## Contents

- ACSP certification benefits .................................................................................................................. 6
- Complete the course ................................................................................................................................... 7
- Study the book ........................................................................................................................................... 7
- Gain experience with macOS ..................................................................................................................... 7
- Use this guide ............................................................................................................................................. 7
- Exam details ................................................................................................................................................ 8
- Lesson 1—Introduction to macOS ........................................................................................................... 9
  - Goals ........................................................................................................................................................ 9
  - Review questions ..................................................................................................................................... 9
  - Answers .................................................................................................................................................... 9
- Lesson 2—Update, Upgrade, or Reinstall macOS ....................................................................................... 9
  - Goals ........................................................................................................................................................ 9
  - Review questions ..................................................................................................................................... 9
  - Answers .................................................................................................................................................... 10
- Lesson 3—Set Up and Configure macOS ................................................................................................. 10
  - Goals ........................................................................................................................................................ 10
  - Review questions ..................................................................................................................................... 10
  - Answers .................................................................................................................................................... 10
- Lesson 4—Use the Command-Line Interface ......................................................................................... 11
  - Goals ........................................................................................................................................................ 11
  - Review questions ..................................................................................................................................... 11
  - Answers .................................................................................................................................................... 11
- Lesson 5—Use macOS Recovery ............................................................................................................. 12
  - Goals ........................................................................................................................................................ 12
  - Review questions ..................................................................................................................................... 12
  - Answers .................................................................................................................................................... 12
- Lesson 6—Update macOS ....................................................................................................................... 13
  - Goals ........................................................................................................................................................ 13
Becoming an Apple Certified Support Professional

The Apple Training and Certification program keeps you at the forefront of Apple technology. Certification creates a benchmark to demonstrate your proficiency in specific Apple technologies and gives you a competitive edge in today’s evolving job market.

Apple offers two macOS certifications:

• Apple Certified Associate—Mac Integration
• Apple Certified Support Professional (ACSP)

ACSP certification is for the help desk professional, technical coordinator, or power user who supports macOS users, manages networks, or provides technical support for Mac users. ACSP certification verifies that you understand macOS core functionality and that you can complete these tasks:

• Configure key services
• Perform basic troubleshooting
• Support multiple Mac users

Passing the macOS Support Essentials 10.13 Exam is an essential part of earning your ACSP certification. For more information, visit the Training and Certification website.

ACSP certification benefits

In addition to differentiating you as a skilled user and support professional for macOS High Sierra, an ACSP certification enables you to benefit from the power of the Apple brand. After you pass the certification exam, you receive an email that details how you’ll receive your Apple certificate, along with instructions on how to order a framed version. The email includes LinkedIn, Facebook, and Twitter icons so you can easily share your certification news with your networks on these sites.

You also receive a login for the Apple Certification Records System, where you can take the following actions:

• Update your profile and opt in to display your Apple Certification in the Apple Certified Professionals Registry.
• Review your certification progress.
• Download your certification logo to use on business cards, résumés, websites, and more.
• Allow employers to verify your certifications.
Recommended Exam Preparation

The following exam preparation is recommended:

- Complete the High Sierra 101: macOS Support Essentials 10.13 course.
- Gain experience with macOS.
- Read this guide and practice completing the sample tasks and answering the review questions.

**Complete the course**

Apple Authorized Training Providers (AATPs) offer courses where you can learn more about macOS by using it. You’ll also benefit from the expertise of Apple Certified Trainers and your peers. LearnQuest is an AATP, and you can visit their website to find nearby course offerings.

**Study the book**

The Apple Pro Training Series book *macOS Support Essentials 10.13* is the basis for the ASCP exam. You can buy the book from several locations:

- iBooks Store—You can buy from the iBooks Store if you use an iOS device or Mac.
- Safari Tech Books Online—An on-demand digital library that offers subscription access to the Apple Pro Training Series, as well as thousands of other reference videos and books.
- Peachpit—Visit the Peachpit website to save 30 percent.

This book may be available in other languages. See the Peachpit website for details.

**Gain experience with macOS**

There’s no substitute for time spent learning macOS technology. After you read the book, take the course, or both, spend time increasing your familiarity with macOS to ensure your success on the certification exam.

**Use this guide**

You might be self-taught, or took courses that don’t use the Apple Pro Training Series curriculum. You can still prepare for the certification exam by practicing the tasks and answering the review questions in the following sections.

The tasks and questions cover the knowledge domains that are assessed by the ASCP exam. Although this guide divides the tasks and review questions into lessons or knowledge areas, questions are presented randomly during the exam.
Exam details

The macOS Support Essentials 10.13 exam is computer-based and offered at Apple Authorized Training Providers (AATPs). To find the closest AATP, visit the LearnQuest website. LearnQuest is Apple’s global training partner. If you don’t see a session scheduled at your nearest LearnQuest training center, contact LearnQuest to find out whether a session can be scheduled for you. All LearnQuest training centers offer all macOS and pro apps exams, even if they don’t offer the corresponding course.

Here are the macOS Support Essentials 10.13 exam details:

- The exam contains five unscored demographic questions. You have 5 minutes to complete them.
- The exam contains 100 scored technical questions. You have 150 minutes to complete them.
- The exam uses a random pool of multiple-choice and interactive-media questions.
- A passing score is 75 percent. Scores aren’t rounded.
- You can find details on exam scoring on the Training and Certification: Exam and Certification Questions webpage.
- You may not access any resources or references during the exam.
- Some exams are available in multiple languages. For details, visit Training and Certification: Localized Apple Certification Exams.

If you have questions about exams, visit Training and Certification: Exam and Certification Questions.
Part One: Installation and Configuration

Lesson 1—Introduction to macOS

Goals
• Describe macOS.
• Describe new macOS High Sierra 10.13 features.
• List macOS versions supported on Mac computers that can also run macOS High Sierra 10.13.

Review questions
1. What is the default file system for Mac computers with all-flash storage running macOS High Sierra?
2. Which industry standard allows a Mac running High Sierra to better deal with the rising popularity of 4K video?
3. What capability does Metal 2 add to High Sierra?

Answers
1. The default file system for all-flash storage Mac computers is Apple File System (APFS).
2. The High Efficiency Video Coding (HEVC), also known as H.265, allows Mac computers to better handle 4K video.
3. Metal 2 adds the capability to use machine learning, virtual reality, and external GPU support for entertainment and professional creative apps.

Lesson 2—Update, Upgrade, or Reinstall macOS

Goals
• Describe the differences between a macOS update, upgrade, and reinstallation.
• Describe the macOS Installer.
• Troubleshoot a macOS upgrade or reinstallation.

Review questions
1. How can you get the macOS installer?
2. What are the differences between a macOS update, upgrade, and reinstallation?
3. What are system requirements to upgrade to macOS High Sierra?
4. What steps should you take before you upgrade to macOS High Sierra?
5. How does the macOS installer know which firmware updates to download for your Mac?
6. What can you use to troubleshoot macOS installation issues?
Answers
1. macOS is free to anyone with a qualifying Mac.

2. These are the differences between a macOS update, upgrade, and reinstallation:
   - macOS update—Installs an incremental update of the Mac operating system but doesn't upgrade it to the next major version.
   - macOS upgrade—Installs the next major standalone version.
   - Reinstall—Installs the same major version of macOS on a disk that already has macOS installed.

3. The system requirements to upgrade to High Sierra are as follows:
   - OS X Mountain Lion 10.8 or later
   - 2 GB of memory
   - 14.3 GB of available storage space

4. Before you upgrade to macOS, High Sierra you should perform these tasks:
   - a. Verify app compatibility.
   - b. Back up important files and folders.
   - d. Open Software Update or App Store.

5. The Installer uses your Mac model number to locate and download firmware updates for your Mac.

6. You can view the Installer Log from the macOS Installer menu bar.

Lesson 3—Set Up and Configure macOS

Goals
- Complete initial macOS configuration.
- Adjust common system settings.
- Identify and install a configuration profile.
- Verify system information.

Review questions
1. Which tool guides you through the initial macOS High Sierra configuration?
2. Which key features do you gain by setting up iCloud?
3. Which feature can significantly improve Apple ID security on Mac computers that have iCloud enabled?
4. After you configure macOS High Sierra, where can you manage iCloud settings?
5. What's a profile? How do you manage profiles?
6. Where can you find system information and repair and warranty coverage information for your Mac?

Answers
1. Setup Assistant guides you through the macOS High Sierra configuration process.
2. iCloud provides cloud storage and communication services for apps, including Mail, Contacts, Calendars, Reminders, Notes, Safari, Keychain, Photos, and any other apps that support iCloud integration. iCloud also provides Find My Mac technology for help locating a lost or stolen Mac.
3. Two-factor authentication can improve Apple ID security if iCloud is enabled.
4. After you set up macOS High Sierra, you can manage iCloud settings from iCloud or Internet Accounts preferences.

5. A profile is a document with the filename extension .mobileconfig that contains system settings as defined by an administrator. When you open a profile document, macOS High Sierra installs the profile and configures the settings. You can manage installed profiles through Profiles preferences.

6. You can find the system information and repair and warranty coverage information for your Mac in the About This Mac window.

Lesson 4—Use the Command-Line Interface

Goals
• Be able to describe when the command-line interface is useful.
• Explore Terminal.

Review questions
1. What are some advantages of using the command-line interface?
2. What are the four parts of a command string?
3. Which terminal command should you use to perform the following?
   a. Print working directory
   b. List
   c. Change directory
   d. Indicate parent directory
   e. Indicate current user home folder
   f. Create a folder
   g. Run the command with root account access
   h. Clear the Terminal screen
4. Which key should you use if you want to automatically complete filenames, pathnames, and command names?

Answers
1. The command-line interface provides these advantages:
   • Additional administrative and troubleshooting options
   • More access to the file system
   • A remote login using the Secure Shell (SSH) protocol
   • The ability to run commands as root using sudo
   • The ability to automate repetitive tasks using scripting
   • The ability to remotely administer multiple Mac computers simultaneously using Apple Remote Desktop (ARD).
2. The four parts of a command string are as follows:
   - Command name
   - Command options
   - Arguments
   - Extras

3. Use these commands to perform the following tasks:
   a. Print working directory: `pwd`
   b. List: `ls`
   c. Change directory: `cd`
   d. Indicate parent directory: `..`
   e. Indicate current user home folder: `~`
   f. Create a folder: `mkdir`
   g. Run the command with root account access: `sudo`
   h. Clear the Terminal screen: `clear` or press Control-L

4. You should use the tab key to automatically complete filenames, pathnames, and command names.

**Lesson 5—Use macOS Recovery**

**Goals**
- Access macOS Recovery utilities.
- Reinstall macOS from macOS Recovery.
- Create an external macOS Recovery disk.

**Review questions**
1. Which utilities are available when you start up from macOS Recovery?
2. What are the different macOS Recovery options and start up key combinations?
3. How can you create an external macOS installation disk?

**Answers**

2. macOS Recovery installs different versions of macOS depending on the start up key combination you use.
   a. Command-R—Install the latest macOS that was installed.
   b. Option-Command-R—Upgrade to the latest macOS that is compatible with your Mac.
   c. Shift-Option-Command-R—Install the macOS that came with your Mac.

3. You can create a macOS Recovery disk that includes the macOS High Sierra tools and installation assets with the `createinstallmedia` command-line tool in macOS Installer.
Lesson 6—Update macOS

Goals
- Configure automatic software update settings.
- Automatically update Apple-sourced software.
- Manually update Apple software.

Review questions
1. Who can install system software updates through the App Store?
2. How does macOS tell you that a software update is available?
3. Which apps does Software Update attempt to update?
4. Which app should you open to initiate Apple software updates?
5. Which items are always installed, by default, through automatic software updates?
6. Which bundled apps are not automatically installed when you erase and reinstall macOS High Sierra?
7. How can you control which software applications automatically update on a Mac?
8. Where can you find Apple software updates if you need to manually install an update?
9. What’s the best way to learn what software is installed on a Mac?

Answers
1. Users with administrator and standard accounts can install system updates through the App Store.
2. macOS displays an Updates Available notification in an alert when software updates are ready to be installed.
3. macOS Software Update attempts to update this software:
   - Currently installed Apple-source software
   - macOS bundled software
   - Software you bought from the App Store
4. You should open the App Store app to initiate software updates.
5. System files and security updates are automatically installed, by default, when they’re available.
6. iMovie, GarageBand and productivity apps—Pages, Keynote, and Numbers—are not automatically reinstalled if you erase the disk.
7. You control software update automation in App Store preferences. You can further restrict a user’s ability to use the App Store by configuring parental controls for the user’s account.
8. You can find and download all Apple software updates at https://support.apple.com/downloads.
9. System Information shows all software installed through the App Store or the Installer app, including installations from either Apple or third parties.
Part Two: User Accounts

Lesson 7—Manage User Accounts

Goals

• Recognize various user account types and user attributes.

• Create and manage user accounts.

• Adjust login and fast user switching settings.

Review questions

1. What are the types of local user accounts in macOS High Sierra? How are they different?

2. What are account attributes?

3. How can you limit a user account from having full access to all apps?

4. What does fast user switching allow you to do?

Answers

1. The local users accounts in macOS include the following:

   • Administrator—Administrator user accounts are part of the admin group and are allowed full access to all apps, preferences, and shared resource locations.

   • Standard—Standard users are allowed to take advantage of nearly all the resources and features of a Mac, but they generally can’t change things that might affect other users.

   • Managed with parental controls—A managed account is a standard account with parental controls enabled.

   • Guest—The default guest account is similar to a standard user, but it doesn’t require a password. When a guest user logs out, the home folder is deleted, including any home folder items that would normally be saved, like preference files or web browser history.

   • Sharing only—“Sharing only” accounts allow you to share files with someone on a different computer, but they can’t log in to your Mac.

   • System Administrator (root)—The System Administrator account has unlimited access to almost everything on a Mac. It is turned off by default on macOS.

   • Group—A group account is a list of user accounts that gives you greater control over file and folder access.

2. Account attributes are the individual pieces of information used to define a user account. Examples include User ID, group, account name, full name, login shell, home directory, universally unique ID (UUID), Apple ID, and aliases.

3. You can use parental controls to restrict what users can do. Examples of limitations include enforcing a simple Finder, limiting apps, limiting App Store content, setting time limits, privacy settings, and more.

4. Fast user switching lets a Mac switch between user accounts without users having to log out or quit apps.
Lesson 8—Manage User Home Folders

Goals
- Be able to describe user home folders.
- Delete users’ accounts and archive their home folder contents.
- Migrate and restore home folders.

Review questions
1. Which folders, by default, are contained in a user’s home folder?
2. What options do you have when you delete a local user account?
3. What does Migration Assistant enable you to do?
4. How do you associate a new local user account with a manually migrated or restored user’s home folder in macOS?

Answers
1. The default folders in a user’s home folder include the Desktop, Documents, Downloads, Movies, Music, Pictures, and Public folders.
2. When you delete a local user account, you have three options:
   a. Save the home folder in a disk image.
   b. Don’t change the home folder.
   c. Delete the home folder.
3. Migration Assistant enables you to transfer settings, user accounts, and content from a Mac or Windows computer or from a Time Machine backup to your Mac.
4. To associate a new local user account with a manually migrated or restored user’s home folder, follow these steps:
   a. Copy the restored user’s home folder to the /Users folder.
   b. Open System Preferences and select Users and Groups.
   c. Create a new local user account with the same account name that was used for the user’s home folder. macOS will prompt you to associate the new local user account with the restored home folder.

Lesson 9—Manage Security and Privacy

Goals
- Be able to describe password types and use.
- Manage secrets in Keychain.
- Enable and manage iCloud Keychain.
- Manage system security and user privacy.

Review questions
1. What are the different types of passwords you use to secure a Mac?
2. Which types of items can you store in a keychain?
3. How does Keychain Access help protect your information?
4. Where are keychain files stored?
5. What app should you use to manage keychain settings?

6. How does two-factor authentication provide added security to your Apple ID?

7. When and why would you use an iCloud Security Code?

8. How can you limit the use of Location Services?

9. How can you ensure that audio recordings used for Dictation service remain private?

10. Which feature can you enable to find a lost Mac?

**Answers**

1. These are the different types of passwords you use to secure a Mac:
   a. Local user account password.
   b. Apple ID and password—For iCloud, iTunes, and the App Store.
   c. Keychain passwords—To protect authentication assets in encrypted keychain files.
   d. Resource passwords—Such as email, websites, file servers, apps, and encrypted disk images.
   e. Firmware password—Prevents your Mac from starting up up from any disk other than your designated startup disk.

2. You use Keychains to store resource passwords, certificates, keys, website forms and secure notes. The keychain system can also securely store Safari AutoFill information, Internet Account settings, and secure text notes.

3. Keychain Access manages encrypted files that are used to securely save your items. They are impenetrable unless you know the keychain password. If you forget the keychain password, you lose the file contents forever.

4. Keychains are stored throughout macOS for different users and resources.
   a. Local login keychains are stored in /Users/username/Library/Keychain/login.keychain.
   b. Other local keychains are stored in /Users/username/Library/Keychains/others.keychain.
   c. iCloud keychains are stored in /Users/username/Library/Keychains/UUID/.
   d. System keychains are stored in /Library/Keychains/System.keychain.
   e. System Root keychains for trusted networks do not appear by default, but can be located here: /System/Library/Keychains/
   f. Other keychains can be found throughout macOS. You should leave these files alone unless you’re instructed by a trusted source to resolve an issue.

5. You should use Keychain Access to view and modify most keychain items.

6. With two-factor authentication, your Apple ID account can be accessed only on devices you trust, like your iPhone, iPad, or Mac.

7. If you use an Apple ID that doesn't have two-factor authentication enabled, iCloud Keychain is automatically enabled. You should use the iCloud Security Code to grant access to use your Apple ID on additional devices.

8. You can use the Privacy pane of Security & Privacy preferences to configure app access to Location Services, Contacts, Calendars, Reminders, and social network services. When a new app requests information that is considered personal, macOS asks you for permission.
9. Enhanced Dictation option is enabled by default. When you use Enhanced Dictation, your Mac converts what you say into text without sending your dictated speech to Apple. Only if you turn Enhanced Dictation off is what you say is sent to Apple to be converted to text.

10. iCloud Find My Mac helps you find a lost Mac by allowing you to remotely access the Mac computer’s Location Services service.

Lesson 10—Manage Password Changes

Goals
- Change known passwords.
- Reset lost user passwords.
- Set a firmware password to secure macOS startup.

Review questions
1. How can you change your local computer account password?
2. How can you reset the another user account password in macOS High Sierra?
3. How are users’ login keychains affected when they change their own account passwords?
4. How can you reset a user’s lost account password if they can’t log in to their Mac?
5. How does resetting a user’s account password affect that user’s login keychain?
6. When can you reset a login password with an Apple ID?
7. How does Firmware Password Utility help prevent users from making unauthorized password changes?

Answers
1. You can change your own local account passwords from the General pane of Security & Privacy preferences.
2. You can reset other user account passwords from Users & Groups preferences by selecting the user account you want to change and then clicking Reset Password.
3. If your login password doesn’t match your login keychain password, when you login into your Mac, macOS creates new empty keychain items for you that match your login keychain.
4. You can use the Reset Password assistant available from macOS Recovery.
5. If your login password doesn’t match your login keychain password, macOS creates new empty keychain items for you that match your login keychain. If the user remembers their old password, you can retrieve the archived keychain.
6. You can reset a login password with an Apple ID if you provided your Apple ID when you created your first user account during Setup Assistant.
7. A firmware password prevents users who don’t have the password from starting up from any disk other than the designated startup disk.
Part Three: File Systems

Lesson 11—Manage File Systems and Storage

Goals

- Recognize systems supported by macOS.
- Manage disks, partitions, and volumes.
- Troubleshoot and repair partition and volume issues.

Review questions

1. What do you call the process of applying logic to storage in the form of partitions, containers, and volumes?
2. Which type of partition schemes does macOS support?
3. Which major volume formats are supported by macOS High Sierra?
4. What are some of the advantages of APFS?
5. What are the five ways you can eject a volume or disk from the Finder?
6. Which two built-in macOS High Sierra apps can you use to gather information about storage devices?
7. What does the Disk Utility First Aid feature do?

Answers

1. Formatting is the process of applying logic to storage.
2. macOS supports three partition schemes:
   a. GUID Partition Map (GPT)—This is the default partition scheme used by Mac computers.
   b. Apple Partition Map (APM)—This is the default partition scheme used by previous PowerPC-based Mac computers.
   c. Master Boot Record (MBR)—This is the default partition scheme used by most non-Mac computers, including Windows-compatible PCs. This partition scheme is commonly used by peripherals that store to flash memory.
3. macOS High Sierra supports these major volume formats:
   - APFS—Used for solid-state drive (SSD) or other all-flash storage device.
   - Mac OS Extended—Used before macOS High Sierra. Also known as HFS Plus.
   - FAT—A legacy volume format used by Windows PCs.
   - ExFAT—Created specifically for large flash storage disks larger than 32 GB.
   - NTFS—The Windows default native volume format. macOS can read but can’t write to or start up from NTFS volumes.
4. APFS makes common operations such as copying files and directories instantaneous, helps protect data from power outages and system crashes, and keeps files safe and secure with native encryption.
5. These are the five methods you can use to eject a volume or disk in the Finder:
   a. Drag the disk icon to the Trash in the Dock.
   b. In the Finder sidebar, click the small Eject button next to the volume you want to eject.
   c. Select the volume you want to eject and then choose File > Eject.
   d. Select the volume you want to eject and then use the Command-E keyboard shortcut.
   e. Select the volume you want to eject and Control-click to reveal a pop-up menu. Select Eject.

6. Disk Utility and System Information can both be used to gather information about storage devices.

7. Use the Disk Utility First Aid feature to verify and repair the partition scheme and directory structure of a volume. These elements contain the information used to locate files and folders on the volume.

Lesson 12—Manage FileVault

Goals
- Describe how FileVault helps protect data.
- Enable FileVault protection.
- Describe how to regain access to a FileVault-protected Mac when all local user account passwords are lost.

Review questions
1. How does FileVault protect user data?
2. How can you turn on FileVault if you didn’t turn it on when you were prompted by Setup Assistant?
3. What are the two ways you can save the FileVault recovery key when you enable FileVault in Security & Privacy preferences?

Answers
1. FileVault uses full-disk encryption to help prevent unauthorized access to the information on your startup disk.
2. You can turn on FileVault at any time from Security & Privacy preferences.
3. FileVault Recovery offers two ways to recover passwords if FileVault passwords are lost:
   a. You can use your Apple ID to unlock the FileVault volume and reset your password.
   b. Record the key that FileVault randomly generates.

Lesson 13—Manage Permissions and Sharing

Goals
- Describe file ownership and permissions.
- Explore macOS default shared folders.
- Securely manage file and folder access.

Review questions
1. How do you identify the ownership and permissions of a file or folder in the Finder?
2. How do ACLs differ from standard UNIX file system permissions?
3. Why is the root (or beginning) level of a user’s home folder visible to other users?
4. How does the default organization of the file system allow users to safely share local files and folders?

5. What’s unique about the permissions of the /Users/Shared folder?

**Answers**

1. You can use the Finder Info window to identify an item’s ownership and permissions.

2. Access control lists (ACLs) expand the standard UNIX permissions architecture to allow more file and folder access control, similar to what’s available on Windows-based NTFS and UNIX file systems.

3. The root level of a user’s home folder is visible to other users so they can navigate to the Public shared folder.

4. Every home folder contains a Public folder that other users can read and a Drop Box folder that other users can write to. All other subfolders in a user’s home folder (except the optional Sites folder) have default permissions that don’t allow access by other users. The Shared folder is also set for all users to share items.

5. The Shared folder is set up to allow all users to read and write files, but only the user who owns an item can delete it from the Shared folder. The “sticky bit” permissions setting prevents other users from deleting items that they don’t own.
Part Four: Data Management

Lesson 14—Use Hidden Items, Shortcuts, and File Archives

Goals

• Navigate to hidden files and folders.
• Examine packages and bundles.
• Manage aliases and links.
• Create and open ZIP archives and disk images.

Review questions

1. Why does the Finder hide certain folders at the root of the system volume?
2. What two methods are used to hide items from the Finder?
3. What does macOS High Sierra use bundles and packages for?
4. How does an alias differ from a symbolic link?
5. Why would you use an archive file instead of a disk image? Why would you use a disk image instead of an archive file?
6. What type of file does the Finder create when you select the Archive option?
7. What action on macOS High Sierra is set as the default for opening zip archive files?

Answers

1. The Finder hides traditional UNIX resources from average users because they don’t need access to those items. If users do need access to UNIX items, they can use Terminal.

2. You can hide items from the Finder by using either of these methods:
   a. Adding a period to the beginning of a filename.
   b. Enabling the hidden file flag.

   Note: Both methods for hiding items can be managed from the command line.

3. Bundles and packages are used to combine complex items into individual folders. Packages have the additional advantage of appearing as a single item in the Finder. This allows software developers to combine resources into a single item and prevents users from seeing and potentially damaging those resources by deleting or moving files.

4. Both aliases and symbolic links act as a shortcut to an original item. However, an alias contains additional information that allows the system to keep track of the original item if it’s renamed or moved within the same volume. In contrast, any change to an original item breaks a symbolic link.

5. Archive files are much simpler to create in the Finder and are compatible with third-party operating systems. Disk images are more difficult to create and manage but offer greater flexibility, primarily because they can be easily modified and converted. However, macOS High Sierra disk images aren’t compatible with third-party operating systems.

6. The Archive option in the Finder creates compressed zip archive files.

7. By default on macOS High Sierra, double-clicking a zip archive causes the system to expand the contents of the zip archive next to the same location as the original zip archive.
Lesson 15—Manage System Resources

Goals
- Navigate to hidden files and folders.
- Examine packages and bundles.
- Manage aliases and links.
- Create and open ZIP archives and disk images.

Review questions
1. What are the four default top-level folders visible in the Finder?
2. What are six common system resources? What purpose does each resource serve?
3. What are the four system resource domains? What purpose does each domain serve?
4. What purpose does the ~/Library/Containers folder serve? What items are in this folder?
5. What happens when a user double-clicks a font file?
6. How can you identify duplicate fonts?
7. How does System Integrity Protection (SIP) help ensure that macOS High Sierra system resources remain secure?

Answers
1. The four default top-level folders visible in the Finder are as follows:
   a. Applications—Apps that local users have access to.
   b. Library—System resources that local users have access to.
   c. System—System resources.
   d. Users—Local user home folders.
2. These are the six common system resources and the purposes they serve:
   a. Extensions—Attach themselves to the system kernel to provide hardware and peripheral driver support.
   b. Frameworks—Shared code libraries that provide additional software resources for apps and system processes.
   c. Fonts.
   d. Preference files—App and system configuration information.
   e. LaunchAgents and LaunchDaemons—Used by launchd to provide services that automatically start when needed at system startup or at user login.
   f. Logs—Text files that contain error and progress entries from nearly any app or system service.
3. These are the four system resource domains and the purpose they serve:
   a. User—Contains apps and system resources that are specific to each user account.
   b. Local—Contains apps and system resources that are available to users on a local Mac.
   c. Network—Optional. Contains apps and system resources available to any Mac that has an automated network share.
   d. System—Contains apps and system resources that provide basic system functionality.
4. The ~/Library/Containers folder contains resources for sandboxed apps. macOS High Sierra creates and maintains a separate container folder for each sandboxed app that a user can open. A sandboxed app is more secure because it can access only items inside its container. Only items intended for sharing are in a group container folder.

5. When you double-click a font file, it automatically opens a preview of the font in the Font Book app. From here, you can click the Install Font button to copy the font into ~/Library/Fonts.

6. The Font Book app shows a small dot next to the name of any font that has duplicate resources.

7. System Integrity Protection prevents users and processes with administrator or root access from modifying core macOS High Sierra items. Protected items include the /System, /bin, /sbin, and /usr folders along with core macOS High Sierra apps.

Lesson 16—Use Metadata, Spotlight, and Siri

Goals

• Describe how macOS stores and uses file metadata.

• Use metadata, such as tags and comments, to organize your files.

• Use Spotlight and Siri to search for local and Internet resources.

Review questions

1. What’s file system metadata? What are some examples?

2. What are some of the common file flags used by macOS High Sierra?

3. What are file system tags? Where can you find tags in the user interface?

4. How does the Spotlight search service use metadata?

5. Where does Spotlight store its metadata index databases and its plug-ins?

6. What are some privacy and security concerns with Spotlight?

7. How do you resolve an issue where a Spotlight search doesn’t find the correct items?

8. How can you ensure that Siri doesn’t send audio recordings to Apple?

Answers

1. Metadata is information stored outside of a file or folder. It provides additional information about files and folders. Examples include file flags, extended file attributes, and permissions.

2. Common file flags include the locked flag, which locks files from changes, and the hidden flag, which hides the item in the Finder.

3. File system tags are a type of metadata that allow you to quickly assign keywords, or “tags,” to any item. A user can customize the tag names and colors.

4. The Spotlight search service creates index databases of file system metadata so that it can perform normally time-intensive searches almost instantly. File system tags can be found in the Finder sidebar, Spotlight search, and any Open or Save document dialogs.

5. Spotlight metadata index databases are stored at the root of every volume in a /.Spotlight-V100 folder. However, a Legacy FileVault user’s database is stored in the user’s encrypted home folder. And the Mail app maintains its own database in each user’s home folder at ~/Library/Mail/V2/MailData/Envelope Index. Spotlight plug-ins can be located in any of the Library folders in a folder named Spotlight.

6. Although Spotlight indexes file and folder permissions, other users can search the contents of locally attached nonsystem volumes when ownership is ignored on those volumes.
7. If you experience problems with local file searching, you can force Spotlight to rebuild the index databases by deleting them and restarting your Mac or by managing the Spotlight preferences, as covered later in this lesson.

8. You can prevent Siri from sending audio to Apple by disabling Siri from Siri preferences.

Lesson 17—Manage Time Machine

Goals

• Describe Time Machine.
• Configure Time Machine to back up data.
• Restore data or macOS from a Time Machine backup.

Review questions

1. What can you back up with Time Machine?
2. Which backup destination disks does Time Machine support?
3. How does Time Machine maintain a backup history of the file system?
4. Which types of files are omitted from Time Machine backups?
5. Why is Time Machine inefficient at backing up large databases?
6. Which feature helps help Time Machine restore data when your Time Machine backup disk isn't available?
7. What are the four ways you can restore data from a Time Machine backup?

Answers

1. Time Machine lets you back up your entire Mac, including system files, apps, music, photos, emails, and documents.
2. The most common format is HFS Plus but it also supports Xsan formats. You can back up from an HFS Plus or APFS-formatted disk to an HFS Plus disk; however, Time Machine can't back up to an APFS-formatted disk.
3. Time Machine saves space by ignoring files that don't need to be backed up—ones that can be re-created after a restoration. Generally speaking, Time Machine ignores temporary files, Spotlight indexes, items in the Trash, and anything that can be considered a cache.
4. Time Machine is inefficient at backing up large databases because it must back up the entire database file every time any change, no matter how small, is made to the database.
5. A previously backed-up item won't be available if your backup volume filled up and Time Machine had to start deleting older items to make room for newer ones.
6. Time Machine creates local snapshots on your built-in startup disk to help when your backup disk isn't available.
7. Methods for restoring from a Time Machine backup include the following:
   • Restore Specific Items from a Time Machine backup.
   • Restore with Migration Assistant.
   • Restore an entire system with macOS Recovery.
   • Manually restore with the Finder.
Lesson 18—Install Apps

Goals
- Install apps from the App Store.
- Describe app support and identify security issues.
- Install apps using software packages and drag and drop.

Review questions
1. How can apps you purchased on one Mac be installed on another Mac you use?
2. How many Apple IDs can be part of a Family Sharing group?
3. Which security technologies does the Mac use to help protect users when they install third-party apps?
4. Which two security options does Gatekeeper allow? Which Gatekeeper option is the macOS High Sierra default?
5. How do you install apps that aren't located in the App Store?
6. What are three ways you can uninstall apps?

Answers
1. If you use more than one Mac, you can enable automatic downloads of purchased apps on your other Mac.
2. A Family Sharing group can have up to six members.
3. The Mac uses these technologies to protect users when they install third-party apps:
   - Process Security—Security mechanisms, including SIP, that prevent access to resources unless specifically allowed. Systemwide privileges are allowed only when needed.
   - App sandboxing—Apps are granted access only to the items they need.
   - Code signing—Used by the system to verify the authenticity and integrity of the software.
   - File quarantine—Displays a warning when you attempt to open an item downloaded from an external source such as the Internet.
   - Malware detection—macOS maintains a list of known malicious software that’s automatically updated by the macOS software update.
   - Gatekeeper—Uses both code signing and file quarantine to protect your Mac from malicious apps.
4. Gatekeeper allows apps downloaded from these sources:
   - The App Store
   - The App Store and identified developers (default option)
5. In addition to using the App Store, you can install software using drag-and-drop installations or installation packages.
6. You can uninstall apps in three ways:
   a. Uninstall the App using Launchpad.
   b. Drag the app to Trash.
   c. Use a custom-built uninstaller package.
Lesson 19—Manage Documents

Goals
- Use Launch Services and Quick Look to open documents.
- Work with apps that support Auto Save and Versions.
- Save and open documents saved to iCloud.
- Optimize local storage to reclaim space on the system volume.

Review questions
1. What identifies the app type that should open when you double-click a document in macOS?
2. How do you engage Quick Look? Which apps support it?
3. What technology enables Quick Look to preview so many file types?
4. What’s Auto Save? How can you identify an app that supports Auto Save?
5. How deep is the version history of a file that you share through email?
6. Which apps can manage document locking?
7. Where can you adjust app Auto Save and Resume options?
8. When you upgrade from iCloud to iCloud Drive, what behavior change occurs?
9. Where can you access items saved in iCloud Drive?
10. Where do you save documents in iCloud Drive if you want to access them from an iOS device?
11. If you have iCloud Desktop & Documents enabled on one Mac and you enable it for another Mac, what happens to the user’s Desktop & Documents folders?
12. What happens to the user’s Desktop & Documents folders if you disable iCloud Desktop & Documents?

Answers
1. macOS High Sierra uses a document filename extension to determine the document type. The Launch Services process maintains a database of installed apps and the document types that they can open.
2. You engage Quick Look by pressing the Space bar when a document is selected. Apps that support Quick Look include the Finder, Time Machine, Mail, and most open-and-save browser dialogs.
3. Quick Look uses plug-ins that give it the capability to preview documents. These plug-ins live in Quick Look folders in any Library folder on macOS High Sierra.
4. Auto Save allows compatible macOS High Sierra apps to automatically save changes to users’ documents. A user just saves a document once, then never has to think about saving changes again. Apps that support Auto Save feature a Duplicate function in the File menu instead of a default Save As function.
5. Documents sent through email or otherwise copied to a shared location don’t retain any version history.
6. Any app that supports Auto Save and the Finder can manage document locking.
7. You can deselect “Reopen windows when logging back in” from the logout verification dialog. From General Preferences, you can perform these actions:
   - Deselect “Close windows when quitting an application.”
   - Select “Ask to keep changes when closing documents,” which turns off Auto Save.
8. When you upgrade an iCloud account to use iCloud Drive, you won’t be able to directly access
documents from OS X Yosemite 10.10 or earlier or iOS 8 or earlier. If you’re using OS X Yosemite 10.10
or earlier, you can still access Cloud Drive items from the iCloud website: www.icloud.com.

9. iCloud Drive items are available in the Finder or in any app that uses standard macOS Open or Save
dialogs.

10. iOS 8 or later devices can access documents in iCloud Drive if they are saved in specific application
    folders. For example, Pages for iOS can access Pages documents if they are stored in the Pages folder
    in iCloud Drive.

11. If you enable iCloud Desktop & Documents on additional Mac computers, the Desktop & Documents
    content from those Mac computers is moved into subfolders inside the iCloud Desktop & Documents
    folders. For example, adding another Mac named “MyMac” results in Desktop & Documents folders
    containing “MyMac - Desktop” and “MyMac - Documents.”

12. When you disable iCloud Desktop & Documents, the items are moved into a subfolder within iCloud
    Drive, and the local Desktop and Documents folders are created as new empty folders for the local user.
    Users must navigate to iCloud Drive and manually copy their files to the new (empty) Desktop &
    Documents folders.

Lesson 20—Manage and Troubleshoot Apps

Goals
  • Describe and support app types.
  • Manage app extensions and widgets in Notification Center.
  • Monitor and control processes and apps.
  • Explore various app troubleshooting techniques.

Review questions
  1. Why would you want to open an app in 32-bit mode?
  2. What functionality do app extensions add in macOS High Sierra?
  3. How do you install new app extensions? After they’re installed, how do you manage app extension
     visibility?
  4. How can you identify the apps that are installed on your Mac?
  5. In macOS High Sierra, what app do you use to examine open apps?
  6. Which steps should you take when you troubleshoot app issues?
  7. Which three ways can you forcibly quit an app from the graphical interface?
  8. What does the diagnostic reporting feature do?
  9. Where are app preferences stored?
 10. Which file format is often used for preference files? How can you view the content of this file type?

Answers
  1. Using the Finder Info window, you can force an app to open in 32-bit mode. This step is necessary for a
     64-bit app to support older 32-bit plug-ins or app resources.
  2. App extensions allow apps from different developers to interact with each other as if they were built into
     another app.
3. App extensions are installed automatically because they’re bundled in the app that provides the extension. You can enable or disable installed app extensions from the Extensions preferences.

4. You can use System Information to scan the appropriate app locations and return a list of installed apps.

5. Use Activity Monitor to monitor open processes and apps.

6. General app troubleshooting steps include the following:
   a. Restart the app.
   b. Open another known working document.
   c. Try another app.
   d. Try another user account.
   e. Check diagnostic reports and log files.
   f. Delete cache files.
   g. Replace preference files.
   h. Replace app resources.

7. These are the three ways to forcibly quit an app from the graphical interface:
   a. From the Force Quit Applications dialog
   b. From the Dock
   c. From the Activity Monitor app

8. The diagnostic reporting feature automatically creates a diagnostic report log any time an app crashes or hangs. You can view the diagnostic report immediately. It’s reported to Apple through the Internet. You can also view it later in the /Applications/Utilities/Console app.

9. Application preferences are almost always stored in a user’s Library folder in the ~/Library/Preferences folder. Newer sandboxed apps must always store their preferences in a ~/Library/Containers/Bundle ID/Data/Library/Preferences folder, where Bundle ID is the unique bundle identifier for the app.

10. Most app preferences are property lists, which are XML files that have the .plist filename extension. You can view the content of these files using Quick Look and edit them using the Xcode development app, which you can get from the App Store.
Part Six: Network Configuration

Lesson 21—Manage Basic Network Settings

Goals
- Describe TCP/IP networking concepts.
- Configure and monitor network settings.
- Connect to a Wi-Fi network.

Review questions
1. What is a MAC address?
2. What’s the purpose of Internet Protocol v4 (IPv4) addresses and subnet masks?
3. How are IPv4 addresses constructed?
4. How does the IP transfer messages between computers over a wide area network (WAN)?
5. How is the Domain Name System (DNS) used to facilitate network naming?
6. What’s used to identify a Wi-Fi network?
7. Which Wi-Fi authentication protocols are supported by macOS High Sierra?
8. How can macOS High Sierra automatically connect to a Wi-Fi network?

Answers
1. The media access control (MAC) address is used to identify a physical network interface on a local network.
2. The IP address identifies the location of a network device. IP addresses are the primary identification used by the Internet protocol suite TCP/IP for both LANs and WANs. Subnet masks are used by network devices to identify their local network range and to determine whether outgoing data is destined for a network device on the LAN.
3. Most common IP addresses and subnet masks share the same IPv4 formatting. An IPv4 address is a 32-bit number represented in four groups of three-digit numbers, known as octets, separated by periods. Each octet has a value between 0 and 255.
4. A network client uses the subnet mask to determine whether the destination IP address is on the LAN. If the destination IP address isn’t, it assumes that the destination address is on another network, and the client sends the data to the IP address of the local network router. The network router then sends the data, through a WAN connection, to another router that it thinks is closer to the destination. This continues across WAN connections from router to router until the data reaches its destination.
5. The DNS is used to resolve a DNS name to the corresponding IP addresses.
6. A Service Set Identifier, or SSID, is used to identify a Wi-Fi network name and associated configuration.
7. macOS High Sierra supports authenticated Wi-Fi by using the following authentication protocols: WEP, WPA/WPA2 Personal, and WPA/WPA2 Enterprise, which includes support for 802.1X authentication.
8. A new Mac can automatically connect only to Wi-Fi networks that have no standard authentication mechanism, known as an “open network.” However, a configured Mac can automatically reconnect to authenticated Wi-Fi networks, if the appropriate information was saved to the Keychain system.
Lesson 22—Manage Advanced Network Settings

Goals
- Describe the macOS network configuration architecture.
- Manage multiple network locations and service interfaces.
- Configure advanced network settings.

Review questions
1. What’s a network location? Who can access network locations?
2. Which interfaces and protocols are supported by default in macOS High Sierra?
3. How does network service order affect network connectivity?
4. In Network preferences, how can you tell which interface is currently being used for network activities?
5. What’s the easiest way to configure VPN settings in macOS High Sierra?
6. How is 802.1X configured on Mac computers?

Answers
1. A network location is a saved state of Network preferences that contain all network interface settings. Only administrators can define network locations, but if more than one location exists, all users can switch between the various network locations by using the Apple menu.
2. macOS High Sierra supports the following network interfaces and protocols:
   - Ethernet IEEE 802.3 family of hardware network interface standards
   - Wireless (Wi-Fi) IEEE 802.11 family of hardware network interface standards
   - FireWire IEEE 1394 bridged network interface
   - Thunderbolt bridged network interface
   - Bluetooth wireless hardware network interface
   - Cellular networks that use USB adapters or iOS devices with cellular network service (Personal Hotspot)
   - Virtual private network (VPN) virtual network interface through Layer 2 Tunneling Protocol (L2TP) over Internet Protocol Security (IPSec); Cisco’s IPSec; and Internet Key Exchange version 2 (IKEv2)
   - Transmission Control Protocol/Internet Protocol (TCP/IP), also known as the Internet protocol suite
   - Dynamic Host Configuration Protocol (DHCP)
   - Domain Name System (DNS) protocol
   - Network Basic Input/Output System (NetBIOS) and Windows Internet Naming Service (WINS) protocols
   - Authenticated Ethernet through the 802.1X protocol
3. The network service order list is used to determine the primary network service interface if more than one service is active. All network traffic that isn’t better handled through local connection to an active network service interface is sent to the primary network service interface. So in most cases, all WAN traffic, Internet traffic, and DNS resolutions are sent through the primary network service interface.
4. In Network preferences, network service interfaces with a green status indicator are being used for network activities. All network traffic that isn’t better handled through a local connection is sent to the primary network service interface. The primary network service interface is the topmost active interface in the listing.
5. The easiest way to configure VPN settings is to use a configuration profile containing all the relevant VPN setup information.

6. macOS High Sierra uses two configuration methods for 802.1X:
   a. Automatic configuration through the selection of a Wi-Fi network that requires WPA/WPA2 Enterprise authentication
   b. Semiautomatic configuration through an 802.1X configuration profile provided by an administrator

Lesson 23—Troubleshoot Network Issues

Goals

• Identify and resolve network configuration issues.

• Verify network configuration with Network preferences.

• Use Network Utility to aid in troubleshooting.

Review questions

1. What are three common issues that can interrupt network services on a Mac computer?

2. How can you identify the MAC addresses for all the Mac computer's network interfaces?

3. How can you verify basic connectivity to another network host?

4. How can you verify that DNS host name resolution is working?

5. How can you verify that the system can establish a connection to a remote network host?

Answers

1. These three common issues can interrupt network services on a Mac:
   a. Local issues—Usually related to either improperly configured network settings or disconnected network connections.
   b. Network issues—Use network diagnostic to help you investigate possible causes.
   c. Service issues—Related to the network device or service you are trying to access.

2. You can identify all the MAC addresses for the Mac computer’s network interfaces from the Info pane in Network Utility.

3. You can use the Ping tab in Network Utility to test basic connectivity to another network host by sending a ping packet and then waiting for its return.

4. You can use the Lookup tab in Network Utility to test name resolution against the currently configured DNS server.

5. You can use the Traceroute tab in Network Utility to verify the connection hops between your Mac and a remote host.
Part Seven: Network Services

Lesson 24—Manage Network Services

Goals
- Describe how macOS accesses shared network services.
- Configure built-in macOS network apps.
- Browse and access network file services using the Finder.
- Troubleshoot network shared service issues.

Review questions
1. What’s the relationship between clients, servers, and network service access?
2. What’s the relationship between a network service and a network port?
3. What’s the primary interface for configuring network service apps?
4. How does macOS High Sierra use dynamic network service discovery protocols to access network services?
5. Which two dynamic network service discovery protocols are supported by macOS High Sierra?
6. Which five network file services can you connect to from the Finder “Connect to Server” dialog?
7. How are items inside the Finder Network folder populated?
8. In what two ways can you automatically connect a network share?
9. What are three common troubleshooting techniques you can use when you can’t connect to network services?
10. How can you verify that a specific network service is available from a service provider?

Answers
1. Client software is used to access network services that are provided by server software. The client and server software use network protocols and standards to communicate with each other.
2. Network services are established using a common network protocol. The protocol specifies which TCP or UDP port number is used for communications.
3. Internet Accounts preference is the primary interface in macOS High Sierra for configuring built-in network apps.
4. Devices that provide a network service advertise their availability through a dynamic network service discovery protocol. Clients who are looking for services request and receive this information to provide the user with a list of available network service choices.
5. macOS High Sierra supports Bonjour and Server Message Block (SMB), including support for the legacy Network Basic Input/Output System (NetBIOS) and Windows Internet Naming Service (WINS) dynamic network service discovery protocols.
6. From the Connect to Server dialog in the Finder, you can connect to these services and systems:
   • Server Message Blocks/Common Internet File System (SMB/CIFS)
   • SMB2/SMB3
   • Apple File Protocol (AFP)
   • Network File System (NFS)
   • Web-based Distributed Authoring and Versioning (WebDAV)
   • File Transfer Protocol (FTP) network file services

7. The Finder populates the Network folder using information provided by the dynamic network services discovery protocols. Computers that provide services appear as resources inside the Network folder, and service discovery zones or workgroups appear as folders. Any currently connected servers also appear in the Network folder.

8. To automatically connect a file share when a user logs in to the system, drag the share from the Finder to the user’s login items in Users & Groups preferences. Or you can drag the share to the right side of the user’s Dock, and it will automatically connect when the user clicks the share’s icon in the Dock.

9. Review Network preferences, review the Network Utility statistics, and try to connect to different network services.

10. To verify whether a specific service is available from a service provider, first use the Network Utility Ping tab to verify basic connectivity. Then use the Network Utility Port Scan tab to verify that the specific service ports are open. You should always limit the port scan to the specific ports required for the network service you’re testing.

Lesson 25—Manage Host Sharing and Personal Firewall

Goals
   • Examine and enable host-sharing services built into macOS.
   • Examine and enable Content Caching services built into macOS.
   • Use screen-sharing tools to access other network hosts.
   • Use AirDrop to quickly and easily share files.
   • Secure shared services by configuring the personal firewall.
   • Troubleshoot shared service issues.

Review questions
1. Which sharing services can macOS High Sierra provide?
2. What is Content Caching?
3. Which app can provide on-demand screen sharing even when the Screen Sharing service isn’t enabled?
4. Which network service or services does Screen Sharing need in macOS High Sierra?
5. What’s AirDrop, and how do you know if a specific Mac supports it?
6. If other devices with AirDrop enabled don’t appear in the AirDrop browser, which two settings on a Mac can you change to potentially make more devices appear?
7. In what primary way does the macOS built-in firewall differ from a traditional network firewall?
8. In macOS High Sierra, what are the firewall settings?

**Answers**

1. The macOS High Sierra Sharing Services include the following:
   - Remote Disk (DVD or CD sharing)
   - Screen Sharing
   - File Sharing
   - Printer (and scanner) Sharing
   - Remote Login
   - Remote Management (ARD)
   - Remote Apple Events
   - Internet Sharing
   - Bluetooth Sharing
   - Content Caching

2. Content caching is the downloading of software distributed by Apple and of data that users store in iCloud by saving content that local devices have already downloaded.

3. Messages provides on-demand screen sharing that you can use when the system screen-sharing service isn’t enabled.

4. In macOS High Sierra, Messages screen sharing uses iMessage. Users on both Mac computers must sign in to iCloud.

5. AirDrop provides a quick and easy way to share files within local Wi-Fi and Bluetooth range. AirDrop creates a secure peer-to-peer network between local devices. From the Finder Go menu, you can verify that a Mac supports AirDrop.

6. On a late-model Mac, you’ll find two settings at the bottom of the AirDrop browser that control AirDrop discovery. The first setting expands AirDrop discovery from only users in your Contacts to everyone within AirDrop range. The second setting makes AirDrop revert to the previous discovery method, which allows your Mac to discover older Mac computers and Mac computers that run previous versions of Mac operating systems.

7. With the firewall built into macOS High Sierra, connections are allowed or denied on a per-app basis. This is unlike traditional network firewalls, where access rules are based on network service port numbers.

8. In macOS High Sierra, these are the firewall settings:
   - Block all incoming connections.
   - Automatically allow built-in software to receive incoming connections.
   - Automatically allow downloaded signed software to receive incoming connections.
   - Enable stealth mode.
Part Eight: System Management

Lesson 26—Troubleshoot Peripherals

Goals
• Manage peripheral connectivity.
• Pair Bluetooth devices to your Mac.
• Troubleshoot peripheral and driver issues.

Review questions
1. What are the four primary peripheral bus technologies supported by Mac computers that run macOS Sierra?
2. What must occur for a Mac to communicate with a Bluetooth peripheral? Where can you configure this pairing?
3. What’s a device driver? What are the three primary types of device drivers?
4. How does macOS High Sierra support third-party devices without needing third-party device drivers?
5. What can you infer about a connected peripheral if it doesn’t appear in the System Information app?

Answers
1. These are the four primary peripheral bus technologies supported by macOS High Sierra:
   a. Universal Serial Bus (USB)
   b. FireWire
   c. Bluetooth wireless
   d. Thunderbolt
2. Bluetooth devices must be paired for communication to occur. Bluetooth preferences in the System Preference app are responsible for pairing a Mac with Bluetooth peripherals. You can quickly open Bluetooth preferences from the Bluetooth status menu.
3. A device driver is software specially designed to facilitate the communication between macOS High Sierra and a peripheral. These are the three primary types of device drivers:
   a. Kernel extensions
   b. Framework plug-ins
   c. Standalone apps
4. macOS High Sierra uses built-in generic drivers based on each device class. For example, generic drivers for scanners and printers can be used instead of official third-party drivers.
5. If a connected peripheral doesn’t appear in System Information, the issue is probably hardware related. Troubleshoot accordingly.
Lesson 27—Manage Printers and Scanners

**Goals**
- Describe the technologies that enable macOS to print.
- Configure macOS for printers and multifunctioning devices.
- Manage and troubleshoot print jobs.

**Review questions**
1. What does the Common UNIX Printing System (CUPS) do?
2. What are PostScript Printer Description (PPD) files responsible for?
3. What’s the best source for acquiring printer drivers for macOS High Sierra?
4. Under what circumstances can a standard (nonadministrative) user configure a printer?
5. How do you share printers with other users?
6. How can you select a new printer driver for a configured printer?
7. If it appears that all configured printers are having problems, what’s a potential quick fix?

**Answers**
1. Common UNIX Printing System (CUPS) manages printing for macOS High Sierra, including local and shared printing.
2. PostScript Printer Description (PPD) files are printer driver files that instruct CUPS on how to communicate with specific printer models.
3. The Apple print drivers are the best source for configuring macOS High Sierra printers. One way to acquire printer drivers for macOS High Sierra is to let the software update system automatically download and install the appropriate printer drivers. Or you can manually download and install printer drivers from the Apple support website.
4. Assuming the default settings for macOS High Sierra, a standard user can configure only directly attached or local network printers from the Print dialog. Also, the appropriate drivers must be installed before the standard user configures the printer.
5. You can enable printer sharing from Print & Scan or Sharing preferences. Windows clients may need additional drivers to access Mac shared printers through the Internet Printing Protocol (IPP).
6. It depends on the printer. From Printing & Scanning preferences, sometimes you can select a new printer driver from the Options & Supplies dialog. In many cases, to select a new printer driver for a configured printer, you must delete and then add the printer again.
7. If your printers are having problems, you can reset the printing system by Control-clicking in the printer list and then choosing “Reset printing system.”
Lesson 28—Troubleshoot Startup and System Issues

Goals
• Describe the macOS startup process.
• Examine the essential files and processes that are required to successfully start up.
• Learn about macOS startup modes.
• Troubleshoot startup and login processes.

Review questions
1. What are the primary system initialization stages in macOS High Sierra? What visual and audible cues do these stages provide?
2. What does the firmware do? What’s the Power-On Self-Test (POST)?
3. What role does launchd serve during Mac startup?
4. Which items are automatically started by launchd during Mac start up?
5. What are the primary user session stages in macOS High Sierra? What visual and audible cues do these stages provide?
6. What’s the difference between launch daemons, startup items, launch agents, and login items?
7. What are Safe Sleep and Power Nap?
8. What happens during user logout?
9. What happens during Mac shutdown?
10. Which keyboard shortcut is used to start up in safe mode?
11. Which keyboard shortcut can you temporarily use to choose another startup disk?
12. Which changes are made when macOS High Sierra starts up in safe mode?
13. Which items aren’t loaded when macOS High Sierra starts up in safe mode?

Answers
1. Each primary stage of system startup can be indicated by the following cues:
   b. Booter—The booter process starts. The Apple logo is displayed in the center of the main display.
   c. Kernel—Kernel startup. The progress bar is displayed.
   d. System /usr/libexec/launchd—Starting other items. The Apple logo is replaced with login window.

2. The firmware initializes the Mac computer’s hardware and locates the startup file on a system volume. The POST checks for basic hardware functionality when a Mac powers on.

3. launchd is responsible for starting macOS High Sierra processes. It also manages macOS High Sierra initialization and starts the loginwindow process.

4. During macOS High Sierra startup, launchd starts these daemons and scripts:
   • /System/ Library/LaunchDaemons
   • /Library/LaunchDaemons

5. Each primary stage of a user session can be indicated by the following signs:
   a. The login screen displays.
   b. launchd loads apps, such as the Finder, after user authentication.
c. The user environment is active any time a user logs in to macOS High Sierra.

6. The administrator account `launchd` process launches Launch daemons and startup items during Mac start up. User account `launchd` processes launch agents and login items during user environment startups.

7. When a Mac battery drains, Safe Sleep saves the macOS High Sierra state to permanent storage. Power Nap enables a Mac to automatically wake in low-power mode. This enables the Mac to perform app and macOS High Sierra updates.

8. During user logout, the user’s loginwindow process performs these actions:
   a. Requests that user apps quit
   b. Automatically quits user background processes
   c. Runs logout scripts
   d. Records the logout to the main system.log file
   e. Resets device permissions and preferences to their defaults
   f. Quits the user’s loginwindow and `launchd` processes

9. When a Mac shuts down, loginwindow logs users out and then tells the kernel to quit the remaining macOS High Sierra processes. Then the Mac shuts down.

10. Hold down the Shift key during startup to initiate safe mode.

11. Hold down the Option key during startup to open Startup Manager. This enables you to temporarily choose another startup disk.

12. Startup in safe mode performs the following permanent actions:
   a. Attempts to repair the system volume structure
   b. Deletes system third-party kernel extension (KEXT) caches
   c. Deletes font caches

13. When macOS High Sierra performs a startup in safe mode, it doesn’t load KEXTs, third-party launch agents, third-party launch daemons, third-party startup items, third-party fonts, any user login items, or any user-specific launch agents.