Chapter 1

Mobile Devices

COMPTIA A+ 220-1201 EXAM OBJECTIVES COVERED IN THIS CHAPTER:

✓ **1.1 Given a scenario, monitor mobile device hardware and use appropriate replacement techniques**

- Battery
- Keyboard/keys
- Random-access memory (RAM)
- Hard disk drive (HDD)/solid-state drive (SSD)
- Wireless cards
- Physical privacy and security components
- Wi-Fi antenna connector/placement
- Camera/webcam
- Microphone
- Exam essentials

✓ **1.2 Compare and contrast accessories and connectivity options for mobile devices**

- Connection methods
- Accessories
- Docking station
- Port replicator
- Trackpad/drawing pad/track points
- Exam essentials

✓ **1.3 Given a scenario, configure basic mobile device network connectivity and provide application support**

- Wireless/cellular data network (enable/disable)
- Bluetooth
- Location services
- Mobile device management (MDM)
- Mobile device synchronization
- Exam essentials

This chapter will focus on the exam topics related to mobile devices. It will follow the structure of the CompTIA A+ 220-1201 exam blueprint, Objective 1, and cover the three subobjectives that you will need to master before taking the exam. The mobile devices domain represents 13% of the total exam.

1.1 Given a scenario, monitor mobile device hardware and use appropriate replacement techniques

In today's environment, laptops and tablets (those names will be used interchangeably) share many of the same types of components. In this section, I'll discuss how to monitor the performance of some of the basic components and how to replace them when appropriate.

The following topics are addressed in Exam Objective 1.1:

- Battery
- Keyboard/keys
- Random-access memory (RAM)
- Hard disk drive (HDD)/solid-state drive (SSD)
- Wireless cards
- Physical privacy and security components
- Wi-Fi antenna connector/placement
- Camera/webcam
- Microphone

Battery

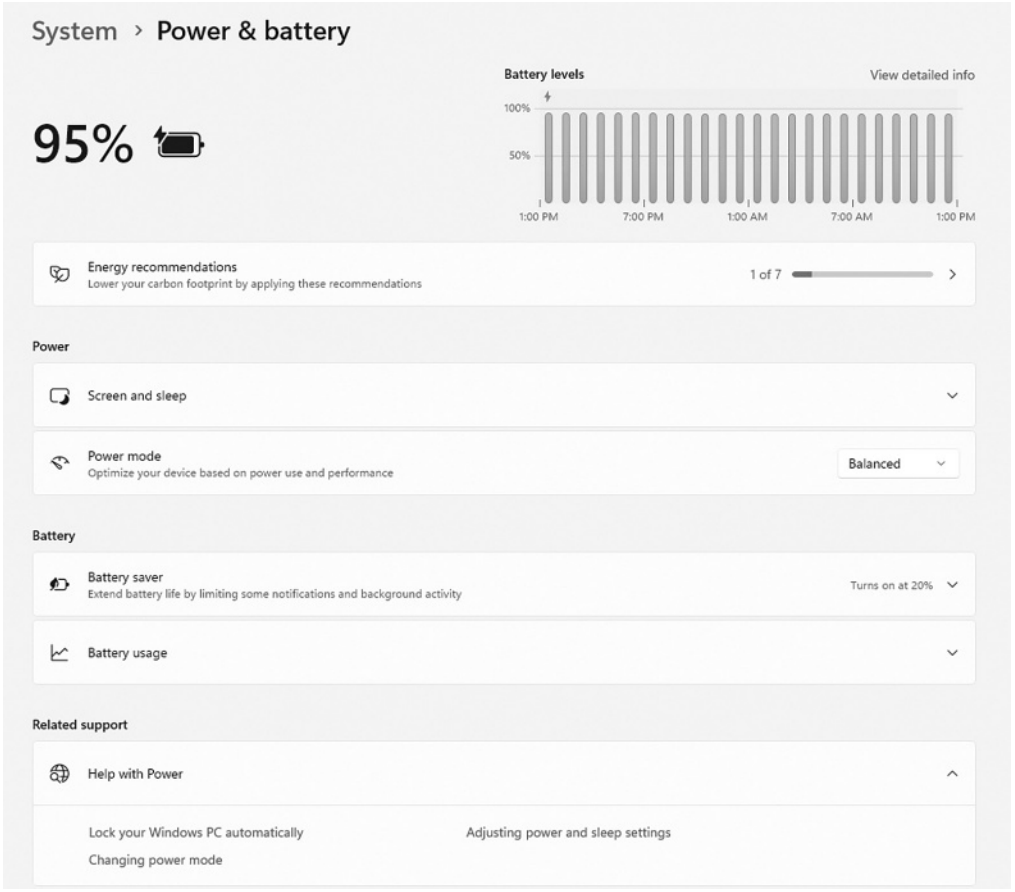
Monitoring and maintaining the battery in a mobile device is very important. After all, you don't want your notebook to die just as you are about to advance to the next level of your favorite video game! In addition to watching the battery-power level, you can manage

several items that control how your battery consumes power. In a Windows machine, type **Power & Battery** in the search bar, which will bring you to the corresponding systems control screen, as shown in Figure 1.1. Here you can adjust the power and battery settings to get the most usefulness when you're running on battery power.

If you find yourself needing to replace your laptop battery, check out the following steps.

Replacing a laptop battery 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.

FIGURE 1.1 Power and battery settings



With all of this said, if the laptop or mobile device does not have an externally accessible battery, opening the case to replace the battery will void the warranty.

Keyboard/keys

Keyboards on laptops are not replaced very often, considering that it is often easier to use an external keyboard. However, if you spill something on your keyboard or the keys break or wear down, you might find yourself in need of a replacement keyboard. While these steps work on most laptops, it's always a good idea to refer to the manufacturer's website for model-specific instructions.

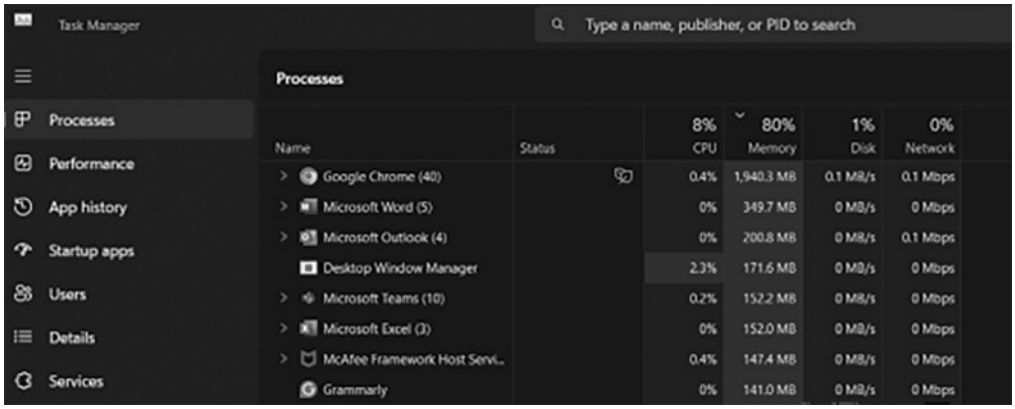
When replacing the keyboard, one of the main things you want to keep in mind is not to damage the data cable connector to the system board. Follow these steps for a smooth replacement:

1. With the laptop fully powered off and unplugged from the electricity source, 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 on the back of the laptop. If not, look up the model online and determine which of the screws are attached to the keyboard.
2. Remove the screws with a T8 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 must have screws removed to get them out of the way; if so, remove the screws and those plastic pieces. In some cases, there may simply be clamps that can easily be removed.
3. With any plastic covers out of the way, remove any screws at the top and then 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 because it can be easily damaged!
4. Take a pick and lift the plastic connectors holding 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 ensure 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 previously.
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 the laptop back on, check functionality. If the keyboard doesn't work, the main component to check is the data connector.

Random-access memory (RAM)

You can monitor your RAM usage a couple of different ways. In Windows, the Task Manager is a great place to start. Hit Ctrl-Alt-Del simultaneously, and in the menu screen, select Task Manager. What you should see is the Task Manager, as shown in Figure 1.2.

FIGURE 1.2 Task Manager



The Processes tab will show you some key metrics, including Memory (RAM) usage by application. As shown in Figure 1.2, Google Chrome is consuming a considerable amount of RAM. Time to shut down some browser tabs!

With that said, installing more RAM in your computer is usually one of the best upgrades to perform.

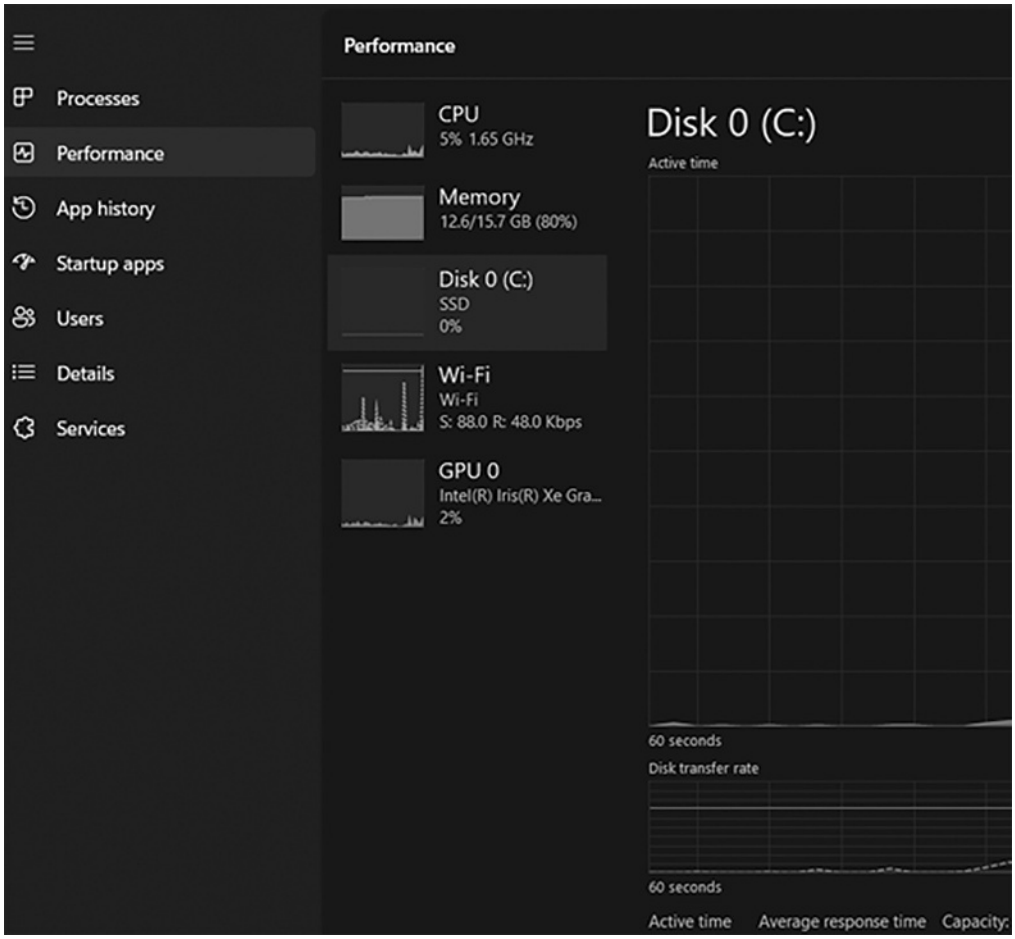
There should be a panel used for access to the memory modules. If the panels are not marked (as many are not), refer to your laptop instruction manual to locate the bottom panel. Follow these steps to perform a memory upgrade:

1. Remove any screws holding the panel in place, then remove the panel from the laptop and set it aside. If you're removing an existing memory module, remove it by undoing the module clamps, gently lift the edge of the module to a 45-degree angle, and then pull 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 computer system's user manual for any additional information.

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

The Task Manager also allows you to monitor your disk performance, whether it is an HDD or SSD. Figure 1.3 shows the Performance tab, indicating disk usage.

FIGURE 1.3 The Performance tab



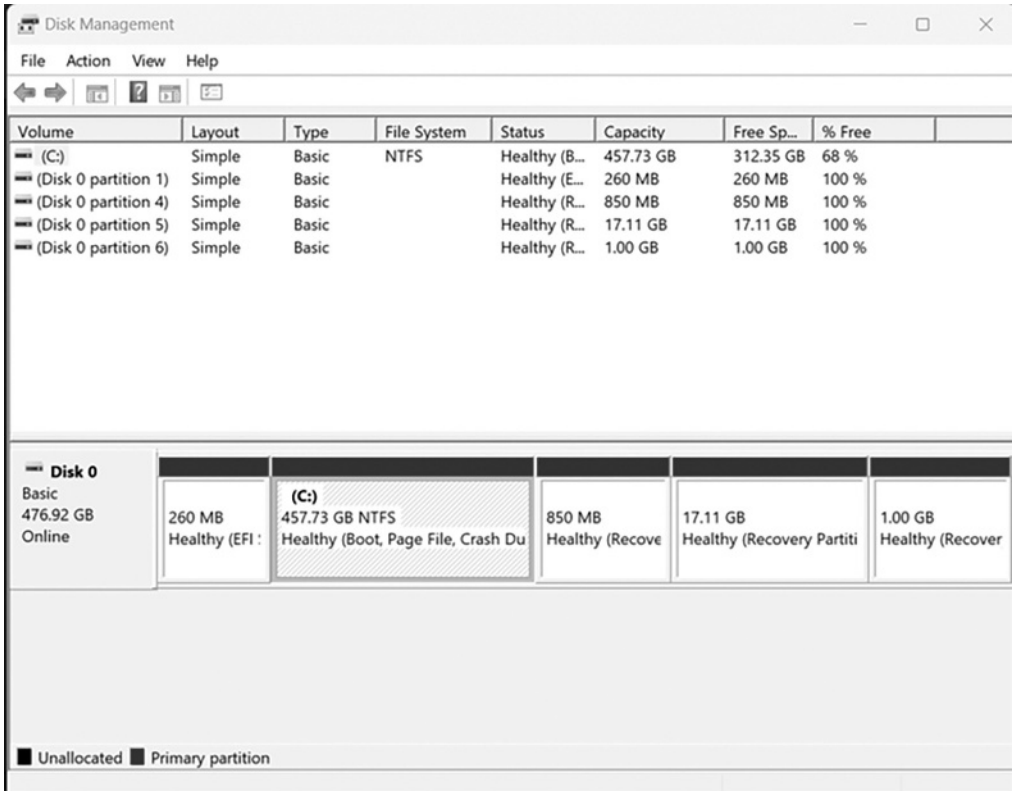
You can also right-click on the Windows logo and select Disk Management from the menu, as shown in Figure 1.4, which will show you the drive status.

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 its place.

FIGURE 1.4 Disk Management



2. You might 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, ensuring it is right side up. Do not force it into place. 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 disk or a complete image disk (before the drive failed, by the way), place it in the optical drive and follow the instructions for restoring the data.

SSDs

Although many devices still use a magnetic disk hard drive, most laptop vendors are moving to using either solid-state drives or hybrid drives. Hybrids 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 inch vs. 2.5 inch

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

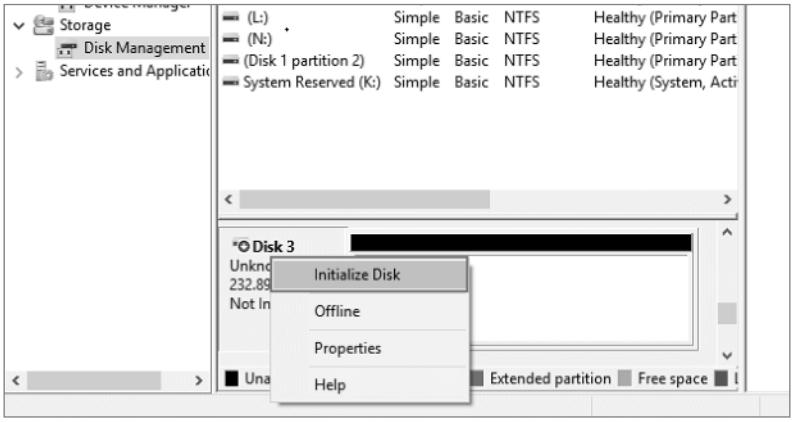
The 1.8 inch drive is the smallest of the three I'm discussing here. It was originally used in subnotebooks and audio players. It has the least capacity of the three, with the largest up to 320 GB.

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

When you have made the decision to migrate data from HDDs to SSDs, 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 set in place.
2. In Windows, go to Disk Management, select the SSD and Initialize Disk, as shown in Figure 1.5. (This assumes the HDD has already been initialized to the local system.)
3. Open the Control Panel and go to Control Panel > System, Security > Backup, and then Restore (Windows 7).
4. Click Create a System Image in the left pane. On the Do You Want to Save Backup page under the On a Hard Disk drop box, choose the SSD. After selecting the destination disk or volume, click Next.
5. Make sure both the System Reserved (System) and (C:) (System) drives (assuming C is where the operating system is located) are selected. Also, select any other drives that may hold data as well. Click Next. Confirm the backup settings and then click Start Backup.

FIGURE 1.5 Initialize Disk



Wireless cards

Wireless cards in notebooks are usually accessed through a panel on the case, but this may vary. In any event, the wireless card is often replaceable in case you want to upgrade to the latest and greatest Wi-Fi version. With that said, there are many settings for performance and access, which are generally described here.

The Task Manager can help you monitor your Wi-Fi performance. Figure 1.6 shows the Wi-Fi tab.

You can also see your wireless card performance by right-clicking on the Wi-Fi symbol in the system tray, then selecting Network and Internet Settings. In the window that pops up, select Advanced Network Settings, then select your wireless adapter. Figure 1.7 shows the Advanced Network Settings tab.

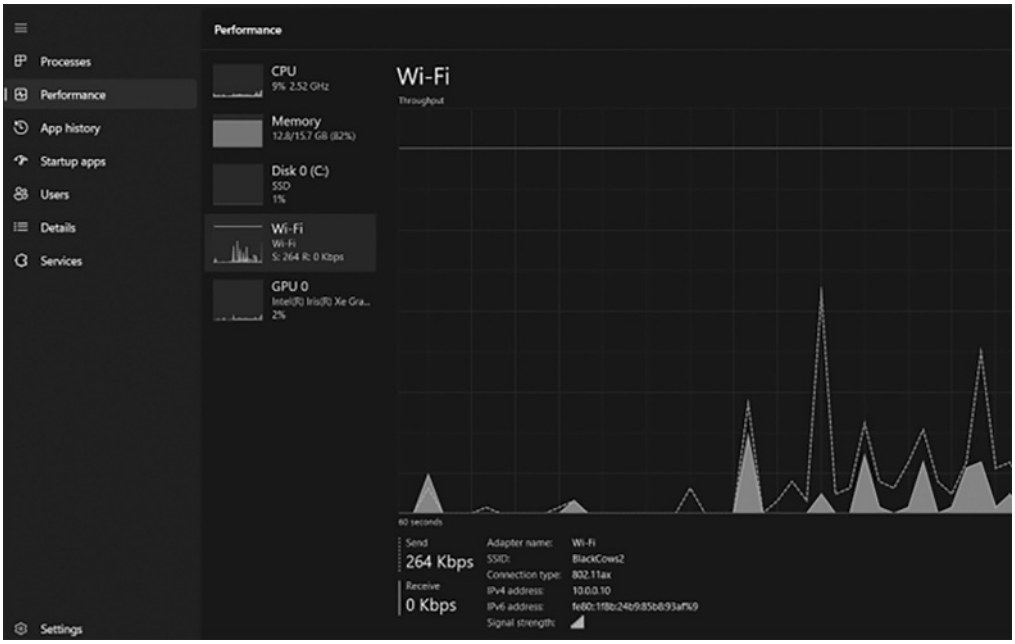
Finally, click on Edit next to More Adapter Options to show the Wi-Fi Properties screen. Here you will find the details on how the wireless card is configured. Figure 1.8 shows the Wi-Fi Properties screen.

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 for Dell Inspiron), you have to remove the memory, keyboard, optical drive, and hand rest to get to the card. 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 laptop's 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

FIGURE 1.6 The Wi-Fi tab



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.

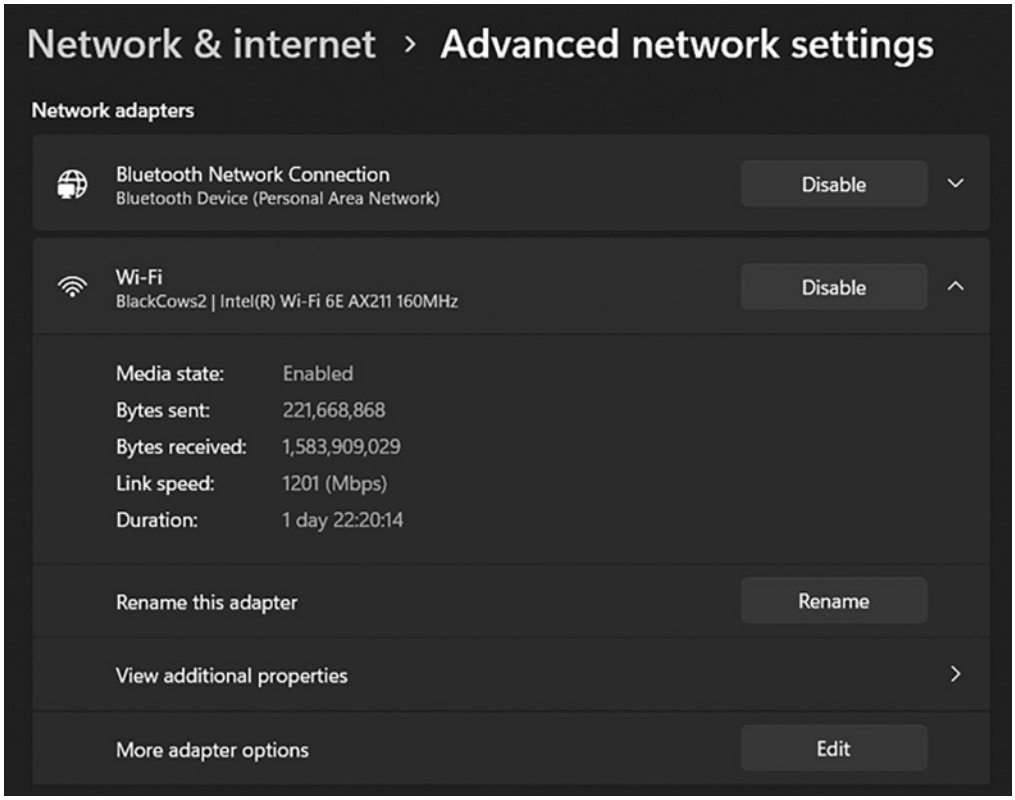
Cellular card

Changing an external mobile broadband card is as simple as pulling out the old USB stick and plugging in the new one. Because the 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 link to their website where the drivers may be downloaded. Changing an internal card is much like 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 card's location in the laptop's documentation. Make sure that the new card is firmly inserted into the slot after removing the old card.

FIGURE 1.7 The Advanced Network Settings tab



Physical privacy and security components

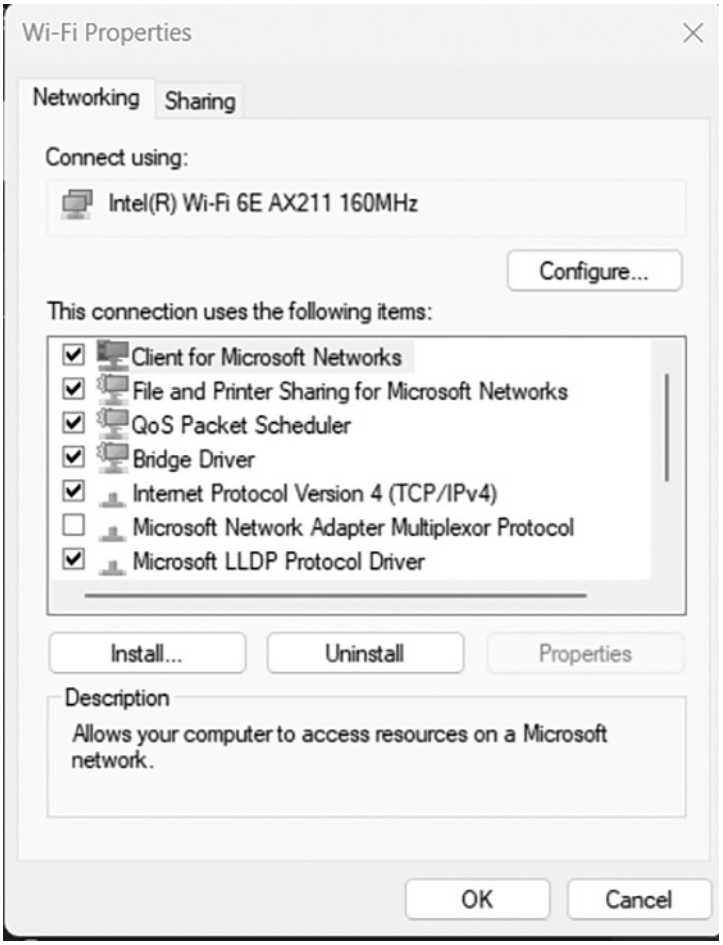
In Windows 11, one of the most common ways to secure your mobile device is through Windows Hello, commonly known as a personal identification number (PIN). This feature allows you to store log-on credentials securely. When you open an application or a website, Windows Hello will retrieve your credentials and apply them once you supply your PIN.

Some features are designed to enhance the privacy of data on a device and 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 use fingerprint or facial recognition technology. While there can be issues with both false negatives (i.e. the denial of a legitimate user)

FIGURE 1.8 Wi-Fi Properties



and false positives (i.e. the admission of an illegitimate user), biometric implementations offer much better security than other authentication mechanisms.

A good example is a fingerprint lock, which uses the user's fingerprint as a credential to authenticate the user and, when authentication successfully 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 11, follow these steps:

1. Search for Settings in the Start menu and click on it. This action will open the Settings app.
2. Select Accounts > Sign-in Options. On the right panel, find the Fingerprint section under Windows Hello and click on the Set Up button.

3. On the Welcome screen, click the Get Started button to continue.
4. Authenticate yourself with a PIN or 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 finished.

Near-field scanner features

Near-field scanners allow you to use the chip feature on credit and debit cards. When the chip end of the card is inserted into the payment device, the near-field scanner reads the information off the chip and processes the transaction.

A near-field scanner allows you to measure and map the electromagnetic interference (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 also be used to analyze potential circuit designs for flaws. These devices are typically handheld.

Wi-Fi 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's 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 might improve your signal by moving your laptop around. This movement changes the antenna's polarization and may cause it to align better with the incoming signal.

Camera/webcam

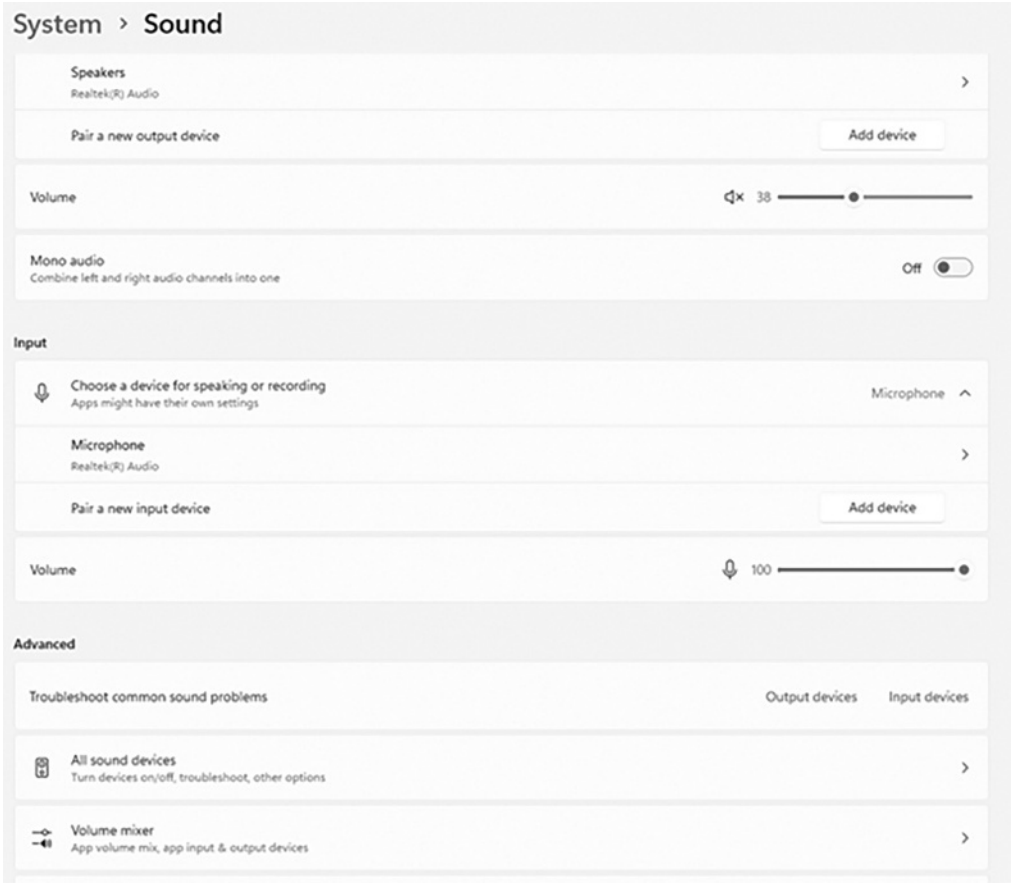
Many displays today, especially laptop displays, have a webcam built in. They come ready to go with all drivers preinstalled and nothing to configure or set up. If you need to replace your webcam, you will have to disconnect the laptop lid (which holds the display) from the base, remove the screw covers 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 you must 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.

Webcams are widely available as a USB peripheral. You might find that purchasing an external camera is a much easier option than replacing the built-in camera.

Microphone

In Windows, controls for the microphone and speakers are located under System > Sound. You can troubleshoot issues with your microphone and speakers in this panel, as shown in Figure 1.9.

FIGURE 1.9 The Sound panel



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 located 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 might 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.

Exam essentials

Know where to monitor hardware issues. Task Manager is the first place to go when you are monitoring hardware issues, such as RAM, HDD, or SSD issues. Use the System panel to see specific device configurations and make adjustments.

Know where to access critical components. SSDs, HDDs, RAM, keyboards, and wireless cards are the components that are most often replaced. If what you're trying to find does not have an access panel, make sure you know how to find your device's user manual or a YouTube video for further replacement panels.

1.2 Compare and contrast accessories and connectivity options

Your mobile device can be the platform to which you can attach many other devices, wirelessly or through a cable. In many cases, your mobile device can be used as a wireless hotspot. The following topics are covered in Exam Objective 1.2:

- Connection methods
  - Wireless
  - Cables
- Accessories
- Docking station
- Port replicator
- Trackpad/drawing pad/track points

Connection methods

Two primary methods are used to connect other devices to your mobile device: a wireless connection and a wired or cabled connection. Both have several variations, and we will cover them in this section.

Universal serial bus (USB)/USB-C/micro USB/mini USB

We will explore the various types of USB connectors. Pay particular attention to the transfer rates and what the connector looks like. Keep in mind that the most common USB connector for mobile devices today is Type C.

USB is an expansion bus type that is used almost exclusively for external devices. All motherboards today have at least two USB ports. Some advantages of USB include hot

plugging (i.e. the ability to plug or unplug a device without shutting the system down) and the capability for up to 127 USB devices to share a single set of system resources. Even if your device has only two USB ports, using a multiport hub will allow you to increase the number of USB devices that you can connect.

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 (i.e. cards 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, tablets, and digital cameras, whereas the mini is used to transfer the data between digital devices and computers. The choice between a standard A and B and a mini A and B is dictated by what is present on the device. The cables used cannot exceed 5 m in length. Figure 1.10 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.

USB-C

The USB-C connectors unite with 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 1.11 next to a USB 3.0 cable.

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

FIGURE 1.10 USB connectors

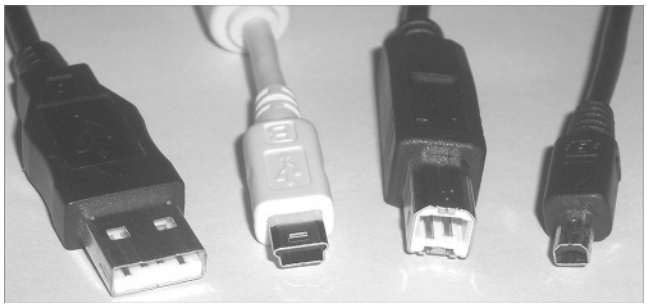
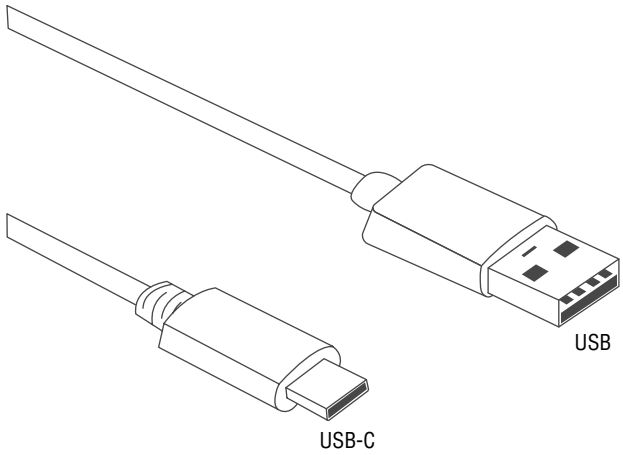


FIGURE 1.11 USB-C and USB 3.0 cable



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 operate at only 2.0 speeds.

By using USB hubs in conjunction with the USB ports available on the local machine, you can connect up to 127 of these devices to a 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

While millions of Apple devices use Lightning connectors for power, Apple is making the transition to USB-C as its primary connector.

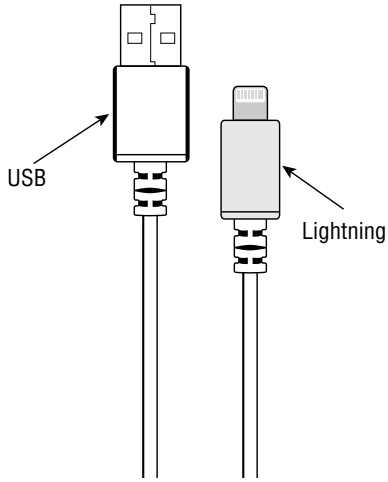
Although it makes an adapter to convert a Lightning connector to mini-USB, Apple doesn't encourage its use because of the limitations the adapter places on the functionality of the proprietary connector.

The Lightning connector 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 MBps. Following are some of the 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 1.12 shows a Lightning connector next to a USB cable.

FIGURE 1.12 Lightning connector and a USB cable



Near-field communications (NFC)

Near-field communications (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 does; 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 International Standards Organization (ISO) and uses tags that are embedded in the device. NFC components include an initiator and a target; the initiator actively generates a radio frequency (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 might 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 using either 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 that can in other cases 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
- Communicating between toys used in gaming
- Communicating with peripherals

Bluetooth

Bluetooth, like USB, has become ubiquitous as a method to connect devices. Bluetooth has even made its way into automobiles, allowing for things like Apple CarPlay and hands-free cell phone operation. If you have a vehicle that monitors your tire pressure, there is a sensor that uses Bluetooth or RFID to transmit your tire pressure information to the car's computer.

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 m (330 ft), and most devices are specified to work within 10 m (33 ft). When printing with a Bluetooth-enabled device (like a tablet or mobile phone) and a Bluetooth-enabled printer, all you need to do is get within range of the device (i.e. 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 1.1 details the speeds for the latest versions.

TABLE 1.1 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

Tethering/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. Often, public hotspots in places like cafes 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

Accessories are items you use with your mobile device to make it more convenient or to increase your productivity. You might want to add a stylus for a tablet, a headset for your mobile phone, or even speakers. We'll take a look at several different accessories.

Stylus

A stylus is an electronic pen that works with a touch screen device. You often see a stylus when you need to sign for purchase at a retail location or a bank. The pen-like device that you "sign" with is a stylus. You can also see a stylus paired with a tablet. The waitstaff in many restaurants use wireless ordering pads, with a stylus to select the menu items tableside.

Headset

There are many headset types that allow you to privately listen to content from your mobile device. Some headsets provide only listening capability, while others have built-in microphones.

There are also specialized headsets for virtual reality (VR) and augmented reality (AR). Both technologies enrich a user's visual experience. AR can be deployed on a smartphone, allowing you to point the smartphone camera at a sign printed in a foreign language and receive instant translation. VR headsets, which look like goggles, immerse the viewer in a 3D environment. Most often seen in gaming systems, VR also has many applications in education, marketing, and e-commerce.

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

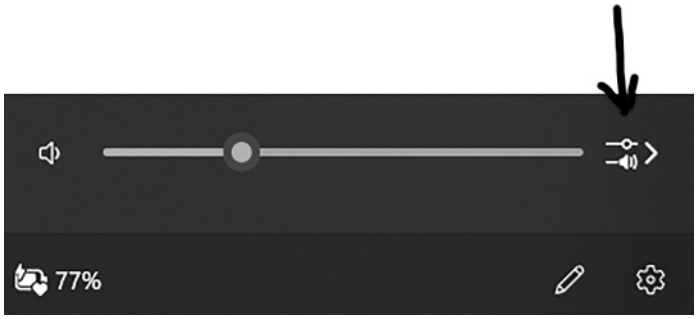
Speakers

On a laptop, you can control many aspects of how the speakers sound by clicking on the speaker icon in the system tray. Figure 1.13 indicates the icon to select to control the sound.

Then, click on the sound controls to raise or lower the sound, as shown in Figure 1.14.

FIGURE 1.13 Sound icon in system tray

FIGURE 1.14 The sound volume control



In the pop-up window, you can select your speaker options. Figure 1.15 shows several speaker options.

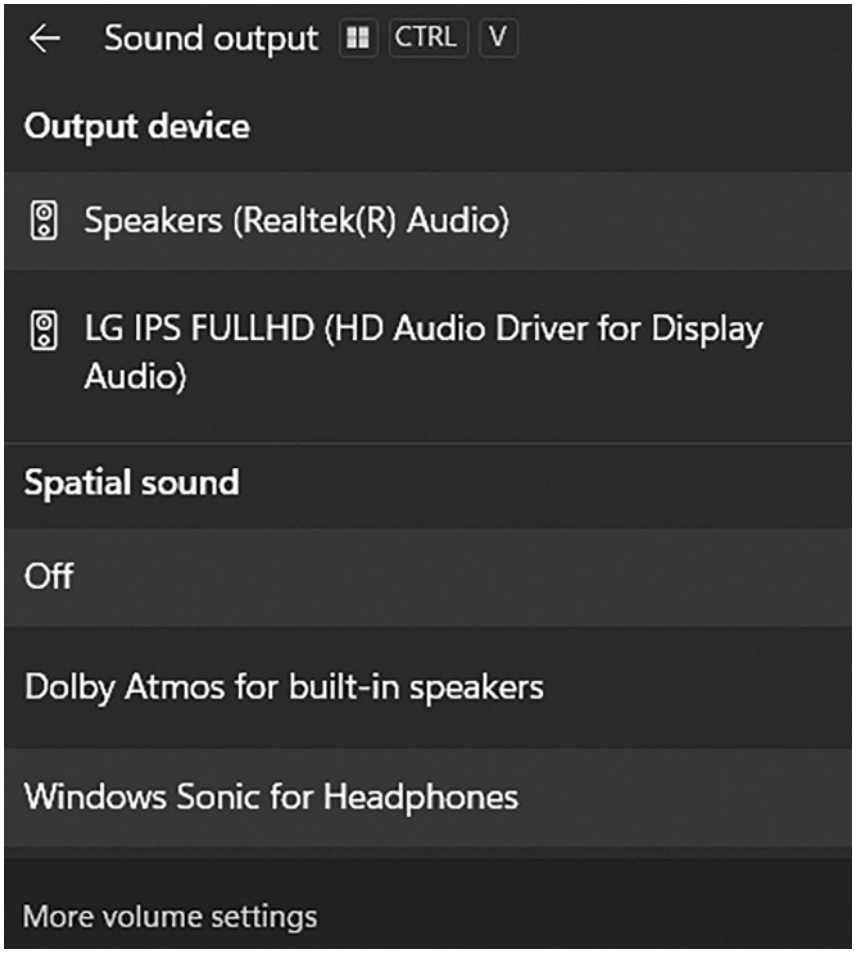
You can further fine-tune your audio characteristics by clicking on More Volume Settings.

Speakers are used in the same fashion as headsets. They can also be connected using the same options, which include using USB, a 3.55 mm audio plug, or Bluetooth. This includes the speaker systems in many cars, which can now be paired with 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 while pressing the 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 might be changing the location of the display output.) If these keys are not present, consult the documentation for which keys to use in conjunction with Fn to lower and raise the volume. Most laptops also include a mute button marked as such.

FIGURE 1.15 Speaker options available



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 the speakers are connected to a power source, connect the speaker cable to the proper plug on 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 laptop's 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 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. However, with laptops, it is possible to replace the internal speakers.

To determine whether the settings are the issue, ensure that the speaker volume is turned 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 hear whether the speaker that you hold up to your ear to listen to people is working properly as well.

On an iPhone, follow these steps:

1. Go to Settings > Sounds & Haptics and drag the Ringtone 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

Webcams are built into most mobile devices. When coupled with the appropriate application, webcams allow you to broadcast full-motion video and audio over the Internet. Alternatively, you can record video for editing and subsequent publishing. Webcams are used for videoconferencing, delivery of education, publishing to social media, and much more.

Earlier in this chapter, you learned about webcams. External 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 – he 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 ports, 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.

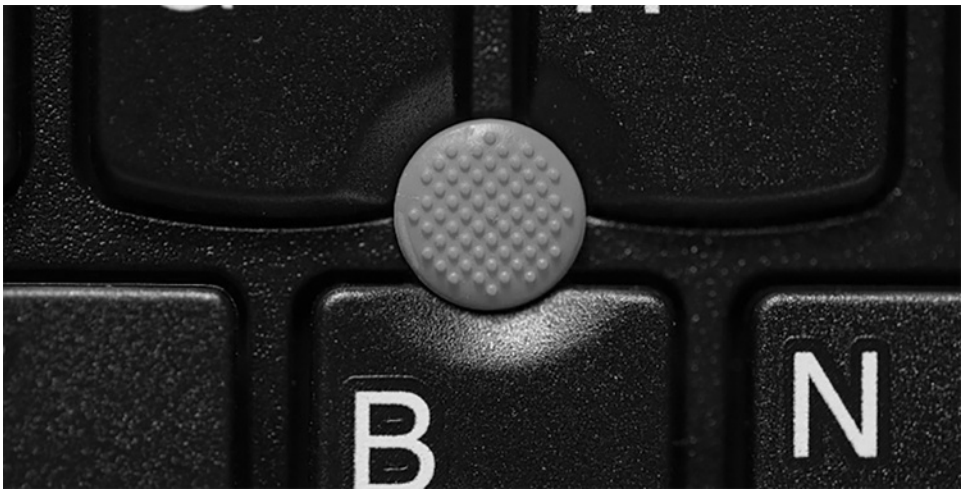
Cold docking The laptop must be turned off and back on for the change to be recognized.

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.

FIGURE 1.16 A track point



Port replicator

Port replicators are a form of docking station and were discussed in the "Docking Station" section.

Trackpad/drawing pad/track points

A track point, sometimes called a pointing stick, is a small button on a laptop's keyboard that can be used as a mouse. Figure 1.16 shows a track point.

An optical trackpad is an input device based on an optical sensor, which detects the finger's movement on top of it. This sensor typically is used in smartphones, where it replaces the drawing or D-pad. The main advantages a trackpad has 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

Identify all types of connection methods. Be able to identify images of the various USB connectors. Know their data transmission rates. Be able to identify a Lightning cable. Know the differences between NFC and Bluetooth. Understand how to tether a mobile device and use it as a hotspot.

Understand the use of accessories. Know how a stylus, headset, speakers, and webcam work. Know where to go to configure the headset and speakers. Understand how docking stations and port replicators are used. Know the difference between trackpads, drawing pads, and track points.

1.3 Given a scenario, configure basic mobile device network connectivity and provide application support

You should be able to configure a mobile device for network connectivity. The following topics are covered in Exam Objective 1.3:

- Wireless/cellular data network (enable/disable)
- Bluetooth
- Location services
- Mobile device management (MDM)
- 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 has not been as good as an 802.11 Wi-Fi connection. With the introduction of newer technologies like 5G, however, the performance delivered by the cell network has become more competitive.

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 your device.

3G/4G/5G

Mobile technology and platforms are typically expressed as 3G, 4G, or 5G, with the "G" representing the term "generation." Each has its own performance characteristics. At this writing, 5G is in rollout throughout much of the United States, but there are a significant number of devices that operate in 3G or 4G.

3G

Third generation, or 3G, introduced web browsing, email, video downloading, picture sharing, and other smartphone technologies. The technology of 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.

5G

With speeds of up to 100 Gbps, 5G is as much as one thousand times faster than 4G. It provides 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. Most wireless carriers 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 Wi-Fi 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 Wi-Fi icon in the system tray.
- The hotspot will show up as a wireless connection.
- Select it and enter the password.
- Click Connect.

Wi-Fi

Making a Wi-Fi connection on a mobile device is much like doing so with a laptop. In the device's settings will be a section for Wi-Fi. (On an iPhone, it's called Wi-Fi, and on an Android device, 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 network 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.

Subscriber identity module (SIM)/eSIM

Subscriber identity module (SIM) cards were originally the size of a credit card but now are the size of a fingernail. SIM cards have a unique number assigned to them that is used to identify the subscriber and validate the device to the mobile network. SIM cards also contain account data like your phone number and other information like text messages and contacts.

SIM cards can be removed from one device and inserted into another, enabling you to keep your phone number when changing devices or phone carriers.

As technology has evolved, the embedded SIM (eSIM) is replacing the SIM on some devices. The eSIM is not a removable card but rather a part of the phone's circuitry. The functionality of the eSim is the same as that of the SIM, just in digital form.

Bluetooth

Bluetooth is a short-range wireless technology that is used to create a wireless connection between digital devices. One application 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 Bluetooth icon so it turns blue.

Enable pairing

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

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 > Connections.

3. Turn on the Bluetooth switch by tapping it.
4. In the list of Available Devices, tap the Bluetooth device to pair it with the phone.
5. Follow any on-screen instructions.
6. If a password is required, consult the device's documentation or try either 0000 or 1234 (i.e. 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 personal identification number (PIN) code

Many external devices will ask for a PIN code when you select the external device from the list of discovered devices. In many cases, the PIN is 0000, but you should check the external device's manual. In some cases, one device will generate a code, and you must enter that generated code on the other device to complete the pairing.

Test connectivity

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

Location services

There are two primary types of location services. Global Positioning System (GPS) uses satellites in geostationary orbits to determine your position. Cellular services locate your position based on your mobile device's proximity to a cell tower. GPS and cellular location services may be used independently or together.

Global Positioning System (GPS) services

GPS uses satellite information to plot the global location of an object and then uses that information to plot the route to a second location. GPS devices are integrated into many mobile devices 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 can not only 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.

Cellular location services

If you use a feature like "Find the nearest gas station," you are using location services. Let's take a look at this feature.

Location services allow 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 whether 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)

In this section, we will cover mobile device management (MDM). Mobile devices with access to the corporate network represent a significant security risk, but this risk may be mitigated through device configurations, policy enforcement, and/or corporate applications.

Device configurations

There are two primary categories of mobile devices that need specific configuration settings to securely access the corporate network: corporate-owned devices and personally owned Bring Your Own Devices (BYODs).

Corporate

If you have a corporate-owned mobile device, your configuration is going to be rather rigid, with minimal opportunities for customization. There are many reasons for these restrictions, such as protecting a company's intellectual property and network security. This is not unlike having a desktop computer, with a standard configuration called an image.

Bring Your Own Device (BYOD)

Many organizations will allow you to use your personal mobile device through a policy called Bring Your Own Device (BYOD). Even though you are using your device, keep in mind that your device has access to sensitive company information and applications. The company will want to ensure that its data and applications are safe on your device. The company may require the installation of a mobile device management (MDM) application to ensure security. MDM is one of a group of centralized MDM tools that 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 MDM 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 BYOD initiative, the application typically manages the configuration and security of itself and its data only. The application and its data are sandboxed (i.e. segregated and stored separately) 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.

Policy enforcement

Remember, while BYOD allows users to use their own devices to access company resources and data, the company wants to ensure safety and security through MDM. MDM creates policies and helps with company policy enforcement.

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 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.

An example of a TOTP password is one that is sent via text or email and must be used within a certain time frame. TOTP is often used in password reset requests.

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 log-ons 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 App 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, a tool, or a 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 might want to deselect the setting shown in Figure 1.17, which is an Android device setting. Apple devices warn users with a pop-up message when they download from an unknown source.

Mobile device synchronization

Keeping information in sync between your desktop or laptop and your mobile device is one feature 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 it. This section discusses mobile device synchronization.

FIGURE 1.17 Disallowing applications from unknown sources

Synchronization methods

When synchronizing the various data types that 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 review all three approaches.

Synchronize to the cloud

One synchronization method is synchronizing all your devices to a cloud server. This provides a central location for your data and settings. This can be set up such that all devices update to the cloud as soon as they attain Internet access.

Synchronize to a 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 one another any time they find themselves on the same network, such as a home wireless network.

Synchronize to an automobile

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

Recognizing data caps

It is very important to know whether your mobile device plan has a data cap, which is the daily or monthly limit on the data you can use. If you travel internationally, it is also important to know how the plan handles data when you cross borders.

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 video or getting turn-by-turn directions. To identify current use, follow these steps:

On an iPhone:

1. Open Settings.
2. Tap Cellular (or Mobile Data, depending on the model).
3. Tap on Usage or Data Plan, depending on the model. Review the Data Usage report.

On an Android device:

1. Open your Android's Settings.
2. Tap Data Usage. You should now see the total amount of mobile data used in the current month at the top of the screen.

Calendar

The Calendar application on the iPhone allows for syncing events from several different calendars and displays them in one central place. This feature allows you to manage your time for virtual and in-person meetings, doctor visits, speaking engagements, and things that you really don't want to forget, like birthdays and anniversaries.

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—which the calendar is part of—is in a different ecosystem (e.g. Google Mail and an iPhone).

Contacts

Synchronizing the contacts on your mobile device offers a whole new level of productivity with the Bluetooth capabilities in newer cars and applications like Apple CarPlay. I can make a call simply by saying "Call …" and a contact name. I can also dictate a text message to a contact or even dictate an email. I often dictate an email to myself while driving, when I remember something I have to do or an idea I want to follow up on. This paragraph, in fact, is a result of a dictated email with the subject "Remember to talk about dictating emails in Chapter 1."

No one wants to enter a long list of contacts into a mobile device when that same list already exists in their 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 sent (pushed) to the other device the next time you connect to that email account from the other device. It will also update if the mobile device makes a direct connection to the desktop.

Business applications

You will want to synchronize your business applications, primarily mail and cloud storage.

Mail

Let's have a brief discussion about incoming email protocols. Incoming email uses one of two protocols: POP3 (which uses port 110) or IMAP (which uses port 143). With Post Office Protocol 3 (POP3), emails are downloaded onto the device requesting new emails and removed from the server, which is fine if you check your email on only one device. Internet Message Access Protocol (IMAP), on the other hand, delivers a copy of the email to the device requesting it but keeps the original on the server. This allows you to see all of your emails on whatever device you use to open them. With IMAP, I can check my email on my phone before a flight and then use the hotel's public computer to work on a critical email. When I open the email application on that public computer, I will be able to see all of my emails.

For many people, having access to their business email on their mobile device is critical. This is particularly true as the lines between "work hours" and "personal hours" become blurred. You also want to ensure that the mail on your mobile device is synced with your primary work computer, which helps with flagging and/or prioritizing emails you need to attend to once you get to the office.

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

iCloud

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

1. Swipe up or Done in the Home screen to access the Apps screen.
2. In Settings, select Accounts, then Add an Account.
3. Click on 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 fully qualified domain name (FQDN) of the Simple Mail Transfer Protocol (SMTP) server, port number, and outgoing server and select Next. Think of the SMTP server as the Internet version of your local post office, which picks up your mail and forwards it to the next post office in the delivery path.
9. After configuring any account options desired (e.g. 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. Then tap Mail and select Use on This [device].

Gmail

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

Outlook

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 Manual 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 > Apps > Mail > Mail Accounts > Add Account > Exchange.
2. Enter your email 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 Done 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 Settings > Apps > Mail > Mail Accounts > Add Account.
2. Tap Add Account.
3. Tap Yahoo.
4. Enter your name, email address, email password, and a description and then tap Next.
5. Optionally, disable aspects of Yahoo Mail from syncing (to decrease the amount of data syncing, which will improve performance).
6. Tap Save.

Cloud storage

Several cloud storage solutions are available that allow you to create, store, and edit documents and spreadsheets as well as store images and video. The biggest advantage to cloud storage is that you have access to your items from anywhere and any device with an Internet connection. With cloud storage, you don't have to remember on which device a document or picture is located. You can share your materials with others should you choose, and many cloud services even offer online collaboration.

We have already covered iCloud. Some other examples of these cloud storage solutions include:

- Dropbox
- Google Drive
- Microsoft OneDrive

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. Detail 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 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 laptop's 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.** T8 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 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 was the smallest hard drive covered in this chapter?
   - **A.** 1.8
   - **B.** 2.5
   - **C.** 3.0
   - **D.** 3.5

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. Adding which of the following will almost always improve performance?
   - **A.** CPU
   - **B.** Disk
   - **C.** Network card
   - **D.** Memory

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.** Port numbers used for both server types
    - **D.** FQDN of your POP3 server or IMAP server

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. What small cards have a unique number assigned to them that is used to identify the subscriber and validate the device to the mobile network?
    - **A.** SIM
    - **B.** SPIM
    - **C.** vCard
    - **D.** iMobile

13. Which of the following uses satellite information to plot the global location of an object and uses that same 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 is the default port number to enter?
    - **A.** 25
    - **B.** 53
    - **C.** 110
    - **D.** 443

17. Which of the following storage systems 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 describes the use of physical factors of authentication?
    - **A.** Mutual authentication
    - **B.** SSO
    - **C.** Multifactor authentication
    - **D.** Biometrics