Chapter 8: Mobile Devices

IT Essentials: PC Hardware and Software v5.0

Cisco Networking Academy®
Mind Wide Open™

Chapter 8 Objectives

- 8.0 Describe mobile devices
- 8.1 Identify mobile device hardware and that most parts are not field replaceable
- 8.2 Compare and contrast Android and iOS mobile operating systems
- 8.3 Explain how to configure network and email connectivity on mobile devices.
- 8.4 Identify methods for securing mobile devices
- 8.5 Describe how to troubleshoot mobile devices

Mobile Devices

- A mobile device is any device that is hand-held, light, and typically uses a touchscreen for input.
- Mobile devices use an operating system to run applications (apps), games, and play movies and music
- Examples are - Android devices, such as the Samsung Galaxy tablet and Galaxy Nexus smartphone, and the Apple iPad and iPhone.
- Many mobile device components, operating systems, and software are proprietary so It is important to become familiar with as many different mobile devices as possible.

Non-Field Serviceable Parts

- Mobile devices do not have field-serviceable parts.
- Broken devices usually sent to the manufacturer for repair or replacement.
- Installing parts from sources other than the manufacturer voids the manufacturer's warranty and might harm the device.
- There are a few mobile device parts that are field-replaceable:
  - **Battery**
  - **Memory card**
  - **Subscriber Identity Module (SIM) card**

Non-Upgradeable Hardware

- Mobile device hardware is typically not upgradeable.
- Many of the components in a mobile device are connected directly to circuit boards.
- Batteries and memory cards, however, can often be replaced with items that have larger capacities.
- Some functionality can be added to mobile devices through the use of built-in ports and docking stations.

Touchscreens

- Most mobile devices use **touchscreens** to allow users to physically interact with the screen and type on a virtual keyboard.
- Two types of touchscreens:
  - **Capacitive -** Consists of a glass screen coated with a conductor. Touching the screen interrupts the electrical field of the screen. This change is how the touch processor calculates location.
  - **Resistive -** Consists of transparent layers of material capable of conducting electricity. Pressure causes the layers to touch and interrupt the electricity. This is how the touch processor calculates location.
- **Multi-touch** - the ability to recognize when two or more points of contact are made on the screen.

Solid State Drives (SSDs)

- The circuit board, flash memory chips, and memory controller in SSDs are installed directly inside the mobile device.
- Advantages of using Flash memory storage (SSD):
  - **Power efficiency** - requires very little power to store and retrieve data.
  - **Reliability** - can withstand high levels of shock, vibration, heat and cold.
  - **Lightweight and Compact**
  - **Performance** – no moving parts, therefore no spin-up time for platters or drive head to move.
  - **Noise** – very quiet..

Android versus iOS

- Android
  - Developed by Google in 2008.
  - Open source- public can change, copy, or redistribute the code without paying royalty fees to the software developer.
- iOS
  - Released by Apple in 2007.
  - Closed source -source code is not released to the public.

Android GUI

iOS GUI

Application and Content Sources

- Some apps can be downloaded free and others must be purchased. Free apps are often loaded with advertisements to help pay for development costs.
- It is important to install apps only from trusted sources.
- Two main methods for installing content on mobile devices: **Push and Pull**
  - When user runs Google Play app or the Apple App Store app content that is downloaded is **Pulled** from a server to their device.
  - When user purchases app on their laptop or desktop and then it is **Pushed** to their android or iOS device.
- **Note**: Read the list of permissions carefully and do not install apps that request permission to access items and features that it should not need.

Home Screen Items (Android)

- Mobile devices organize icons and widgets on multiple screens for easy access.
- Android OS uses the system bar, displayed on the bottom of the screen, to navigate apps and screens.
- HTC designed the **TouchFLO** interface over Android for its phones which has now been replaced by HTC Sense.

Managing Apps, Widgets and Folders

- **Apps** - Each home screen is set up with a grid where apps can be placed.
- **Widgets** are programs (or pieces of programs) that display information
- **Folders** - On some mobile devices, multiple apps can be grouped into folders to help organize them

iOS Touch Interface

- iOS interface works in much the same way as the Android interface. Home screens are used to organize apps and apps are launched with a touch.
  - **Note:** iOS does **not** have navigation icons, widgets or app shortcuts.
- **Home button** performs many of the same functions as the Android navigation buttons:
  - Wake the device, Return to the home screen, Return to the main home screen, Open the multitasking bar, Start Siri or voice control, Open audio controls, Open the search screen.
- **Notification Center -** displays all of the alerts from apps in one location.

Managing Apps and Folders

- **Apps** - all the apps installed on the device are located on the home screens.
  - Many apps use an **alert badge** which is displayed as a small icon over an app. For example, number of missed calls.
  - An alert badge with exclamation point indicates a problem with the app.
- **Multitasking Bar -** iOS allows multiple apps to run at the same time.
- **Folders -** can be created on iOS devices to help organize them.

Common Mobile Device Features

- **Screen Orientation** - Portrait and landscape
  - Auto rotation-Content is automatically rotated to the position of the device, either landscape or portrait.
- **Screen Calibration** -Adjusting the brightness of the screen
- **Global Positioning System (GPS) –**A GPS radio receiver uses at least four satellites to calculate position. Uses in mobile devices:
  - **Navigation** - A mapping app that provides turn-by-turn directions
  - **Geocaching** - App that shows the location of geocaches - hidden containers around the world.
  - **Geotagging** - Embeds location information into a digital object, like a photograph or a video, to record where it was taken.
  - **Device tracking** - Locates the device on a map if it is lost or stolen.

Wireless Data Network

- Mobile devices are widely used and becoming more powerful.
- Mobile devices using wireless networks can perform many tasks that previously needed computers connected to a physical network.
- Connect to Wi-Fi networks when possible because data used over Wi-Fi does not count against the cellular data plan.
  - Connecting to Wi-Fi networks conserves battery power.
- Protect Wi-Fi communications on mobile devices:
  - Never send login or password information using clear, unencrypted text.
  - Use a VPN connection when possible.
  - Enable security on home networks.
  - Use WPA2 security.

Cellular Communications

- **1G** - First-generation phones primarily used analog standards, including Advanced Mobile Phone System (AMPS) and Nordic Mobile Telephone (NMT).
- **2G**- Second-generation cell phones switched from analog to digital standards. Standards included Global System for Mobile (GSM), Integrated Digital Enhanced Network (iDEN), and Code Division Multiple Access (CDMA).
- **2.5G** - As 3G cell phone standards were being developed, extensions to the existing 2G standards were added.
- **3G** - Third-generation standards enable cell phones to send and receive text, photos, video, access the Internet and use the Global Positioning System (GPS).
- **4G** - Fourth-generation standards provide ultra-broadband Internet access, allowing users to download files much faster, video conference and watch hi- definition television. Standards include Mobile WiMAX and Long Term Evolution (LTE).

Bluetooth for Mobile Devices

- Bluetooth technology provides a simple way for mobile devices to connect to each other and to wireless accessories.
  - Wireless, automatic, and uses very little power.
  - Up to eight Bluetooth devices can be connected together at any one time.
- How mobile devices use Bluetooth:
  - Hands free headset, Keyboard or mouse, Stereo control,

  Car speakerphone.
  - **Tethering –** connecting to another mobile device or computer to share a network connection.

Bluetooth Pairing

- **Bluetooth Pairing -** two Bluetooth devices establish a connection to share resources.
- Pairing process:
  - Both devices on.
  - One device searches for other devices.
  - Other device must be in discoverable (visible) mode.
  - PIN may be requested to authenticate the pairing process.
  - PIN is stored after initial pairing, so it does not have to be entered the next time the device tries to connect.

Introduction to Email

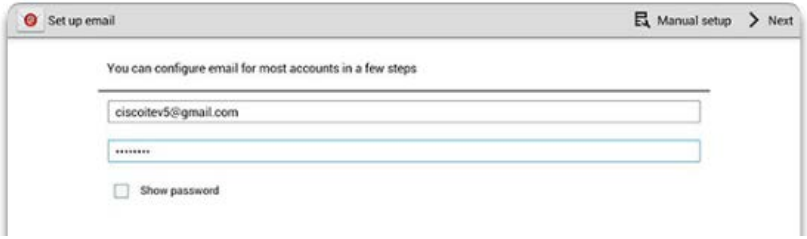
- **Information needed to set up an email account:**
  - Display name, email address, protocol used by incoming mail server, incoming and outgoing server names, username, account password.
- **Protocols used in email:**
  - **Post Office Protocol Version 3 (POP3)** retrieves email from remote server, does not leave copy of email on server.
  - **Internet Message Access Protocol (IMAP)** allows local email clients to retrieve email from a server, leaves original email on server.
  - **Simple Mail Transfer Protocol (SMTP)** is a simple, text-based protocol that transmits emails.
  - **Multipurpose Internet Mail Extensions (MIME)** is normally used in conjunction with SMTP to extend the email format to include pictures and word processor documents.

Configuring Email

Android

- Use the Google account sign-in page to create a new Gmail account.
- Android devices also have an email app for connecting to other email accounts.

Android Gmail Setup



iOS

- The iOS Setup Assistant guides you through the process of connecting the device, creating an Apple ID, and creating an iCloud email account.

iOS email Setup

Data Synchronization

- Data synchronization is the exchange of data between two or more devices, while maintaining consistent data on those devices.
- Types of data that are typically synchronized:
  - Contacts
  - Email
  - Calendar entries
  - Pictures
  - Music
  - Apps
  - Video
  - Browser links and settings

Application Installation Software

- Synchronization of data on an iOS device requires installation of iTunes
  - iTunes is a media player application that downloads, plays, and organizes content for use with iOS devices and computer.
  - iTunes manages iOS devices by activating them and restoring if there is a malfunction.
  - iTunes is used to upgrade the iOS.
- Synchronization of data on an Android device requires no application.
  - Automatic synchronization with Google is accessed by selecting **Settings > Personal > Accounts & sync**

Synchronization Connection Types

- USB and Wi-Fi connections are the most common connection types used to synchronize data between devices.
  - Android users often sync with Google's different web services, even when synchronizing with a desktop or laptop computer.
  - iOS 5 allows the use of Wi-Fi Sync to synchronize with iTunes wirelessly.
- **Cross-Platform Data Synchronization -** Synchronization of data between different operating systems require:
  - Third-party applications that can synchronize between Outlook and iTunes
  - Applications such as Dropbox

Passcode Locks

- **A Passcode Lock secures a device and puts it in a power-saving state.**
  - The passcode must be entered each time the device is turned on or resumes from a power-saving state.
- **Common types of passcode locks:**
  - **None** - Removes any other type of passcode if one is set.
  - **Slide -** User slides an icon, such as a lock or arrow. Least secure.
  - **Face Unlock -** Unlocks when a face is recognized.
  - **Pattern –** Locks and unlocks the device when the user slides a finger over the screen in a certain pattern.
  - **PIN –** Use a PIN number or code to unlock.
  - **Password –** Can be most secure.
  - **Simple Passcode** – iOS devices only. When option ON –passcode is a 4 digit number. When option Off more complex passwords can be used.

Restrictions on Failed Login Attempts

- iOS devices - the device is disabled after five failed attempts.
  - On the sixth failed attempt, the device remains disabled for 1 minute.
  - Each failed attempt after six results in additional waiting time.
  - For extra security, the **Erase all data on this device after 10 failed passcode attempts** option can be used.
  - To restore, connect device to the computer to which it was last synchronized and use the **Restore** option in iTunes.
- **Android Devices** - the number of failed attempts before lockout depends on the device and version of the Android OS.
  - After a device is locked, it can be unlocked by entering the Gmail account information used to set up the device.

Cloud Enabled Services for Smart Devices

- **Remote Backup**
  - iOS users are given 5 GB of storage free on iCloud.
  - Android device users have Calendar, Mail and Contacts automatically backed up.
- **Locator Applications -** Many different apps available for remotely locating a device:
  - iOS most often used is **Find My iPhone** app.
  - Uses cell towers, Wi-Fi hotspotss and GPS to locate the device.
- **Remote Lock -** allows remote locking of device with a passcode.
- **Remote Wipe -** deletes all data from the device and returns it to a factory state.

Antivirus

- **Antivirus apps are available for both Android and iOS**
  - Depending on the permissions set up when installed on an Android device, the antivirus app might not be able to scan files automatically or run scheduled scans. Must be initiated manually in those cases.
  - iOS never allows automatic or scheduled scans as a safety feature to prevent malicious programs from using unauthorized resources. Must be initiated manually.
- **Rooting (Android)and Jailbreaking (iOS) -** Unlocking the bootloader so that a custom OS can be installed.
  - Voids the manufacturers warranty.
  - Opens the device up to malicious programs or virus infection.

Patching and Updating Operating Systems

- **Updates** add functionality or increase performance.
- **Patches** can fix security problems or issues with hardware and software.
- Android updates and patches use an automated process for delivery.
  - When a carrier or manufacturer has an update for a device, it shows up as a notification on the device that an update is ready.
- iOS updates also use an automated process for delivery.
  - To check for updates to iOS, connect the device to iTunes.

Basic Troubleshooting Process for Mobile Devices

- Check to make sure the device is under warranty.
- If yes, it can often be returned to the place of purchase for an exchange.
- If no, compare the cost of the repair with the replacement cost of the mobile device.
- Mobile devices change rapidly in design and functionality, so they are often more expensive to repair than to replace.

Troubleshooting Process

Step 1 Identify the problem

Step 2 Establish a theory of probable causes

Step 3 Test the Theory to Determine cause

Step 4 Establish a Plan of Action to Resolve the Problem and Implement the Solution

Step 5 Verify Full System Functionality and Implement Preventative Measures

Step 6 Document Findings, Actions, and Outcomes

Step 1 - Identify the Problem

Open-ended Questions	• What is the problem you are experiencing? • What is the make and model of your mobile device? • What service provider do you have? • What apps have you installed recently?
Closed-ended Questions	• Has this problem happened before? • Has anyone else used the mobile device? • Is your mobile device under warranty? • Have you modified the operating system the mobile device? • Have you installed any apps from an unapproved source? • Does the mobile device connect to the Internet?

Step 2 - Establish a Theory of Probable Causes

Common causes of mobile device problems	• The Power button is broken. • The Battery can no longer hold a charge. • The mobile device cannot send or receive email. • There is excessive dirt in the speaker,microphone,or charging port. • The mobile device has been dropped. • The mobile device has been submerged. • An app has stopped working. • A malicious app has been sideloaded. • The mobile device has frozen. • Mobile device software or apps are not up to date. • A user has forgotten their passcode.

Step 3 - Test the Theory to Determine cause

Common steps to determine cause	• Force a running app to close. • Reconfigure email account settings. • Restart the mobile device. • Plug the mobile device into an AC outlet. • Replace the mobile device battery. • Reset the mobile device to factory defaults. • Restore the mobile device from a backup. • Remove any removable battery and reinstall it. • Connect an iOS device to iTunes. • Clean the speaker, microphone, charging port, or other connection ports. • Update the mobile device software and apps.

Step 4 - Establish a Plan of Action to Resolve the Problem and Implement the Solution

If no solution is achieved in the previous step, further research is needed to implement the solution.	• Helpdesk Repair Logs • Other Technicians • Manufacturer FAQs • Technical Websites • Device Manual • Online Forums • Internet search

Step 5 - Verify Full System Functionality and Implement Preventative Measures

Verify full system functionality and if applicable implement preventive measures	• Reboot the mobile device. • Browse the Internet using Wi-Fi. • Browse the Internet using 4G, 3G, or another carrier network type. • Make a phone call. • Send a text message. • Open different types of apps. • Operate the mobile device using only the battery.

Step 6 - Document Findings, Actions, and Outcomes

- Discuss the solution with the customer.
- Have the customer confirm that the problem has been solved.
- Give the customer all appropriate paperwork.
- Document the process in the work order and in your technician's journal:
  - Problem description
  - Solution
  - Components used
  - Amount of time spent in solving the problem

Common Problems and Solutions

- Many mobile device problems can be solved by simply turning off the device and turning it back on. When a mobile device does not respond to a reboot, a reset may need to be performed.
- **Android devices reset:**
  - Hold down the **power** button until the mobile device turns off. Turn the device on again.
  - Hold down the **power** button and the **volume down** button until the mobile device turns off. Turn the device on again.
  - Factory reset **Settings > Backup and reset > Factory data reset > Reset device**
- **iOS devices reset:**
  - Press and hold both the **Sleep/Wake** button and the **Home** button for 10 seconds, until the Apple logo appears.
  - Factory reset **Settings > General > Reset > Erase All Content and Settings**
- **See chart of Common Problems and Solutions in Curriculum**

Chapter 8 Summary

This chapter introduced mobile devices and the following important concepts about mobile devices:

- Mobile device hardware has few field-repairable units.
- Mobile devices are often replaced instead of repaired due to the high cost of repairs.
- Mobile devices often contain proprietary parts that cannot be interchanged.
- Touchscreens are used instead of other input devices, such as mice and keyboards.
- SSDs are used in mobile devices because of their size, energy efficiency, and lack of noise.
- Open source software can be modified by anyone with little or no cost.

Chapter 8 Summary

- Use only trusted content sources to avoid malware and unreliable content.
- Both Android and iOS have similar GUIs for using apps and other content.
- Mobile devices use sensors, such as GPS and accelerometers, to enhance their functionality.
- Network connections for mobile devices are made with cellular, Wi-Fi, and Bluetooth connections.
- Email accounts are closely tied to mobile devices and provide many different data synchronization services.
- Android devices use apps to synchronize data not automatically synchronized by Google.
- iOS devices use iTunes to synchronize data and other content.

Chapter 8 Summary

- Passcode locks secure mobile devices.
- Remote backups can be performed to backup mobile device data to the Cloud.
- Remote lock or remote wipe are features to secure a mobile device that has been lost or stolen.
- Antivirus software is often used on mobile devices to prevent the transfer of malicious programs to other devices or computers.