURE 1.3 USB connectors



USB-C The USB-C connectors connect to both hosts and devices, replacing various USB-B and USB-A connectors and cables with a standard. This type is distinguished by its twofold rotationally symmetrical connector. The cable is shown in Figure 1.4 next to USB 3.0 cable.

FIGURE 1.4 USB C and USB



USB 2.0/3.0 USB 1.1 runs at 12 Mbps and USB 2.0 runs at 480 Mbps. USB 3.0 has transmission speeds of up to 5 Gbps, significantly reduces the time required for data transmission, reduces power consumption, and is backward-compatible with USB 2.0. Because USB is a serial interface, its width is 1 bit. It is useful to note, however, that a USB 2.0 device will perform at 2.0 speeds even when connected to a 3.0 port. If you connect a USB 3.0 to a USB 2.0 port, it will also only operate at 2.0 speeds

By utilizing USB hubs in conjunction with the USB ports available on the local machine, you can connect up to 127 of these devices to the computer. You can daisy-chain up to four external USB hubs to a USB port. Daisy chaining means that hubs are attached to each other in a line. A USB hub will not function if it is more than four hubs away from the root port.

Lightning

Apple uses what it calls the Lightning connector for power. Although it makes an adapter to convert this connector to mini-USB (see the next section), Apple doesn't encourage its use because of the limitations the adapter places on the functionality of the proprietary connector.

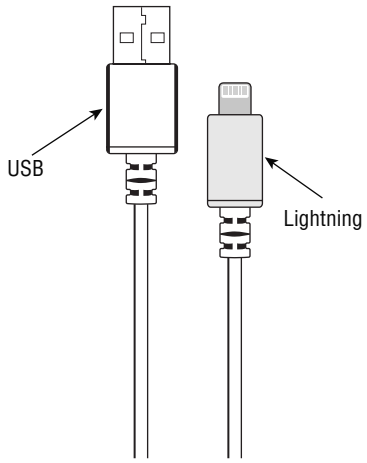
This is an eight-pin connector that while not standard has advantages over USB, according to Apple. It operates at USB 3.0 speeds of 640 MB. The following are some of these advantages:

- It can supply more power.
- It can be inserted either way.

- It is physically more durable than USB.
- It can detect and adapt to connected devices.

Figure 1.5 shows a Lightning connector next to a USB cable.

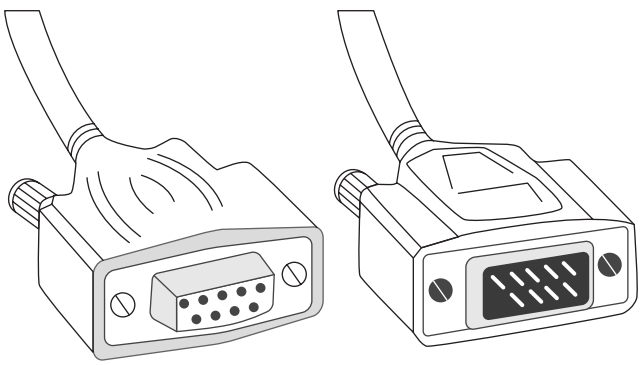
FIGURE 1.5 Lightning connector and USB



Serial interfaces

Although an older cable type, a serial connector may be found connecting some peripherals to the serial connection on the system. This connector is shown in Figure 1.6. The maximum speed is 115,200 bps.

FIGURE 1.6 Serial connector

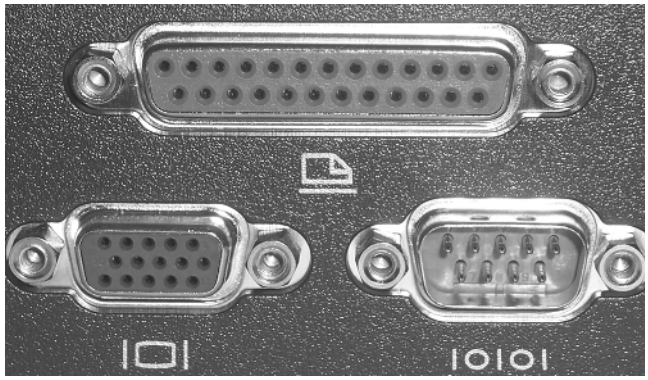


RS-232

The RS-232 standard had been commonly used in computer serial ports. A serial cable (and port) uses only one wire to carry data in each direction; all the rest are wires for signaling and traffic control.

Common bit rates include 1,200; 2,400; 4,800; 9,600; 14,400; 19,200; 38,400; 57,600; and 115,200 bits per second. The connector used for serial is a D-shaped connector with a metal ring around a set of pins. These are named for the number of pins/holes used: DB-25, DB-9, HD-15 (also known as DB-15), and so on. Figure 1.7 shows DB-25, DB-15, and DB-9.

FIGURE 1.7 DB-25, DB-15, and DB-9 ports



Near-field communication (NFC)

Near-field communication (NFC) is a wireless technology that allows smartphones and other equipped devices to communicate when very near one another or when touching. NFC operates at slower speeds than Bluetooth but consumes far less power and doesn't require pairing. It also does not create a personal area network (PAN) like Bluetooth; rather, the connections are point-to-point. NFC can operate up to 20 cm at a transfer rate of 0.424 Mbps.

NFC is also a standard managed by the ISO and uses tags that are embedded in the devices. NFC components include an initiator and a target; the initiator actively generates an RF field that can power a passive target. This enables NFC targets to take simple form factors such as tags, stickers, key fobs, or cards that do not require batteries.

You may have noticed these small devices in retail outlets. They communicate wirelessly with NFC cards and smartphones. In some cases, it requires tapping the phone on the device, and in other cases that is not required. These devices connect either using USB or in some rare cases a serial connection. Consult the documentation to determine whether you need a special driver installed.

The technology was first used in radio frequency ID (RFID) tagging and was implemented on mobile devices first as a way to share short-range information and later as a method to make payments at a point of sale. It operates by reading tags, which are small

microchips with antennas that can in some cases only be read and other cases can be read and written to.

A mobile device must have the support for NFC built in, and many already do. Special applications are available that make it easy to use the technology in various ways.

- Making point-of-sale payments
- Reading information stored in tags in posters and advertisements
- Communication between toys used in gaming
- Communication with peripherals

Bluetooth

Mobile devices also support Bluetooth wireless connections. Bluetooth is a technology that can connect a printer to a computer at a short range; its absolute maximum range is 100 meters (330 feet), and most devices are specified to work within 10 meters (33 feet). When printing with a Bluetooth-enabled device and a Bluetooth-enabled printer, all you need to do is get within range of the device (that is, move closer), select the print driver from the device, and choose Print. The information is transmitted wirelessly through the air using radio waves and is received by the device. Bluetooth speed depends on version. Table 1.2 shows this for the latest versions.

TABLE 1.2 Bluetooth speeds

Version	Speed
2.0	2.1 MB
2.1	2.1 MB
3.0	24 MB (over Wi-Fi connection)
4.0	2.1 MB over Bluetooth and 24 MB over Wi-Fi
4.1	2.1 MB over Bluetooth and 24 MB over Wi-Fi
4.2	2.1 MB over Bluetooth and 24 MB over Wi-Fi
5.0	2.1 MB over Bluetooth and 24 MB over Wi-Fi

Hotspot

Another way that many mobile devices can connect to other devices is through a hotspot or when tethered to another device. Many mobile devices can act as 802.11 hotspots for other wireless devices in the area. There are also devices dedicated solely to performing as mobile hotspots.

Hotspots are publicly provided points of access to an 802.11 wireless network connected to the Internet. They typically have little or no security configured to make it as easy as possible for users to connect. Vendors have also created devices that allow a single device to act as a hotspot for other devices in the area. Sometimes these are called mobile hotspots. Some mobile devices can be turned into mobile hotspots with a software upgrade or an addition to the service plan.

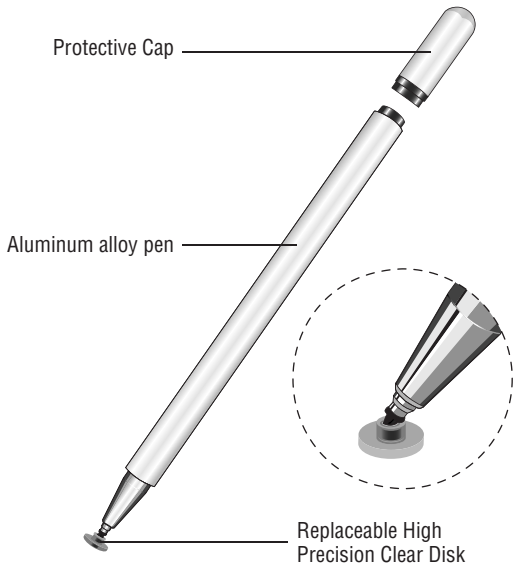
Accessories

Mobile devices require a lot of accessories to take advantage of many of the features they provide. While many of these are also commonly used with desktop and laptop devices, some are much more likely to be used with mobile devices. In this section, you'll take a brief look at the types of accessories you may find attached to a mobile device.

Touch pens

While there is a specific product called the Touch Pen, in many cases this is a synonym for the stylus that comes with a touchscreen system. An example of a stylus or touch pen is shown in Figure 1.8

FIGURE 1.8 Touch pen or stylus



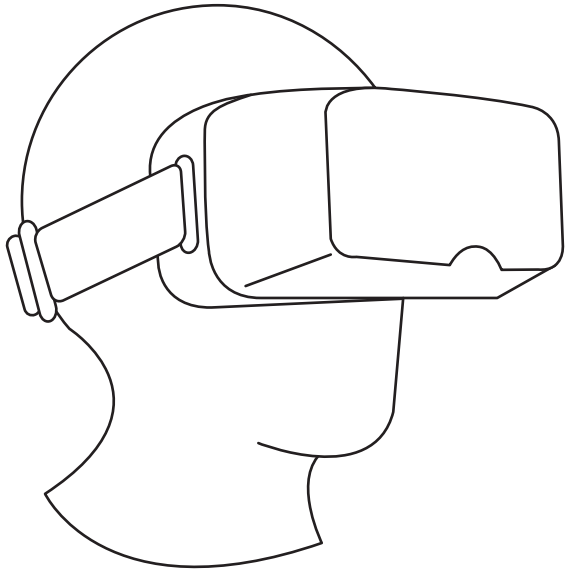
Headsets

Headsets provide the ability to take your conversation offline or to listen to your music in private. They can be connected both through a wired connection, usually a 3.55 mm audio connector or USB, and by using Bluetooth to pair the device with the headset.

VR/AR headsets

Extended reality is an exciting new field that includes both augmented reality and virtual reality. Both concepts involve wearing special headsets that deliver the visual experience. While reality immerses the user into a virtual environment, much like a four-dimensional game, augmented reality involves glasses that, while permitting a clear vison of the real world, can project graphics and text onto this view using a small side screen. A virtual reality headset is shown in Figure 1.9.

FIGURE 1.9 VR headset



VR headsets are widely used with computer games, but they are also used in other applications, including simulators and trainers. They are worn on the head and cover the eyes with stereo sound and head motion tracking sensors. Most connect to either the USB or HDMI connector, although some are wireless. Several additional types are shown in Figure 1.10.

By now, everyone has heard about and probably seen Google Glass, the most well-known and recognizable computing device worn as glasses. Just in case you haven't, Figure 1.11 shows a drawing of the glasses. This is no longer commercially available as a retail product

FIGURE 1.10 Different types of VR headsets

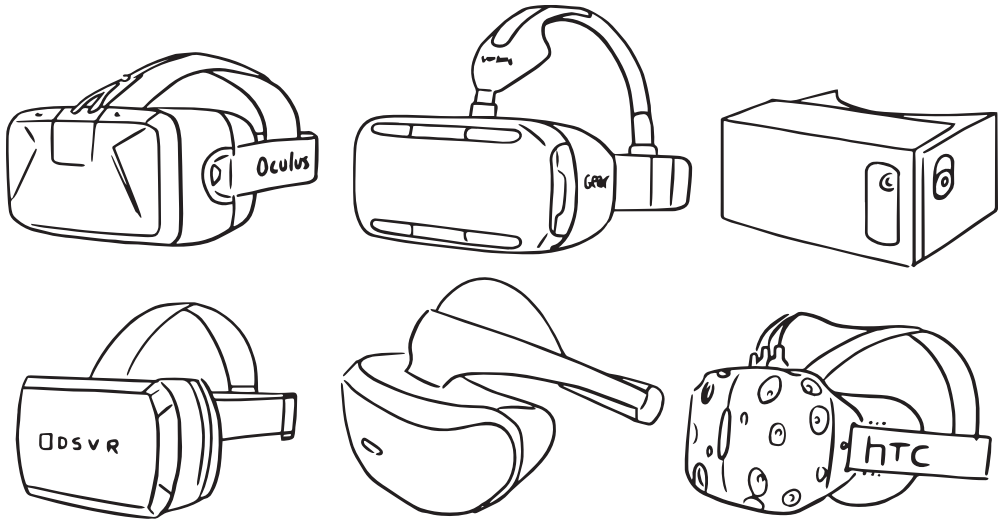
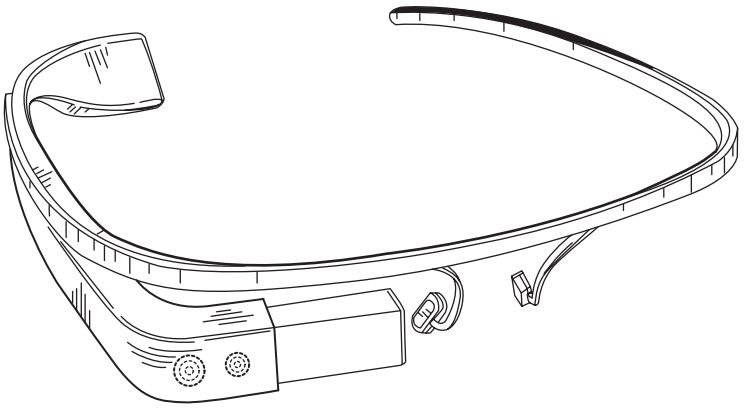


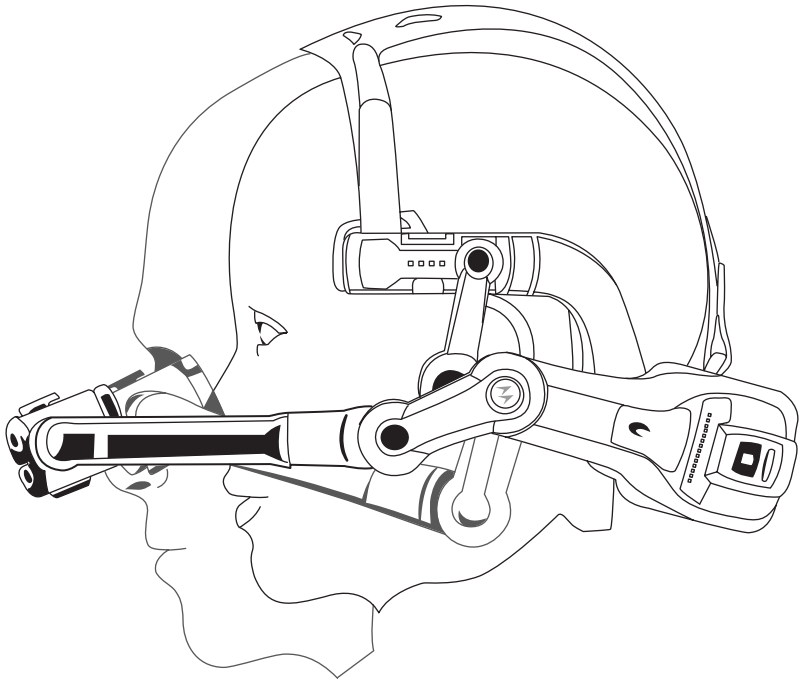
FIGURE 1.11 Google Glass



While worn as glasses, they also have a small screen just to the side of one of the eyes that houses the computer screen (think Cyborg). The user can view the screen at any time by just casting a glance at it. Many promising uses have been proposed for the devices, with a number in the healthcare field. Although sale of the devices to individuals was halted, sales to organizations that have or are working to find ways to use the glasses continue.

Another similar device that is not based on glasses but around a headset format is the HC1 headset computer by Zebra. It can respond to voice commands and body movements. One of these is shown in Figure 1.12.

FIGURE 1.12 Headset computer



Speakers

Speakers are used in the same fashion as headsets. They can also be connected using the same options that include using USB, using a 3.55 mm audio plug, or by pairing the speakers with the devices using Bluetooth. This includes the speaker systems in many cars, which can now be paired with the devices using Bluetooth as well.

Volume settings

On the top row where the keys labeled F1–F12 are located, there are usually a couple of keys (typically F8 and F9) with icons that look like speakers. These keys can be used to raise and lower the volume of the sound. If the icon is blue, you have to hold down the Fn key. Otherwise, you do not need to use the Fn key to activate them. (As a matter of fact, if you hold down the Fn key and use the F8 key, you may be changing the location of the display output. If these keys are not present, consult the documentation for the key to use in conjunction with Fn to lower and raise the volume. Most laptops also include a mute button marked as such.

Installation

Installing speakers is more a matter of connecting them properly than installing them. Usually, one of the speakers will connect to a power source, and the other will connect to the

powered speaker. Once they are connected to a power source, connect the speaker cable to the proper plug in the PC. These plugs will be marked with icons that indicate which is for a microphone and which is for speakers.

Replacement

To replace speakers, first follow the earlier instructions to remove the hard drive, the battery pack, and all the screws holding the body together.

1. Lift the screen up and separate it from the body. Do not remove the wires connecting the screen to the motherboard.
2. Separate the two pieces of plastic body frame to view the inside of the laptop. Locate the speakers, using the documentation if necessary.
3. Unscrew the speakers and note where they connect to the motherboard. Disconnect the old speakers, and connect the new ones to the same location as where the old speakers were removed.
4. Replace all the parts in the reverse order you removed them.

No sound from speakers

When a speaker on a mobile device is not functioning, in most cases it has simply been inadvertently turned off. After checking the settings described later in this section, you can assume that there is a hardware problem. In that case, with smartphones, it is typically advisable to send the device to the manufacturer, but with laptops, it is possible to replace the internal speakers.

To determine whether the settings are the issue, ensure that the speaker volume is up and the speaker is not disabled. On an Android, first test the loudspeaker by following these steps:

1. Go to the Home screen and tap the Phone icon.
2. Type ***#7353#** into the dialer as though you are dialing a phone number. A list of options will appear.
3. Tap Speaker, and music should start to play. You can tap Speaker again to silence the music.

To test the internal speaker, follow the same steps, but in step 3, tap Melody. Music should start to play from the earpiece on the phone and allow you to see whether the speaker that you hold up to your ear to talk with people is working properly as well.

On an iPhone, follow these steps:

1. Go to Settings ➢ Sounds and drag the Ringer And Alerts slider to turn the volume up.
2. If you can hear sound from the speaker, then the speaker works.
3. If the device has a Ring/Silent switch, make sure it's set to ring. If you can see orange, it's set to silent.

Voice-enabled, smart speaker/digital assistant

Smart speakers that fulfill your commands are an extension of the digital assistants found in many operating systems today. Alexa, Cortana, and other digital assistants are installed in the speaker. Installing one of these is usually just a matter of turning it on and going through some prompts to enter the wireless network's SSID and password. Then you're up and running.

Webcam

Earlier in this chapter you learned about webcams. Digital cameras usually connect to the PC with a USB cable. In many cases, the operating system comes with software that may detect the camera and assist you in accessing the pictures and moving them to the computer. In other instances, you may want to install software that came with the camera. Doing so will often allow you to take fuller advantage of the features the camera offers. SD cards can be used to transfer images from the camera if a cable is not available.

Docking station

Some notebook PCs have optional accessories called docking stations or port replicators. They let you quickly connect/disconnect with external peripherals and may also provide extra ports that the notebook PC doesn't normally have.

A docking station essentially allows a laptop computer to be converted to a desktop computer. When plugged into a docking station, the laptop has access to things it doesn't have stand-alone—the network, a workgroup printer, and so on. The cheapest form of docking station (if it can be called that) is a port replicator. Typically, you slide a laptop into the port replicator, and the laptop can then use a full-sized monitor, keyboard (rather than the standard 84 keys on a laptop), mouse, and so on. Extended, or enhanced, replicators add other ports not found on the laptop, such as PC slots, sound, and more. The most common difference between port replicators and docking stations is that port replicators duplicate the ports the laptop already has to outside devices, and the docking station expands the laptop to include other ports and devices that the laptop does not natively have.

Laptops can support plug and play at three levels, depending on how dynamically they're able to adapt to changes.

Cold Docking The laptop must be turned off and back on for the change to be recognized.

Warm Docking The laptop must be put in and out of suspended mode for the change to be recognized.

Hot Docking The change can be made and is recognized while running normal operations.

Each docking station works a little differently, but there is usually a button you can press to undock the notebook from the unit. There may also be a manual release lever in case you

need to undock when the button is unresponsive. Moreover, the docking station must be purchased from the same vendor you purchased the laptop from because docking stations are vendor-and model-specific.

Port replicator

Port replicators are a form of docking station and were discussed in the previous section.

Trackpad/drawing pad

An *optical trackpad* is an input device based on an optical sensor, which detects the movement of a finger that is moving on top of it. The sensor is used typically in smartphones where it replaces the D-pad. The main advantages over a D-pad are:

- It can track movements in 360 degrees and with varying speeds.
- It uses space efficiently, without the need for small buttons that are difficult to press.

A *drawing pad* is a computer input device that enables a user to hand-draw images, with a special pen-like stylus.

Exam essentials

Describe the various connection methods. These include Universal Serial Bus (USB), Lightning, serial interfaces, near-field communication (NFC), Bluetooth, and through a hotspot.

Differentiate various mobile device accessories. Understand the use of touch pens, headsets, speakers, webcams, docking stations, port replicators, and trackpads/drawing pads.

Differentiate between docking stations and port replicators. A docking station essentially allows a laptop computer to be converted to a desktop computer. Extended, or enhanced, replicators add other ports not found on the laptop, such as PC slots, sound, and more. The most common difference between port replicators and docking stations is whether the peripheral provides network access and expands the laptop's capabilities.

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

For mobile devices to deliver the functionality that most expect, they must be connected to a network. To use email (one of the most important functions to many users), the device must be set up properly. The subobjectives covered in this section include the following:

- Wireless/cellular data network (enable/disable)
- Bluetooth

- Location services
- Mobile device management (MDM)/mobile application management (MAM)
- Mobile device synchronization

Wireless/cellular data network (enable/disable)

Like most computing devices, mobile devices provide more robust functionality when connected to a network (especially if that network is the Internet). Two types of networks can be used to gain access to the Internet: cell phone networks and Wi-Fi networks.

Cell phone networks have in the past been the second choice because the performance is not as good as an 802.11 Wi-Fi connection. With the introduction of 4G Long-Term Evolution (LTE) technologies, however, the performance delivered by the cell network may become more competitive. The latest standard is 5G and promises better performance.

In either case, most mobile devices will have the ability to make an 802.11 connection or use the cell network. If you want to disable the automatic connection to the cell phone network or if it was somehow turned off and needs to be turned back on, you can do this through the settings. One example of the steps to access these settings is Settings ➢ Wireless ➢ Mobile ➢ Enable Data (select or deselect this). This is only one navigational example, and you should consult the documentation that came with the device.

Making a Wi-Fi connection is much like doing so with a laptop. In the settings of the device will be a section for Wi-Fi (in iPhone it's called Wi-Fi, and in Android it's called Wireless And Networks). When you access it, you will see all the Wi-Fi networks within range. Just as you would do with a laptop, select one and attempt to connect to the Wi-Fi network. If the connection requires a password, you will have to supply it. You also can preconfigure a wireless profile for commonly used secure wireless networks as well as those where the service set identifier (SSID) has been hidden.

2G/3G/4G/5G

Cell phone technology has come a long way from its beginnings. There have been four major milestones of data speed and connection resilience. Let's take a look.

2G

2G is also called second-generation cellular. It uses the Global System for Mobile Communications (GSM), a standard developed by the European Telecommunications Standards Institute (ETSI). Three primary benefits of 2G networks over their predecessors were:

- Digitally encrypted phone conversations between the mobile phone and the cellular base station
- More efficient use of the radio frequency spectrum supporting more users
- Data services starting with SMS text messages

3G

Third generation, or 3G, introduced web browsing, email, video downloading, picture sharing, and other smartphone technologies. 3G should be capable of handling around 2 Mbps.

4G

Fourth generation, or 4G, is a later cellular technology that specifies 100 Mbps and up to 1 Gbps to pass as 4G. Outside of the covered areas, 4G phones regress to the 3G standards.

LTE

Long-Term Evolution (LTE) is based on the Global System for Mobile Communications/ Enhanced Data rates for GSM Evolution (GSM/EDGE) and Universal Mobile.

5G

With speeds of up to 100 gigabits per second, 5G is as much as 1,000 times faster than 4G and will provide greater network stability to ensure that business-critical mobile functions do not go offline and have the speed necessary to give employees a fully equipped virtual office almost anywhere. Verizon, Art and T and T-Mobile currently offer 5G broadband Internet in most big cities.

Hotspot

When the devices using the Internet connection on the cellular device are connected wirelessly using 802.11, it is sometimes called a mobile hotspot. This is also the term used for devices that can act as a hotspot for surrounding WiFi devices. The mobile hotspot device may get its Internet access through either cellular or 802.11. To enable connection to a hotspot, follow these steps:

- Click the WiFi icon in the system tray.
- The hotspot will show up as a wireless connection.
- Select it, and enter the password.
- Click Connect.

Global System for Mobile Communications (GSM) vs. code-division multiple access (CDMA)

Mobile devices have made cellular networking popular, though they are not the only devices capable of using networking; for example, a cellular modem can also be quickly added to a laptop. Cellular networks use a central access point (a cell tower) in a mesh network design. For a long time, two competing standards were the Global System for Mobile Communications (GSM) and code-division multiple access (CDMA); the latest technology is 5G, discussed earlier.

The basic difference between GSM and CDMA is that GSM is specific to a SIM card that is used with the mobile phone. On the other hand, the CDMA is handset specific. GSM uses time division multiple access (TDMA) and frequency division multiple access (FDMA). In TDMA multiuser access is provided by slicing the channel into different time slices. In FDMA multiple user access is made possible by separating the frequencies in the channel. As GSM is used and accepted worldwide, there is no problem of roaming in GSM mobile phones.

The technology used in CDMA is code-division multiplexing (CDM). In CDM multiple users in a channel are separated by the code they use to send the signal. Because CDMA is not used or accepted worldwide, it has limited roaming accessibility.

Preferred Roaming List (PRL) updates

The Preferred Roaming List (PRL) is a list of radio frequencies residing in the memory of some kinds of digital phones. It lists frequencies the phone can use in various geographic areas. Each area is ordered by the bands the phone should try to use first. Therefore, it's a priority list for which towers the phone should use. When roaming, the PRL may instruct the phone to use the network with the best roaming rate for the carrier, rather than the one with the strongest signal at the moment. As carrier networks change, an updated PRL may be required.

The baseband is the chip that controls all radio functions. An update makes the code in the chip current.

All mobile devices may require one or more of these updates at some point. In many cases, these updates will happen automatically, or "over the air." In other cases, you may be required to disable WiFi and enable data for these to occur.

PRL updates

In Android phones, the location of the PRL update option will differ, but you'll generally find it in one of a few places in the Settings menu.

- Settings ➢ System Updates ➢ Update PRL
- Settings ➢ Sprint System Updates ➢ Update PRL
- Settings ➢ About Phone ➢ Update PRL

In iOS, there is no separate PRL update command on iOS devices, but running a software update will force an update of the PRL.

Bluetooth

Bluetooth is a short-range wireless technology that is used to create a wireless connection between digital devices. One of its applications is to create connections between mobile devices and items such as speakers, headphones, external GPS units, and keyboards. Before you can take advantage of this technology, the devices must be configured to connect to one another. This section will discuss how to configure a Bluetooth connection.

Enable Bluetooth

On Android mobile devices, follow these steps:

1. From the Home screen, select the Menu button. From the menu, choose Settings ➢ Connections ➢ Bluetooth.
2. Once Bluetooth is selected, wait until a check mark appears next to Bluetooth. Bluetooth is now enabled.

On iOS mobile devices, follow these steps:

1. On the main page, choose Settings ➢ Bluetooth.
2. Tap the slider to enable Bluetooth.

Enable pairing

Pairing a mobile device with an external device (speaker, headphone, and so forth) will enable the two devices to communicate. The first step is to enable pairing. This is much simpler than it sounds. For either mobile operating system, simply turn the external device on, and you are ready for the next step. In some cases, you may need to make the external device discoverable. Check the documentation for the external device to see whether this is the case and how you do this.

Find a device for pairing

Now that the external device is on and transmitting a signal, the mobile device is ready for pairing.

On an Android mobile device, follow these steps:

1. Swipe up on an empty spot on the Home screen to open the Apps tray.
2. Select Settings and then Connections.
3. Turn on the Bluetooth switch by tapping it.
4. If the mobile device stops scanning before the Bluetooth device is ready, tap Scan again.
5. In the list of available devices, tap the Bluetooth device to pair it with the phone.
6. Follow any on-screen instructions.
7. If a password is required, consult the documentation or try either **0000** or **1234** (common passcodes).

On an iOS mobile device, when Bluetooth is enabled, it automatically starts scanning for Bluetooth devices. When your device appears in the list, select it. If a PIN is required, move on to the next step.

Enter the appropriate pin code

Many external devices will ask for a PIN when you select the external device from the list of discovered devices. In many cases, the PIN is 0000, but you should check the manual for the external device.

Test connectivity

Once the previous steps are complete, test communication between the two devices. If you're using a headset, turn on some sound and see whether you can hear it in the headphones.

No Bluetooth connectivity

Bluetooth is also enabled and disabled with a key combination and can be disabled easily. The first thing to try is to reenable it. The second thing to try is to reseat the antenna cable. If all else fails, try a new antenna. This can also be a hardware switch on the side, front, or back of the case.

In smartphones and laptops, the problem also can occur after an upgrade or update of some sort. In these cases, it can be that the proper driver is missing from the upgrade or was somehow corrupted or overwritten during the upgrade process. Here are some additional things you might try on a smartphone:

1. Power-cycle the device.
2. Remove the battery and put it back in.
3. Clear the Bluetooth cache. While each device is different, a common way to access this setting and clear the cache on Android is to open the phone's Settings, tap the More tab, tap Application Manager, select to view all, select Bluetooth Share, and tap Clear Cache.
4. Clear the Bluetooth data. While each device is different, a common way to access this setting and clear the data is to go to Settings, tap the More tab, tap Application Manager, select to view all, select Bluetooth Share, and select Clear Data.
5. Reboot the device in safe mode.
6. Make sure the device to which you are pairing has no issues.
7. As a last resort, perform a hard reset, which resets the device to factory defaults.

Unintended Bluetooth pairing

Unintended Bluetooth connections or pairings can also occur with mobile devices. This is also a security issue because several wireless attacks are made through a Bluetooth connection. Many users leave their Bluetooth settings in a state that makes connections to their peripheral devices easier to make. However, leaving them in a discoverable state also makes it easier for malicious individuals to create a Bluetooth pairing with your mobile device that makes wireless attacks through the Bluetooth connection possible.

Even though it adds a step to the process of pairing a new device to the mobile device, users should make their mobile devices undiscoverable as a default setting and enable this setting only when they need to create a new pairing with a trusted device. Many new devices (for example, iPhone 6) unfortunately don't have a setting to turn off discovery without disabling Bluetooth entirely. While the logic behind this is that the iPhone automatically prevents access to personal data through the Bluetooth connection, on any devices that make turning off discovery possible, it should be done.

Given all this, if a device that is supposedly secured makes an unintended Bluetooth connection, it could be a clue that the device has been compromised through either malware or social engineering.

Location services

Location services making use of GPS services can track the geographic location of your device. In this section you'll learn about these two related services.

Global Positioning System (GPS) services

A global positioning system (GPS) uses satellite information to plot the global location of an object and use that information to plot the route to a second location. GPS devices are integrated into many of the mobile devices discussed already and are used for many things, but when I use the term for a stand-alone device, I am usually referring to a navigation aid.

These aids have grown in sophistication over time and now not only can plot your route but also help you locate restaurants, lodging, and other services along the way. Another use for these devices is tracking delivery vehicles and rental cars.

GPS not functioning

When location services do not appear to be working (these are the services that make the GPS feature work), keep the following principles in mind:

- Make sure GPS is turned on!
- Keep in mind it always works best outdoors rather than indoors.
- Check for Internet access. If you don't have that, you won't have GPS services.
- The first time you use the GPS service, it will take longer because it must find the GPS location.
- As always, the first thing to try is restarting the device.

The GPS performance on some mobile devices can also be affected by the position of your hand on the device. If your hand covers the antenna used for GPS, performance can be negatively affected. It also has been reported that certain UV-protected windshields can block GPS.

Cellular location services

Location services allows the device to determine your location for the purpose of tailoring search results. Location tracking can be disabled on a mobile device. In most cases, disabled location tracking is the default, and users will be asked by certain applications if they want to enable it. When a user has never enabled this feature or has disabled this feature and it suddenly begins to track the location of the device, it is another indication that the device has been compromised.

Mobile device management (MDM)/mobile application management (MAM)

Centralized mobile device management tools are becoming the fastest-growing solution for both organization issues and personal devices. Some solutions leverage the messaging server's

management capabilities, and others are third-party tools that can manage multiple brands of devices. Systems Manager by Cisco is one example that integrates with their Cisco Meraki cloud services. Another example for iOS devices is the Apple Configurator. One of the challenges with implementing such a system is that not all personal devices may support native encryption and/or the management process.

Typically, centralized mobile device management tools handle company-issued and personal mobile devices differently. For organization-issued devices, a client application typically manages the configuration and security of the entire device. If the device is a personal device allowed through a bring-your-own-device (BYOD) initiative, the application typically manages the configuration and security of itself and its data only. The application and its data are sandboxed from the other applications and data. The result is that the organization's data is protected if the device is stolen, while the privacy of the user's data is also preserved.

Mobile device management (MDM) policies can be created in Active Directory (AD), or they can be implemented through MDM software. This software allows you to exert control over the mobile devices, even those you do not own if they have the software installed. These policies can force data encryption and data segregation, and they can be used to wipe a stolen device remotely.

Corporate email configuration

Email is one of the most important functions that people access on their mobile devices. This section will discuss how to configure email on a mobile device. The following procedures are common examples, and your specific device may differ slightly. Please consult the documentation for your device.

Before you can access email on your mobile device, you must know the settings for the email server of your email provider. There are two protocols that can be used to access email accounts: Post Office Protocol (POP) 3 and Internet Message Access Protocol (IMAP). If your account offers the use of IMAP, you should select it in the following steps because IMAP accounts have more functionality. You will need the following information to complete this setup:

- The fully qualified domain name (FQDN) of your POP3 server or IMAP server (this server receives the emails sent to you, so it's sometimes called incoming)
- The FQDN of your Simple Mail Transfer Protocol (SMTP) server (this server sends your email to the recipient's email server, so it's sometimes called outgoing)
- The port numbers used for both server types
- The security type used (if any)

POP3

On an Android mobile device, follow these steps:

1. In Settings, select Clouds And Accounts and then Accounts.
2. In Accounts, select Add An Account and select Email as the type.

3. Enter the email address and password and select Sign In.
4. After your account is recognized and set up, select Pop3 as the account type.
5. Enter the name of the incoming POP3 server, and if desired, select to enable encryption.
6. Enter **110** as the incoming port, and if desired, select Delete Email Off The Server.
7. Enter the name of the outgoing PO3 server and enter port number 25.
8. Finally, if desired, turn on SMTP authentication.

On an iOS mobile device, follow these steps:

1. Select Settings ➢ Accounts And Passwords ➢ Add Account.
2. Select Other.
3. Select Add Mail Account. Fill in your name, your email address, your password, and a description. Click Next.
4. Select POP. Verify that the name, address, and description carried over from the last page.
5. Under Incoming Email Server, enter the FQDN of the POP3 server, your email address, and your password.
6. Under Outgoing Mail Server, enter the FQDN of the SMTP server and your email address.
7. Click Next. Click Save in the upper-right corner.

IMAP

On an Android mobile device, follow these steps:

1. In Settings, select Accounts, then Add An Account.
2. Click the appropriate account type.
3. If prompted for an account subtype, select the type.
4. After entering the email address, tap Next.
5. After entering the password, tap Next.
6. If prompted, enter the username, password, or server.
7. After configuring any account options desired (Sync Frequency, Inbox Download Size, and so on), click Next.
8. Complete any account options based on the account type chosen.
9. Enter the account name and, if prompted, the name for outgoing messages.

On an iOS mobile device, follow these steps:

1. Select Settings ➢ Accounts And Passwords ➢ Add Account.
2. Select Other.
3. Select Add Mail Account. Fill in your name, your email address, your password, and a description. Click Next.

4. Select IMAP. Verify that the name, address, and description are carried over from the last page.
5. Under Incoming Email Server, enter the FQDN of the IMAP server, your email address, and your password.
6. Under Outgoing Mail Server, enter the FQDN of the SMTP server and your email address.
7. Click Next. Click Save in the upper-right corner.

Port and SSL settings

With either operating system, you can (and should) select to use security if your email server supports it. This will encrypt all traffic between the mobile device and the email server. The choices offered are usually SSL or TLS, so you will need to know which of these is in use.

Two-factor authentication

Authentication factors describe the method used to verify the user's identity. There are three available authentication factors:

- Something you know (such as a password)
- Something you are (such as a fingerprint)
- Something you have (such as a smartcard)

When two different types of factors are required (such as something you know and something you have), it is called two-factor authentication. It is important to understand that using two or more of the same type of factors (such as a password and a PIN, both something you know) is not multifactor authentication. However, when multifactor authentication is used for mobile devices, the level of security is significantly increased.

Corporate applications

Authenticator applications, such as Google Authenticator, make it possible for a mobile device to use a time-based one-time password (TOTP) algorithm with a site or system that requires such authentication. In the setup operation, the site provides a shared secret key to the user over a secure channel to be stored in the authenticator app. This secret key will be used for all future logins to the site. The user will enter a username and password into a website or other server, generate a one-time password for the server using TOTP running locally, and type that password into the server as well. The server will then also run TOTP to verify the entered one-time password. While Google makes versions for multiple mobile platforms, there are also other third-party solutions.

Trusted sources vs. untrusted sources

Applications and utilities for mobile devices can come from both trusted and untrusted sources. An example of a trusted source is the official Google Play site or the Apple Store. That doesn't mean these are the only trusted sources, but users should treat this issue with the same approach they have been taught with regard to desktop and laptop computers.

Any piece of software, be it an application, tool, or utility, can come with malware attached. Users should be trained to regard any software downloads with suspicion. It may be advisable to use an enterprise mobility management system to prevent users from downloading any software to a company-owned mobile device. You also may want to deselect the setting shown in Figure 1.13, which is an Android device setting. Apple devices warn users with a pop-up message when they download from an unknown source.

FIGURE 1.13 Allowing applications from unknown sources

Mobile device synchronization

Keeping information in sync between your desktop or laptop and your mobile device is one of the features that many users want to take advantage of. There are many types of information that can be synced, applications that can be installed to perform the synchronization, and connection methods that can be used to do this. This section discusses mobile device synchronization.

Synchronization methods

When synchronizing the various data types we will discuss shortly, there are three basic ways to make this happen: you can synchronize to the cloud, a desktop, or an automobile's computer system. In this section, you'll look at all three approaches.

SYNCHRONIZE TO THE CLOUD

One synchronization method that is gaining in popularity (along with all things "cloud") is synchronizing all your devices to a cloud server. This provides a central location for your data, settings, and all other items This can be set up such that all devices update with the cloud as soon as they attain Internet access.

SYNCHRONIZE TO THE DESKTOP

Another approach is to set up a sync process directly between two devices such as a smartphone and a desktop computer. In this case, the two devices will sync with each other any time they find themselves on the same network, such as a home wireless network.

SYNCHRONIZE TO THE AUTOMOBILE

Yes, cars have computing systems and as such can be synced to the mobile device either by using Bluetooth or by using cables designed by the vendors to connect to the car system.

Recognizing data caps

Many smartphone accounts have a data cap. Regulating data use is complicated, because most users have no idea how much data they're using by streaming a video or getting turn-by-turn directions. To identify the current use, follow these steps:

iPhone

1. Open Settings. It's a gray app with gears that you'll likely find on the Home screen.
2. Tap Cellular. This option is near the top of the Settings page. On phones that use a UK English keyboard, tap Mobile Data.
3. Scroll down to view the Cellular Data Usage section.

Data listed under Current Period does not automatically reset for your billing cycle. You can reset your data usage statistics by tapping Reset Statistics at the bottom of the page.

Data may be listed differently on different cellular carriers and data plans. If you do not see Current Period, tap Usage below the header with your carrier's name to view your data usage.

ANDROID

1. Open your Androids Settings, typically found on the Home screen or in the app drawer.
2. Tap Data Usage. You should now see at the top of the screen the total amount of mobile data used in the current month.

Microsoft 365

In April 2017, Microsoft announced the ending of mainstream support for Office 2016 in October 2020. Today enterprises use a subscription-based product, first called Office 365 and later changed to Microsoft 365 since it incorporates many services that are not a part of Office.

ActiveSync

ActiveSync allowed a mobile device to be synchronized with either a desktop PC or a server running a compatible software product. Starting with Windows Vista, ActiveSync has been replaced with the Windows Mobile Device Center, which is included as part of the operating system.

Calendar

The calendar is a critical application for both work and play. All mobile devices support syncing the calendar between devices. In some cases, it may require a small application, especially when the email system of which the calendar is part is in a different ecosystem (for example, Google Mail and an iPhone).

Contacts

No one wants to enter a long list of contacts into a mobile device when that same list already exists in your email account. Using push synchronization (*push* means it's automatic and requires no effort on the part of the user), you ensure that any changes made to the contact list either on the mobile device or on the desktop will be updated on the other device the next time you make a connection to the email account from the other device. It will also update if the mobile device makes a direct connection to the desktop.

Commercial mail application

You probably also want to set up your personal email on a device from a commercial provider. This section will look at some of the major email systems you may encounter.

iCloud

To set up iCloud email on an Android device, follow these instructions:

1. Swipe up or down in the Home screen to access the Apps screen.
2. In Settings, select Accounts, then Add An Account.
3. Select the account type.
4. If prompted, select the account subtype.
5. After entering the email address, select Next.
6. After entering the password, select Next.

7. If promoted for the username, password, or server name, enter them and select Next.
8. Enter the SMTP server, port number, and outgoing server, and select Next.
9. After configuring any account options desired (Sync Frequency, Inbox Download Size, and so on), click Next.
10. Address any additional options you encounter and select Next.
11. Enter an account name for outgoing messages.

As you can imagine, setting up iCloud email on an iOS device is simple because the applications all reside in the Apple ecosystem. First set up an iCloud email account. If you have an email address that ends with @ *mac.com* or @ *me.com*, you already have an equivalent address that's the same except it ends with *@icloud.com*. On your iOS device, go to Settings, tap your name, and then select iCloud. Choose the apps—such as Photos, Contacts, Calendars, and third-party apps—that you want to use with iCloud.

GOOGLE/INBOX

On an Android mobile device, follow these steps:

1. Select the Gmail icon.
2. Select Already Have A Google account.
3. In the Sign In With Your Google Account field, enter your username and password and select Sign In.

On an iOS mobile device, follow these steps:

1. Select Settings ➢ Accounts & Passwords ➢ Add Account.
2. Select Gmail.
3. Fill in your name, address, password, and description if desired. Click Next.
4. Verify that the address carried over from the last page. Click Next.
5. Select the items you want to sync automatically with the email server and click Done.

EXCHANGE ONLINE

To set up Outlook on Android, first, if required, install Outlook for Android. Follow these steps:

1. On the Android device, select the Email icon.
2. After entering the email address and password, select Manually Setting.
3. Complete the Domain\Username field.
4. After entering the password for the Exchange Server, select Use Secure Connection (SSL) and then Next.
5. In the Account Options interface, select a frequency for checking email and click Next.
6. Finally, if desired, enter a name for the account in the Give This Account A Name field and select Done.

On iOS, follow these steps:

1. Add your Exchange account by tapping Settings ➢ Passwords & Accounts ➢ Add Account ➢ Exchange.
2. Enter your address.
3. Choose either Configure Manually or Sign In to connect to your Exchange Server.

If you select Configure Manually, you can set up an Exchange account with Basic authentication. Enter your email password. You might also be prompted to enter additional server information.

If you select Sign In, your email address is sent to Microsoft to discover your Exchange account information. If your account uses multifactor authentication, you'll be guided through a custom authentication workflow.

YAHOO

Because Yahoo recommends using IMAP as an email client, these are the instructions for setting up IMAP on Android systems:

1. Swipe up or down on the Home screen to access the Apps screen.
2. In Settings, select Accounts and then add an account.
3. After selecting the account type, select the subtype if required.
4. Enter the email address and then select Next.
5. After entering the password, select Next.
6. If prompted, enter the username, password, or server and click Next.
7. Configure the SMTP server, port number, and outgoing server and click Next.
8. Select any account options desired, such as Sync Frequency, Inbox Download Size, and so on, and select Next.
9. If prompted, enter an account name and an account for outgoing messages.

On an iOS device, use these instructions:

1. Tap Select Settings ➢ Accounts & Passwords.
2. Tap Add Account.
3. Tap Yahoo.
4. Enter your name, your email address, your email password, and a description; then tap Next.
5. Optionally, disable aspects of Yahoo Mail from syncing.
6. Tap Save.

Exam essentials

Enable Bluetooth and pair a Bluetooth device with a mobile network. Describe the process for both the iOS and Android operating systems.

Configure email on a mobile device. Describe the process of configuring email, including both Exchange and Gmail for both the iOS and Android operating systems.

Review Questions

You can find the answers in the appendix.

1. Which email client does Yahoo recommend when you are setting up Yahoo email?
   - **A.** SMTP
   - **B.** IMAP
   - **C.** POP3
   - **D.** S/MIME
2. Which action can invalidate a laptop warranty?
   - **A.** Reinstalling the OS
   - **B.** Opening the case
   - **C.** Flashing the BIOS
   - **D.** Performing a remote wipe
3. What special screwdriver is typically required to work on a notebook?
   - **A.** Phillips head
   - **B.** T-8 Torx
   - **C.** Hex
   - **D.** Metric
4. If you have an email address that ends with *@mac.com* or *@me.com*, you already have an equivalent address that's the same except that it ends with which of the following?
   - **A.** @iapple
   - **B.** @icloud
   - **C.** @iemail
   - **D.** @istorage
5. Which component if damaged can render the hard drive useless?
   - **A.** The caddy
   - **B.** The rails
   - **C.** The signal pins
   - **D.** The chassis
6. What tool replaced ActiveSync?
   - **A.** iSync
   - **B.** MS Mobile Wizard
   - **C.** Windows Mobile Device Center
   - **D.** Office 365

7. Which is *not* an advantage of solid-state drives?
   - **A.** Cheaper
   - **B.** Not as susceptible to damage
   - **C.** Faster
   - **D.** No moving parts

8. Which of the following makes it possible for a mobile device to use a time-based one-time password (TOTP) algorithm with a site or system that requires such authentication?
   - **A.** Hardware security modules
   - **B.** Non-transitive trust
   - **C.** Authenticator applications
   - **D.** In-plane switching

9. Which display is a newer technology that solves the issue of poor quality at angles other than straight on?
   - **A.** Passive matrix
   - **B.** Active matrix
   - **C.** Twisted nematic
   - **D.** In-plane switching

10. Which of the following will you *not* need to set up corporate email?
    - **A.** FQDN of your SMTP server
    - **B.** IP address of your SMTP server
    - **C.** FQDN of your POP3 server or IMAP server
    - **D.** Port numbers used for both server types

11. In what mode of plug and play must the laptop be turned off and back on for the change to be recognized?
    - **A.** Hot docking
    - **B.** Warm docking
    - **C.** Cold docking
    - **D.** Open docking

12. Which of the following is *not* an example of two-factor authentication?
    - **A.** Smartcard and password
    - **B.** Smartcard and iris scan
    - **C.** Password and PIN
    - **D.** Voice recognition and password

13. Which of the following uses satellite information to plot the global location of an object and uses that information to plot the route to a second location?
    - **A.** GPS
    - **B.** Geofencing
    - **C.** Remote wipe
    - **D.** Local wipe

14. Which of the following provides centralized device management for company-issued and personal mobile devices?
    - **A.** MDM
    - **B.** DFS
    - **C.** PCM
    - **D.** PS/2

15. Which is the most common PIN code when selecting discovered Bluetooth devices?
    - **A.** 0000
    - **B.** 5555
    - **C.** 1111
    - **D.** 0135

16. When setting up POP3, which of the following port numbers should you enter?
    - **A.** 25
    - **B.** 53
    - **C.** 110
    - **D.** 443

17. Which of the following storage system monitors the data being read from the hard drive and caches the most frequently accessed bits to the high-speed flash memory?
    - **A.** SSD
    - **B.** HDD
    - **C.** Hybrid drive
    - **D.** Virtual

18. Which of the following is the use of physical factors of authentication?
    - **A.** Mutual authentication
    - **B.** SSO
    - **C.** Multifactor authentication
    - **D.** Biometrics