220-1101 Mobile Devices Study Guide

General Information - The purpose of assessing your knowledge and skills in this area is to be sure you know how to configure and install all types of mobile devices, including, but not limited to, laptops. This does not stop after the installation and configuration are complete, however. You must also be able to ensure continued connectivity for the end-users. Approximately **15%** of the questions on the **CompTIA A+ Core Series 1101 test** pertain to mobile device concepts. Note that approximately **75%** of these questions will begin with a **scenario**.

Laptop Hardware and Components - You must be able to **install and configure** the hardware and components of a laptop in a given scenario. You should be aware of the following hardware and be comfortable replacing it.

Hardware/Device Replacement - in laptops differs from desktop replacements. Space comes at a premium and the **correct tools** should be used to disassemble and reassemble laptops and their components. Be aware of the main techniques and tools used to replace laptop components. Always check **manufacturer documentation** before attempting hardware/device replacement.

Battery - Laptop **battery chemistry** is most commonly nickel-cadmium (NiCd), lithium-ion (Li-ion), nickel-metal hydride (NiMH), or lithium-polymer (Li-poly). When replacing a battery, determine if it is **internal or external** first. If the battery is external, remove the battery pack and replace it with a new one. If the battery is internal, remove the bottom cover, locate the battery, disconnect it from the motherboard, and remove any screws holding it in place, then remove the old battery, insert the new battery, and replace the screws and back cover.

Keyboard/Keys - The keyboard on a laptop is **typically smaller** than a traditional desktop keyboard. Laptop keyboards are located in the lower portion of the clamshell and can be either simple to remove in order to access the peripherals below or more involved and may entail removing numerous components to access the keyboard.

Random-Access Memory (RAM) - The industry-standard form factor for RAM in laptops is the **small outline inline memory module (SODIMM)**. When replacing a SODIMM, ensure that the SODIMM is compatible with the motherboard. SODIMMs can be 200-pin DDR and DDR2, 204-pin DDR3, 260-pin DDR4, or 262-pin DDR5, and they can be 32-bit or 64-bit configurations. The RAM is located in the bottom of the clamshell.

Hard Disk Drive (HDD)/Solid State Drive (SSD) Migration - After HDD or SSD replacement, data stored on the old drive may need to be migrated to the new drive. Migration can be done either **manually** or through the use of **migration software**. Manual migration is typically preferable when only user data needs to be migrated. Before replacement, move all data to a separate location, such as the cloud or external device, and copy the data to the new drive once installed. Manual migration does not move user settings or configurations. Migration software can be used to move files, settings configurations, and applications from one drive to another. Typically, **both drives need to be accessible** for migration software to work.

HDD/SSD Replacement - HDDs and SSDs for laptops come in **three possible form factors**: 2.5", 1.8", or M.2. Most laptops use SSDs to save space and most laptops have a single cable connecting the drive to the laptop, providing both data and power to the drive. The drive will be located in the bottom of the clamshell. Remove the bottom cover, locate the drive, remove any screws (between one and four, typically), disconnect the SATA cable, and replace.

Wireless Cards - The wireless **network interface card (NIC)** allows for wireless communication between the laptop and wireless access points. The wireless NIC is located in the bottom of the clamshell. Remove the bottom cover, remove the screw holding the wireless NIC in place, disconnect the two antenna wires, and pull straight out of the M.2 socket. Replace by reversing the procedure.

Physical Privacy and Security Components - Physical privacy and security components are designed to prevent the loss of information through physical means such as shoulder surfing or theft.

Biometrics - Biometrics is the use of a **physical body part** to enhance security. Commonly used biometrics are **facial recognition** or a **fingerprint scanner** with older models. Biometrics can also be added to a laptop as a peripheral device via a USB port.

Near-Field Scanner Features - (NFC) is a wireless communication method that sends signals between compatible devices in close proximity, up to 10 cm, to another NFC compatible device. NFC scanners are often used for wireless payments and can be intercepted by malicious devices in close proximity. Be aware of surroundings and suspicious electronic devices when using NFC.

Mobile Device Components - perform the same functions as desktop components and control input and output, processing, storage, display, and connection capabilities. *Note:* You must be able to **compare and contrast** mobile device components for the exam.

Types

There are **two primary types** of mobile display units: liquid crystal display and organic light-emitting diode.

Liquid Crystal Display (LCD)

LCD is a display technology that uses a current passed through a semi-crystalline liquid to produce images. The liquid crystals do not produce light and require a light source, the backlight, to display the image. *Note:* If a device states that it is LED, it uses LCD technology with an LED backlight. There are **three popular variants** of LCDs: IPS, TN, and VA, all of which use liquid crystals and transistors to form patterns in different ways.

In-plane switching (IPS)— offers the widest viewing angle and the best color reproduction. Ideal for vertical mounting and those needing high-quality color, such as graphic and video artists.

Twisted nematic (TN)— oldest of the LCD technologies, has limited viewing angles and washed out or blended color reproduction. Minimal lag time makes them ideal for competitive gamers , are an inexpensive option for office use.

Vertical alignment (VA)— offers the best contrast ratio of the three technologies and is a solid middle ground choice with decent color reproduction and only a slight lag.

Organic Light-Emitting Diode (OLED) - displays contain both the image-producing components and the light source in a **single panel**. An organic light-emitting compound is sandwiched between an anode and a cathode which produces a current. The current runs through the electroluminescent compound producing light. The structure of OLEDs allows them to be flexible for curved displays. **Power consumption** with an OLED is less than with an LCD, and the **contrast ratio** is higher, producing sharper images. OLED is popular in high-end monitors and smaller devices such as smartphones.

Mobile Display Components - Besides the display unit, mobile device components contained in the top part of the clamshell include the backlight (for LCDs), the inverter (for LCDs), the screen (LCD or OLED), the digitizer (if applicable), the webcam, the microphone, and the Wi-Fi antenna.

Wi-Fi Antenna Connector/Placement - Almost all laptops today include 802.11, or wireless, functionality. The Wi-Fi antenna is generally located in the top of the clamshell case so as to place the antenna higher up for better signal reception. The antenna will be connected to the motherboard by running the wire from the top of the clamshell, through the hinge, and into the bottom of the clamshell to the motherboard.

Camera/Webcam - The most common placement for a webcam or camera is in the center at the top of the clamshell above the display. Most laptops also include a built-in light next to the webcam to illuminate the user.

Microphone - The microphone can be placed either next to the webcam and light in the top of the clamshell, or in the bottom of the clamshell, depending on the model of the laptop.

Touch Screen/Digitizer - A digitizer is a device that takes analog input in the form of written or drawn content, such as by a finger or stylus, and converts it into digital images. The digitizer, commonly called a touchscreen, can be **built into** the display as the top glass sheet or as an **overlay** for the display screen.

Inverter - An inverter is a small circuit board located behind an LCD panel that turns DC current into the AC current which is needed by the backlight of the LCD display. Flickering screens and dimness are common signs of inverter malfunction.

Mobile Device Accessories and Ports - allow for **enhanced user interaction** with a mobile device and include touch pens, headsets, speakers, webcams, trackpads/drawing pads, docking stations, and port replicators. *Note:* You must be able to **set up and configure** these accessories based on given scenarios.

Connection Methods - vary by device but may include all of the same connection methods as desktop devices.

Universal Serial Bus (USB)/USB-C/Micro USB/Mini USB - USB is the **most common type** of connection and can be in any USB form factor, including USB-C, micro USB, or mini USB.

Lightning - connection is **proprietary to Apple products** and is usually the only connection type on iPhones and iPads. Macs and MacBooks can also have lightning ports for device charging.

Serial Interface - is a peripheral device that is placed between two devices, such as a type of plug, that allows for data transfer serially in smaller bits between the devices. Serial interfaces include USBs, Thunderbolt, and HDMI connections. Common serial connection accessories include displays, external hard drives, and input/output devices.

Near-Field Communication (NFC) - is a wireless connection type with a **very short range** and is primarily used in mobile commerce, RFID tags, or wireless accessories.

Bluetooth - is a wireless connection method primarily used for the connection of headsets, speakers, and input devices. Bluetooth has a **limited range**.

Hotspot - is a wireless connection type that allows for connection to the internet through a wireless access point, typically used for **public connection** in places such as libraries and restaurants.

Accessories - for mobile devices are numerous and include input/output tools, security devices, communication enablers, and mobile commerce endpoints.
Touch Pens - or stylus, is a pen-shaped accessory used as a writing implement or pointing device that acts as an input device allowing for **freeform writing, drawing, or clicking**.
Headset - is an audio input/output device that typically uses a USB or audio jack for connection. Most laptops will automatically detect and configure a headset when it is connected to the mobile device.
Speakers - are audio output devices that connect by USB or audio jack and configure automatically upon connection.
Webcam - A **peripheral web camera** can be connected to a mobile device via a USB port and will typically configure automatically upon connection.
Docking Station - is a laptop peripheral that allows for the connection of a compatible laptop to an **increased bank of expansion capabilities**, additional ports, full-sized drive bays, expansion bus slots, optical drives, memory card slots.
Port Replicator - is a laptop peripheral device that allows for the connection of a compatible laptop to additional ports, such as the ones found on the mobile device itself, and can be used to connect a keyboard, mouse, or printer. The port replicator allows for the **continual connection** of these peripheral devices, which can be used when the mobile device is connected to the port replicator.
Trackpad/Drawing Pad - is used in conjunction with a touch pen and is connected via USB. A trackpad/drawing pad is a larger version of the built-in trackpad on a laptop and offers additional features, such as on-pad menu management.
Mobile Device Network Connectivity and Application Support - Application support is provided through network connectivity. *Note:* You must be able to **configure** mobile connectivity methods through provided scenarios.
Wireless/Cellular Data Network - is the largest and farthest-reaching wireless connection method. Enabling and disabling wireless connectivity options via the settings page and can be toggled on/off on both Android and iOS devices.

- **2G**, or 2nd generation, has a max data rate of 64 Kbps with limited network range.
- **3G** sets the data rate standard at 200 Kbps. Both 2G and 3G use traditional telephone circuits.
- **4G** uses IP instead of traditional telephone circuits and comes in two varieties, WiMax and Long-Term Evolution (LTE). It offers a higher range and faster download and upload speeds.
- **5G** was announced in 2016 and implemented in 2018. 5G has three classifications: enhanced mobile broadband (eMBB) for cell phone and mobile communication, ultra-reliable low-latency communications (URLLC) for autonomous vehicles and industrial applications, and massive machine-type communications (mMTC) for sensors supporting Internet of Things (IoT) devices.

Hotspot - is a wireless connection method that allows for a **shared cellular internet connection** with Wi-Fi-capable devices. To enable the hotspot on an iOS device, go to Settings, then Personal Hotspot, and slide toggle to *On*. To enable a hotspot on an Android device, go to Settings, Connections, Mobile Hotspot, then Tethering, and toggle to *On*.
Global System for Mobile Communication (GSM) vs. Code-Division Multiple Access (CDMA) -) were both **cellular connection standards** used with **3G** technology and were incompatible with one another. GSM was used by AT&T and T-Mobile and was initially slower than CDMA, which was used by Sprint and Verizon. These standards are no longer in use after the technology advanced to 4G.
Preferred Roaming List (PRL) Updates - updates are updates to the reference guide used by mobile phones to connect to the appropriate cell phone tower when roaming and typically update with phone updates.
Bluetooth - The IEEE 802.15 standard specifies criteria for wireless personal area networks (WPAN) that use Bluetooth for data-link transport. It also allows for paired devices to exchange and synchronize data over a Bluetooth connection. The CompTIA A+ exam content lists five steps for Bluetooth pairing.
Step 1: Enable Bluetooth - can be enabled on a device by toggling the Bluetooth connection to *On*. To connect, both the host and the receiving device must be enabled. On a Windows device, enable Bluetooth by going to Settings, Devices, then Bluetooth and Other Devices, and toggling to *On*. On an Android device, go to Settings, Connections, then Bluetooth, and toggle to *On*. On an iOS device, go to Settings, then Bluetooth, and toggle to *On*.
Step 2: Enable Pairing - The toggle will appear once Bluetooth is on.
Step 3: Find Device for Pairing - When Bluetooth pairing is enabled, it will locate any pairable Bluetooth devices within its range. The pairable devices will be listed. Choose the appropriate one.
Step 4: Enter the Appropriate PIN Code - When pairing a Bluetooth device, a generated code will typically be displayed for first-time pairing. Enter the appropriate code to link the two devices.
Step 5: Test Connectivity - Once the two devices are paired using Bluetooth, ensure connectivity by testing the connection through data transmission, such as an audio or file transfer.

Location Services - are used to identify device positioning and location and include GPS and cellular location services. Location services can be configured on all mobile devices. To configure location services on an iOS device, go to Settings, Privacy, then Location Services, and toggle to *On*. To configure location services on an Android device, go to Settings, then Location, and toggle to *On*. Individual applications have location services options, as well, with varying permissions.
Global Positioning System (GPS) Service - is a **satellite-based** navigation system that can provide current location and tracking for enabled devices using **triangulation** between receivers and satellites. GPS uses **three primary components**: the satellite constellation, the ground control network, and the receiver.
Cellular Location Service - also use triangulation to determine location, but they **use cellular towers** instead of satellites to triangulate a receiver's location. Cellular location services are **carrier-based** and are limited to within the range of cellular towers.
Mobile Device Management (MDM)/Mobile Application Management (MAM) - are used to help companies ensure mobile device security. MDM is a software package used to enroll corporate devices for oversight and security. MDM allows for the implementation of security policies on all enrolled devices and offers the ability to remotely track, lock, unlock, encrypt, and wipe mobile devices. MAM is software designed to ensure the security of software on an enrolled mobile device. MAM allows for the remote installation, deletion, encryption, and wipe of corporate applications and related data on an enrolled device.
Corporate Email Configuration - connects mobile devices to allow email access to corporate email accounts and can be done through either a commercial provider, such as Gmail, or through a corporate or ISB-based email service. To configure a mobile device to connect to a commercial provider, only the email address and password are usually needed.

- To configure an email account on an **iOS device**, go to Settings, Mail, then Accounts, and choose *Add Account*. If the account provider is listed, click the provider and provide the proper credentials. If the provider is not listed, click Other, then Add Account. Add the name, email, password, and description, and click *Next*. Choose IMAP or POP protocol. Configure incoming and outgoing mail server names and click *Next*. Verify the username and password and click *Save*.
- To configure an email account using an **Android device**, go to Settings, Accounts and Backup, then Manage Accounts, and choose *Add Account*. Choose the account type (IMAP, SMTP, or POP), enter the email address and password, and click *Next*. A validation screen will appear. Click *Next* to validate.

Two-Factor Authentication - increases device security by requiring an **additional piece of information for access**, such as a PIN from a token or authentication application.
Corporate Applications - should be enrolled in a MAM, with all accessing devices enrolled for remote install, wipe, lock, and unlock capabilities.
Mobile Device Synchronization - is the process of mirroring all unique changes and additions from one device to another. Synchronization **allows a mobile device to be an extension** of a primary computing device. Synchronization can occur via wired connection, Wi-Fi, Bluetooth, or cellular connection.
Account Setup - Account synchronization setup varies depending on the device and operating system used.
Microsoft 365—is a **subscription service** that offers access to the Microsoft Office Suite of programs and storage space in Microsoft Cloud. To synchronize Microsoft 365 accounts, go to Start, Settings, Accounts, then Sync Your Settings, and toggle to *On*. This will sync all devices logged in using that particular user credential.
Google Workspace— **Android devices** often use Google Drive and Google Workspace for synchronization. To sync an Android device, go to Settings, Accounts and Backup, then Backup Data, and toggle to *On*.
iCloud—iCloud is **Apple's version of the cloud** and uses the user's **Apple ID** for access. To activate iCloud sync, go to Settings, Apple ID, then iCloud, and toggle to *On* for synchronization or backups.
Data to Synchronize - All utilities typically synchronize the most common types of data, including contacts, applications, email, pictures, music, videos, calendar, bookmarks, documents, location data, social media data, e-books, passwords.
Mail—Email is synchronized between connected devices to ensure access via all connected devices.
Photos—Photos are commonly synchronized across connected devices.
Calendar—Calendars are synchronized across connected devices and may even synchronize with additional applications and programs to ensure continuity.
Contacts—unless otherwise specified, are synchronized across connected devices.
Recognizing Data Caps—A data cap is a **limit placed on the amount of data** that can be stored in a synchronization location such as a cloud. Data caps are dependent upon the provider and the usage contract of the user. Managing data to stay within the specified data cap is vital to ensure continuity of synchronization.