Chapter 10: Mobile, Linux, and OS X Operating Systems

IT Essentials v6.0

Cisco | Networking Academy®
Mind Wide Open™

Chapter 10 - Sections & Objectives

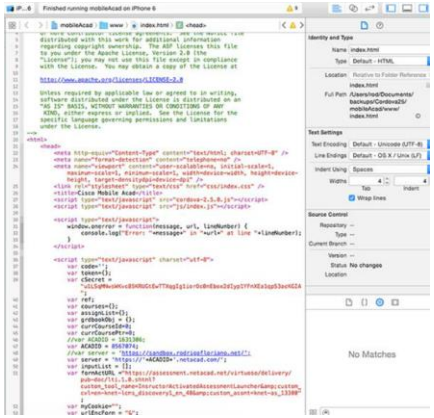
- 10.1 Mobile Operating Systems
  - Explain the purpose and characteristics of mobile operating systems.
- 10.2 Methods of Securing Mobile Devices
  - Explain methods for securing mobile devices.
- 10.3 Network Connectivity and Email
  - Explain how to configure network connectivity and email on mobile devices.
- 10.4 Linux and OS X Operating Systems
  - Explain the purpose and characteristics of Linux and OS X operating systems.
- 10.5 Basic Troubleshooting Process for mobile, Linux and OS X Operating Systems
  - Explain how to troubleshoot other operating systems.
- 10.6 Chapter Summary

10.1 Android Vs. iOS

Cisco | Networking Academy®
Mind Wide Open™

Android vs. iOS

- Open Source Vs. Closed Source
  - Open Source: the source code is provided with the compiled program.
  - Closed Source: the source code is not provided with the compiled program.
  - Android is open source while iOS is not.
- Mobile Application Development
  - Mobile operating systems became software platforms.
  - Apps are designed and developed to run on mobile OSs.
  - Apple and Google provide development tools to app developers.

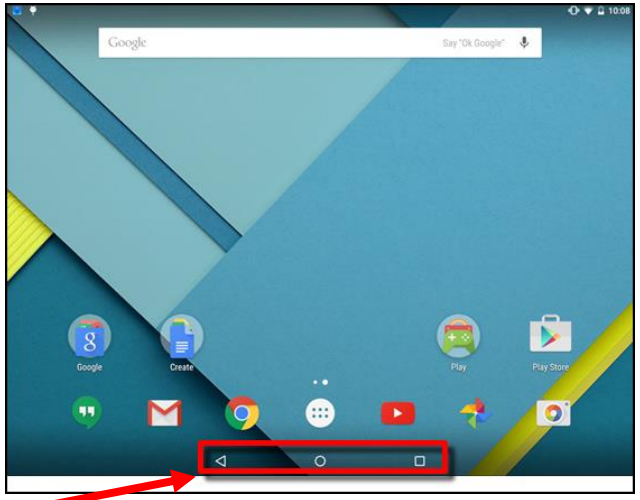


Android vs. iOS

- Application and Content Sources
  - Apps are essentially programs designed for mobile devices.
  - Mobile OS manufacturers usually maintain an online store where users can locate, download and install apps (Google Play).
  - Android users can also sideload apps.
  - Users of stock iOS must use the official App Store to install apps.
- Navigation
  - iOS has a physical Home button, but Android uses navigation icons.
  - In iOS, the icon for an app represents the app itself. Deleting the icon in iOS deletes the app. In Android, the icon on the Home screen is a shortcut to the app.

Android Touch Interface

- Home Screen Items
  - Android mobile devices organize icons and widgets on multiple screens.
  - Android's home screen elements include: Navigation Icons, Google Search, Special Enhancements and Notification and System Icons.
  - The format of the home screen is defined by the launcher.
- Managing Apps, Widgets and Folders
  - Apps are represented by icons and arranged in a grid.
  - In Android, home screen apps are simply a link; removing an app from the home screen does not uninstall it.
  - The user can customize the position of the apps.
  - Folders can also be created to group apps.
  - Widgets display information right on the home screen.



Android Screen

iOS Touch Interface

- Home Screen Items
  - iOS mobile devices organize icons on multiple screens.
  - iOS home screen has no navigation icons and no widgets.
  - iOS relies on a few UI elements, including: Home Button, Notification Center and Spotlight (search tool).
  - The format of the home screen in stock iOS is defined by Apple and cannot be changed by the user.
- Managing Apps and Folders
  - Apps are represented by icons and arranged in a grid.
  - In iOS, home screen apps are the actual app; removing an app
    from the home screen also uninstalls it.
  - The user can customize the position of the apps.
  - Folders can also be created to group apps.
  - There are no widgets on iOS.
  - The small number that appears on an app is an **alert badge** that indicates the number of items requiring attention for that app.

Windows Mobile Touch Interface

- Home Screen Items
  - Also referred to as Start.
  - Based on Tiles
  - Tiles are apps and can display information or allow interaction right on the home screen
  - No icons
  - Navigation icons include: Back, Windows Button and Search
- Managing Apps and Folders
  - Apps are represented by Tiles
  - Apps can be pinned to or unpinned from Start
  - Unpinning an app does not uninstall it
  - The user can customize the position of the apps
  - Tiles can also be resized
  - Folders can also be created to group apps
  - The digital/virtual assistant in Windows 8.1 is known as **Cortana**.

Common Mobile Device Features

- Screen Orientation and Calibration
  - Mobile devices can operate in portrait or landscape.
  - Sensors such as the accelerometer, allow the OS to detect movement and automatically adjust screen orientation.
  - The user can also adjust brightness to match ambient conditions.
- GPS
  - Modern mobile devices include a GPS receiver.
  - Uses include: navigation, geocaching, geotagging, tailored search results and device tracking.
- Convenience Features
  - These features are designed to make life easier.
  - These features include: Wi-Fi Calling, Mobile Payments and VPNs.
- Information Features
  - These features are designed to make access to information easier; they include: Virtual Assistant, Google Now and Emergency Notifications.

10.2 Methods for Securing Mobile Devices

Cisco | Networking Academy®
Mind Wide Open™

Passcode Locks

- Overview of Passcode Locks
  - Protects sensitive or private information.
  - Prevents unauthorized use of the device.
  - Types of Passcodes include: None, Swipe, Pattern, PIN, Password, Trusted Devices, Trusted Places, Trusted Face, Trusted Voice, On-body Detection and Touch ID.
- Restrictions on Failed Login Attempts
  - Prevents Passcode brute-force attacks.
  - Usually, the device is temporarily disabled after a certain number of failed unlocking attempts.
  - Different devices implement different restriction policies.

Cloud-Enabled Services for Mobile

- **Remote Backup**
  - Mobile devices can automatically back up user data to the cloud.
  - Different cloud backup options are available.
- **Locator Applications**
  - Extremely useful if the device is lost or stolen.
  - Locator apps allows the user to locate the device on a map.
  - Can use cellular towers and Wi-Fi hotspots to determine the position of the device.
- **Remote Lock and Remote Wipe**
  - Other options include: remotely lock the device, send alerts to the device, or remotely erase it.
- Doing a **factory reset** erases all user data and settings and erases all installed apps.
- Note: All these require the device to be powered on and connected to a network.

Software Security

- Antivirus
  - Mobile devices are also vulnerable to malicious software.
  - The sandbox limits the damage in mobile devices.
  - User data can still be stolen and PCs can be infected.
  - Mobile antivirus apps are available for iOS and Android.
  - There are techniques to grant full access to a mobile device's file system. The process is called Rooting on Android and Jailbreaking on iOS.
  - A Rooted/Jailbroken device will lose most (if not all) of the protection provided by sandboxing.
  - **Signature Files** contain sample code from known viruses and malware that is used by security software to identify malicious software.
- Patching and Updating Operating Systems
  - Updates add functionality or increase performance.
  - Patches can fix security problems or issues with hardware and software.
  - Both Android and iOS use an automated process for delivery.

Rooting or Jailbreaking

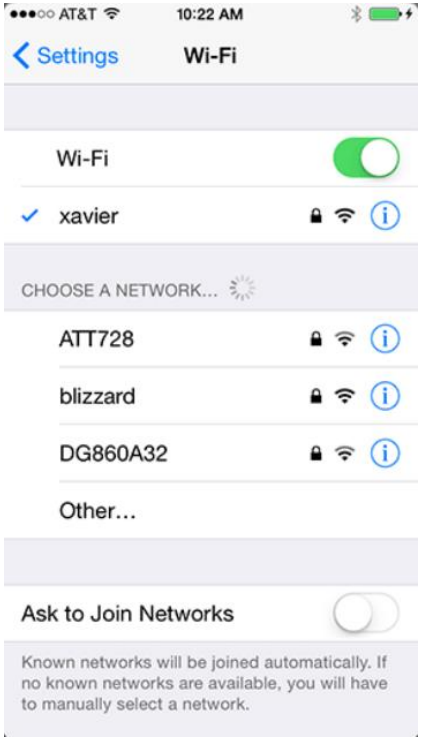
- Advantages:
  - The user interface can be extensively customized
  - The operating system can be fine-tuned to improve the speed of the device
  - Tethering
  - Unrestrictive apps
- Disadvantages:
  - Voids warranty
  - Susceptible to viruses
  - Security Risks
  - No system updates
  - Instability issues

10.3 Network Connectivity and Email

Cisco | Networking Academy®
Mind Wide Open™

Wireless and Cellular Data Network

- Wireless Data Network
  - Mobile devices can connect to the Internet via local Wi-Fi router.
  - Data transferred via local Wi-Fi router does not use the cellular carrier network and does not incur data charges to the user.
  - Coffee shops, libraries, schools, homes and work places are locations that usually provide free local Wi-Fi and Internet connections.
  - When the device roams out of the range of any Wi-Fi networks, it can connect to the cellular data network if this feature is enabled.
  - **Wi-Fi Calling** is a way to make mobile phone calls over a wireless data network
- Cellular Communications
  - Usually broken down into generations.
  - There are currently four cellular technology generations: 1G, 2G, 3G and 4G (mobile WiMax and LTE).
  - Cell phones that use a single standard can often only be used in specific geographic areas.



Bluetooth

- Bluetooth for Mobile Devices
  - Designed to connect devices in physical proximity to each other.
  - Bluetooth is wireless, automatic, and uses very little power.
  - Common Bluetooth devices include: headsets (hands-Free), keyboards, mice, car speakerphones and stereo controllers.
- Bluetooth Pairing
  - Term used to describe two Bluetooth devices establishing a connection to share resources.
  - The Bluetooth radios must be on.
  - One device must be set to scan for possible peers; the other must be set to advertise its presence (discoverable mode).
  - For security, a PIN may be required before the pairing can be completed.
- Tethering
  - connecting a mobile device to another mobile device or computer to share a network connection

Wireless Emergency Alerts

- WEA is a public safety system that allows customers who own certain wireless phones and other enabled mobile devices to receive geographically-targeted, text-like messages alerting them of imminent threats to safety in their area.
- Can save lives by sending emergency text messages to mobile phones.

Airplane Mode

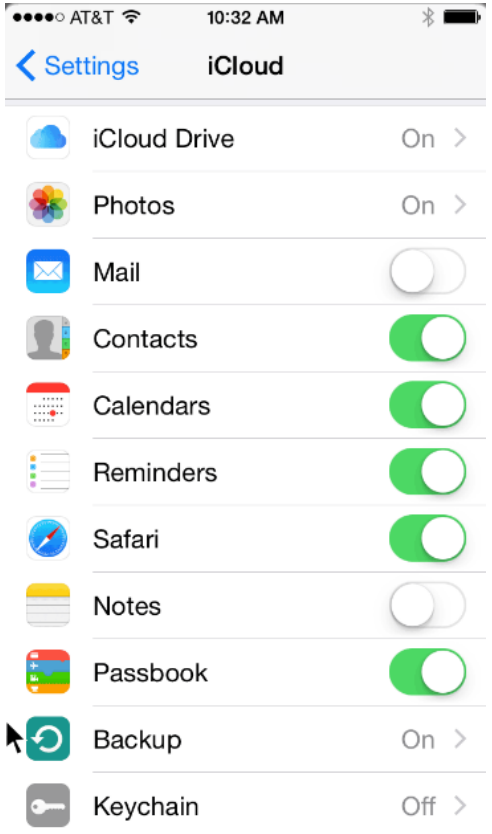
- **Airplane mode** is a setting on your phone that lets you turn off the cellular connection, Wi-Fi, FM radio, and Bluetooth on your phone simultaneously. This way you can use other apps (including ones that let you listen to music or watch videos that are on your phone) that don't require a cellular connection.

Configuring Email

- Introduction to Email
  - The email structure relies on servers and clients.
  - Email servers are responsible for forwarding email messages.
  - Users utilize email clients to compose, read and manage their messages.
  - While many different email clients exist for mobile devices, their configuration and operation is very similar.
- Android Email Configuration
  - Many of the advanced web services are powered by Google.
  - While Android relies on a Gmail account for many services, other email providers are also supported by the OS.
- iOS Email Configuration
  - iOS relies on an Apple ID for App Store access and other services.
  - iOS includes the Mail app which supports many different email accounts simultaneously.

Mobile Device Synchronization

- Internet Email
  - Usually provided through a web-based interface.
  - Some companies will also provide a mobile client app.
  - Mobile client apps usually present a better user experience than webmail on a mobile device.
- Types of Data to Synchronize
  - Data synchronization updates user data in multiple devices.
  - The types of data that can be synchronized include: Contacts, Email, Calendar Entries, Pictures, Music, Apps, Video, Browser Links and Browser Settings.
- Synchronization Connection Type
  - The most common connection types for syncing are USB and Wi-Fi.
  - Android syncs user data to web services such as Gmail and Google Calendar.
  - iOS uses iTunes to sync user data to a storage location which can be local or remote.



Email Protocols

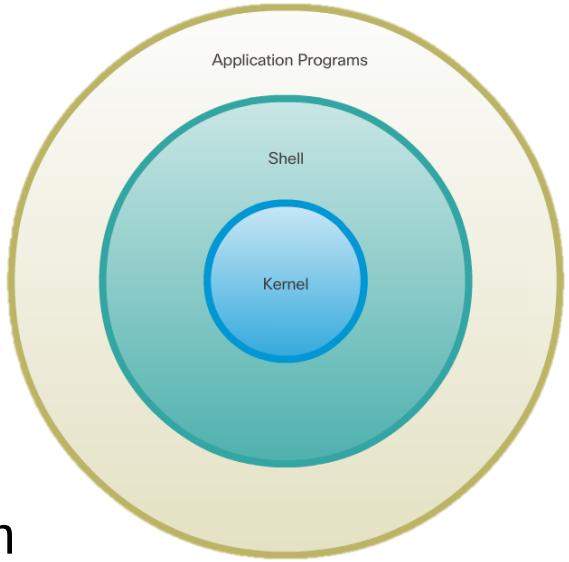
- **Post Office Protocol (POP3)** – A client/server protocol in which e-mail is received and held for you by your Internet server then download to your device. It is designed to delete mail on the server as soon as the user has downloaded it.
  - Uses port 110
- **Internet Messaging Address Protocol (IMAP)** – Used by Internet Mail applications. The user is able to keep the original email on the server, organize it into folders, and synchronize the folders between the mobile device and the server.
  - Uses port 143 or 993
- **Simple Mail Transfer Protocol (SMTP)** – Used for sending messages to a mail server or relaying to other servers.
  - Uses Port 25 or 465

10.4 Linux and OS X Operating Systems

Cisco | Networking Academy®
Mind Wide Open™

Linux and OS X Tools and Features

- Introduction to Linux and OS X Operating Systems
  - Linux and OS X are UNIX derivatives.
  - Both OSs kept most of the UNIX basic structure traits.
  - OS X 10.10 uses code name Yosemite
- Overview of Linux and OS X GUI
  - Modern versions of Ubuntu Linux include Unity.
  - Modern versions of OS X include Aqua.
  - Unity and Aqua GUIs have similar UI elements.
- Overview of Linux and OS X CLI
  - Due to their relation to UNIX, both Linux and OS X have similar CLI interfaces.
  - Text-based tools, the use of a *shell*, file system structure, file permissions and case-sensitivity are a few common characteristics inherited from UNIX and present in both OSs.

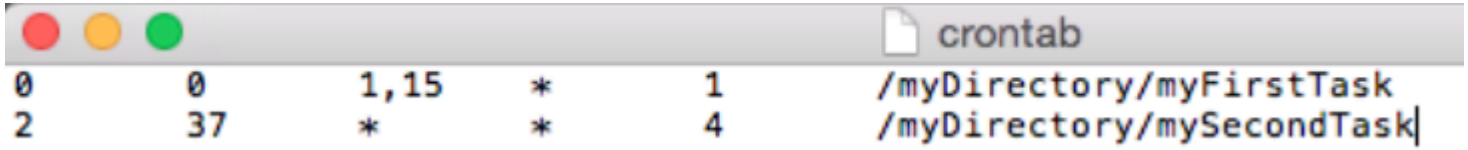


Linux and OS X Tools and Features (Cont.)

- Overview of Backup and Recovery
  - Allow backup and recovery of data using local, remote, or cloud storage in case of failure.
  - Déjà Dup is an easy and efficient tool for backing up data in Linux.
  - OS X users can use Time Machine, a very user-friendly and efficient backup tool.
  - Déjà Dup and Time Machine are also very similiar.
- Overview of Disk Utilities
  - Modern operating systems include disk tools to help troubleshoot and solve disk-related problems.
  - Most disk problems are the same regardless of the OS.
  - A good disk tool should be able to provide partition management, mount/unmount disk partitions, disk format, bad sector check and S.M.A.R.T. queries.
  - Disk tools include Disks (Linus) and Disk Utility (OSX).
  - To install and boot more than one OS, a boot manager is required
    - GRUB (Linus) and Boot Camp (OSX) are popular boot managers.

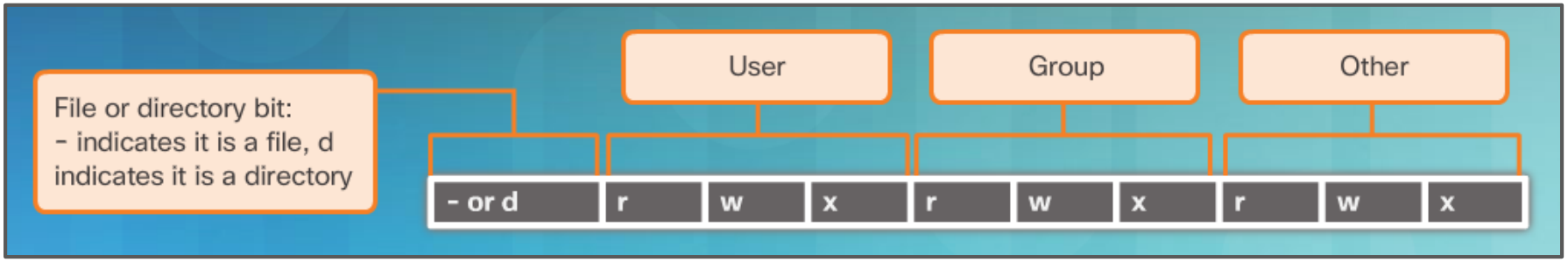
Linux and OS X Best Practices

- Scheduled Tasks
  - Maintenance tasks should be scheduled and performed frequently.
  - Computer systems can be programmed to perform tasks automatically.
  - Backups and Disk checks are two good examples.
  - The **cron** service runs in the background and can be used to schedule tasks in Linux and OS X.
- Security
  - Measures can and should be taken to prevent malicious software from getting in a mobile computer system.
  - Common measures include: operating system updates, firmware updates, antivirus, and antimalware.



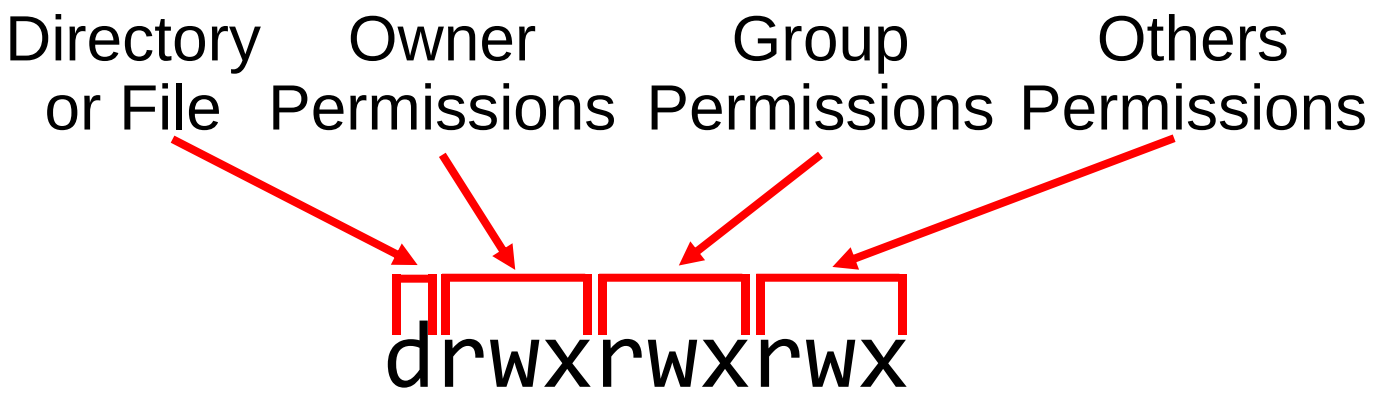
CLI

- File and Folder Commands
  - A number of command line tools are included in Unix-like systems by default.
  - Common file and folder related commands include: ls, cd, mkdir, cp, mv, rm, grep and cat.
- Administrative Commands
  - UNIX and its derivatives utilize file permissions to create boundaries within the system.
  - Every file on Unix systems carries its file permissions.
  - UNIX file permissions can be Read, Write or Execute.



File and Folder Permissions

- d Directory
- r The file can be read
- w The file can be created, written, and modified
- x The file can be executed
- - The file cannot be read, modified, or executed



File and Folder Permission Examples

drwx------	Owner has full access to the Documents directory. He can list, create files and rename, delete any file in Documents, regardless of file permissions.
dr-x------	Owner has full access except he can not create, rename, delete any file. He can list the files and (if file's permission empowers) may access an existing file in Documents.
d-wx------	Owner can not do 'ls' in Documents but if he knows the name of an existing file then he may list, rename, delete or (if file's permission empowers him) access it. He is also able to create new files.
d--x------	Owner is only capable of (if file's permission empowers him) access those files in Documents which he knows of. He can not list already existing files or create, rename, delete any of them.
-rw-r--r--	This is a file, not a directory. Owner has the ability to read and write but not execute. The group has the ability to read the file but not write/edit it in any way (read-only). The same permissions apply to everyone else.

Keep in mind that directory permissions have nothing to do with the individual file permissions. When you create a new file it is the directory that changes. That is why you need write permission to the directory.

10.5 Basic Troubleshooting Process for Mobile, Linux, and OS X Operating Systems

Cisco | Networking Academy®
Mind Wide Open™

Troubleshooting Process

Computer problems can result from a combination of hardware, software, and network issues. Computer technicians must be able to analyze the problem and determine the cause of the error to repair the computer. This process is called troubleshooting.

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

Applying the Troubleshooting Process to Mobile, Linux and OS X OSs

- Identify Common Problems and Solutions
  - Computer problems can be attributed to hardware, software, networks, or some combination of the three.
  - Many problems can be solved with a reboot.
  - When a mobile device does not respond to a reboot, a reset may need to be performed.
  - When a standard reset does not correct the problem, a factory reset may need to be performed.
  - When a reboot does not fix a PC, more investigation should be done.
  - Some configuration could be changed, software updates could be required or a misbehaving program is the culprit and must be reinstalled.

10.6 Chapter Summary

Cisco | Networking Academy®
Mind Wide Open™

Summary

- This chapter introduced you to mobile devices, the operating systems used on mobile devices, how to secure mobile devices, the uses of cloud-enabled services for mobile devices, and the way that mobile devices connect to networks, devices, and peripherals.
- This chapter also covered Ubuntu Linux and Apple OS X operating systems and some of its main characteristics including: command line interface, command line-based tools, graphical user interfaces used and some GUI-based tools. This chapter also covered the primary maintenance tasks and related tools.
- The basics of troubleshooting mobile operating systems, Linux and OS X were discussed with examples of simple solutions for common problems. The following concepts from this chapter are important to remember:
  - Open source software can be modified by anyone with little or no cost.
  - Use only trusted content sources to avoid malware and unreliable content.
  - Both Android and iOS have similar GUIs for using apps and other content.
  - Email accounts are closely tied to mobile devices and provide many different data synchronization services.

Summary (Cont.)

- The following concepts from this chapter are important to remember:
  - Android devices use apps to synchronize data not automatically synchronized by Google.
  - iOS devices use iTunes to synchronize data and other content.
  - Passcode locks can secure mobile devices.
  - Remote backups can be performed to backup mobile device data to the cloud.
  - Remote lock or remote wipe are features used 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.


Cisco | Networking Academy®
Mind Wide Open™


CISCO™